INTERNATIONAL HELLENIC UNIVERSITY

Security baseline frameworks - a case study for public administrations

Dorotheos Epeslidis

SID: 3307210001

Supervisor: Assoc. Prof. Konstantinos Rantos

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

JANUARY 2023

THESSALONIKI – GREECE

Abstract

In an era of financial and environmental crisis, many daily procedures have been affected by attacks that only aim to harm the common good and interfere with the normality of the current administrative, and not only, operations. The actions of those cyber-related vulnerabilities can easily be countered if only the proper measures are taken. This dissertation suggests a functional and operationally feasible way of defending against such attacks in the particular case of public administrations. This case study consists of numerous implementations made as a result of extensive study of already established cybersecurity frameworks with emphasis in those created by the National Institute of Standards and Technology (NIST) and the Center of Internet Security (CIS), while also, from Information Security Management Systems, like that of the European Union Agency for Cybersecurity (ENISA) and the International Organization for Standardization (ISO). This is not a formal implementation of a security baseline framework but stands as a suggestion explicitly made for the needs and the current situation around the Greek public administrations.

Keywords: Cybersecurity Framework, Threat, Vulnerability, Malicious Actor, Controls, Public Administration

Dorotheos Epeslidis

Date 07/01/2023

Disclaimer

The suggested cybersecurity baseline framework does not represent a complete and tested framework like the already published and well-established ones. In the implementation of the framework, the needs of the Greek public administration bodies were taken into consideration. Medium sized (for the Greek standards) organizations were taken into consideration.

The information that was collected and is displayed in this dissertation is originating from publicly available information and is follows the country’s existing legal framework.

Acknowledgments

I would like to say a special thank you to my supervisor, Assoc. Prof. Konstantinos Rantos, His support, guidance, and overall insights in the creation, editing and completion of this dissertation were crucial and made this an inspiring experience for me. Hopefully, this dissertation can help the Greek public administrations understand the risk of the internet and can later consider a different approach around the cybersecurity.

Contents

FIGURE CONTENTS

1 Introduction

1.1 Background

It all begun back in 1834 when a pair of thieves decided to hack into the French Telegraph System and steal financial market information which later on, agreed to be the world’s first ever cybercrime. Ever since, as the technological evolution was proceeding, more and more attacks like this, were happening. In the beginning we have the telephones and the call centers, where attacks were a result of human interventions and manipulations of assets such as redirection of calls and intentional misdirecting and disconnecting of them. Years after, in 1940, during World War 2, the first ever Ethical Hacker acts on behalf of the Resistance in the Nazi-occupied France and finds out that the Nazis were using punch-card machines in order to process and track down Jews and then intervenes to prevent their plan[1].

As years pass, similar attacks are happening more regularly without the governments having a way to counter them or prove them. Viruses, malicious software, and worms have started being created by people who try to infiltrate into other systems and retrieve the information of their liking. During those times, this kind of attacks are in high focus as they are considered something extremely new and therefore something very hard to control.

As a result, this had to stop. Right after the end of World War 2, companies started forming plans in order to protect themselves against attacks like the previously mentioned ones, while also, natural attacks that were not manipulated by humans. Therefore, they created a series of actions that should been taken based on the type of attack they were experiencing. Companies that were incapable of creating their own, due to lack of personnel with this knowledge or lack of funds, were contacting organizations that were experts in this field.

One of the first organizations that created a complete security framework is the well-known International Organization of Standardization (ISO), that in 1998, released some guidelines for the management of the IT security. Until now, not only ISO but other organizations like the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS) have developed guidelines that cover a vast number of possible threats. As it is obvious, those guidelines cannot fully provide a complete list of counter measures, due to the increasing number of the cyber-threats.

All those series of guidelines are integrated into an information security risk management process that each organization forms differently. But they all aim in one thing; to identify a threat and treat it accordingly, without allowing it to enter the target system and perform any malicious action.

1.2 Dissertation subject

The aim of this dissertation is to develop a security baseline framework that supports the proper defending of a Greek public administration against any cyber incidents that could alter the integrity of it and hurt, in general, the cause it represents. The way such administrations are formed through the years, has left behind possible openings for threats to occur, and exploit the overall system they belong in. Those threats can either be a result of human interventions or of a natural occurrence that has not been planned and therefore cannot be foreseen.

In this dissertation, the developed security baseline framework, will have its own risk assessment and treating process that will immediately reflect from the capabilities and the given financial and social situation of the public administration.

2 Cybersecurity

We live in a world that needs desperately to feel and be safe. Starting from the normal security we all know, there has always been of high importance for people everywhere in the world whether they are poor or rich, live in the city center or in a village, to be safe and protected. Same goes to the Internet world. A new world that is presented to us relatively late. Nevertheless, we have all acknowledged its existence and usefulness and that is why we are almost depending on it on our daily operations. The cybersecurity, as it is called, is the ability to have protection of our electronic equipment, our communication systems, and any other device we use. One of its many features is to prevent the damage to those devices and ensure that the basic principles of cybersecurity are being preserved. These principles are called in short, the "CIA triad" that refers to Confidentiality, Integrity, and Availability of information in the development of a security system.

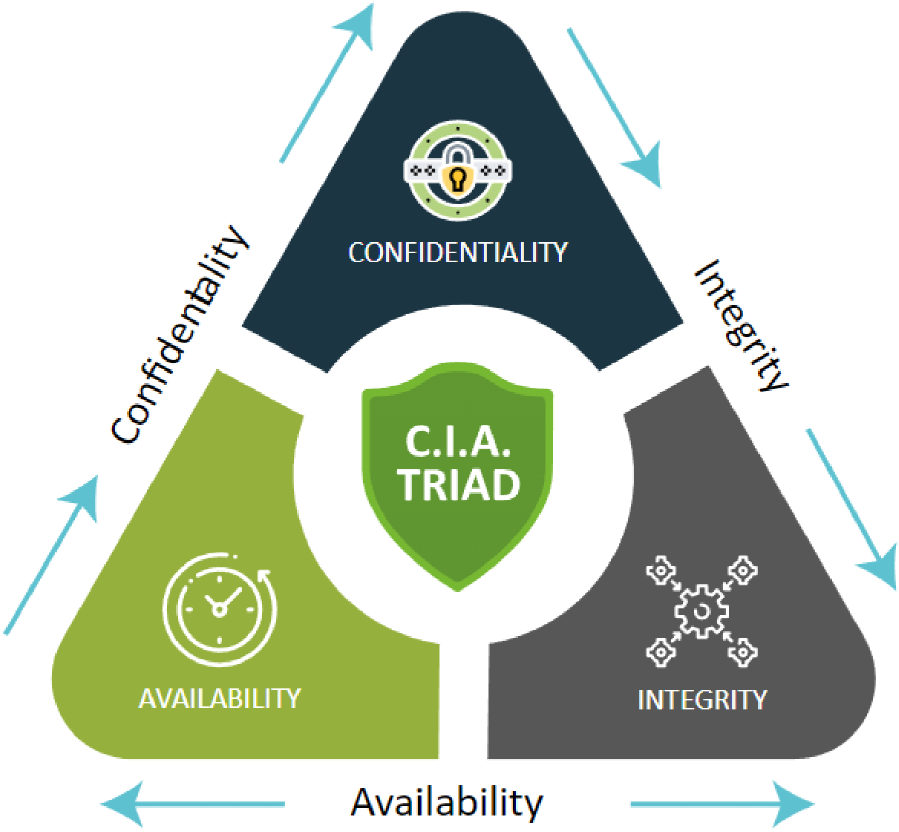


Figure 1: Confidentiality, Integrity, and Availability

2.1 Current Situation of Cybersecurity

As of now, some things are guaranteed when talking about the security of the Information Technology (IT) world. Every system consists of points, called vulnerabilities, that are likely to be exfiltrated by unknown sources. For this we need a way to protect it, such as a Firewall, an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS), all of which play a different role in this process. Then we know, that in some point in the near or distant future, every system will be subject of an attack or will be influenced by some threat, and based on the severity, negative outcome will be produced. And finally, no system or combination of systems can detect, prevent, and counter all the threats. For this reason, the CIA triad should be followed as it offers a simple yet complete guidance that allows the organizations to have a full self-evaluation of the defensive approach the utilize.

2.1.1 CIA Triad

Before we procced deeper into this dissertation it is very important to have an understanding around the base principles of information security. The previously mentioned CIA Triad[2].

Confidentiality

In the first principle we must ensure that nobody outside of our organization should be involved in our transactions and operations. Hence the content will be confidential to some and not to all. The data must be protected, and only authorized entities should have access to them. If we want to send a message to our supervisor for instance and we only want our supervisor to access it, we need to ensure that only legitimate parties can do that. If a third-party entity tries and manages to grand access to our message and views the content of it, we have loss of privacy and therefore absence of confidentiality. Given that we encrypt the message, only the sender and the receiver will know both the message and the key to perform the necessary actions to view it. Then we ensure the confidentiality.

Integrity

In the second principle, we must make sure that the exact amount of data sent is actually received without any alterations. We do not want any modifications of messages by unauthorized entities. If we want for example to send specific data to our supervisor and even though we make the transaction, but the data ends up on a different person, an intermediate threat actor like a hacker has managed to alter the information that accompany the message and manipulated the destination of the message. That means that we cannot ensure that there is no modification of the transmitted message and as a result, we have loss of integrity. In addition to the encryption of our message we should use other preventive mechanisms such as a digital signature. This way, we will guarantee to the receiver that the origin of the message is the on it should have been in first place and no manipulation has occurred during its sending. Then we ensure the integrity.

Availability

In the third principle, we must make sure that the means we use for the sending of our message are always available. It is not acceptable to try and send confidential information and have no way to do that. We need to be sure that we are authorized to access the needed resources whenever we need to. After we have encrypted our message and digitally signed it, we have achieved the first two steps of the security process, but all is in vain if our application has been under a denial-of-service attack. This is why, we need to prevent in advance similar possible attacks and update and upgrade our systems. Then we will ensure the availability of our systems.

2.2 Cyber world terminology

In this section we need to explain some of the key terms that are included in all the security frameworks and in combination to the CIA Triad, surround the overall landscape of the cybersecurity world.

2.2.1 Threat

According to NIST the (National Institute of Standards and Technology), a threat is “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”[3]. In the Internet world, a cyber or cybersecurity threat is originating from people or groups of people that are called threat actors. They can be as small as Hacktivists, who act individually or in small groups that spread propaganda rather than causing actual damage to systems or services. Or they can be as big as entire nations classified as

Hostile Nation States that are considered to be one of the highest risk threat actors due to their expertise and ability to cause serious damage to enemy infrastructures. On the other hand, there are threat actors that we cannot identify or measure. They are the natural disasters that can easily and without notification disrupt any key infrastructure just like any other cyber-attack will. They have no target, and they have no mercy or morality. A very important point, security frameworks try to counter putting a lot of effort in, other with bigger and other with smaller success.

Every cyber threat is evolving and is becoming smarter day by day, month by month, year by year. Threat actors are becoming more in numbers and better in expertise. As a result, each year, lists of the most pernicious cyber threats are published so people and organization know how they should change their approach. Year 2022, so far, is full of Covid-Themed Phishing attacks, Ransomware attacks and Malvertising (malicious advertising) among others.

As we all understand, we need to first be able to identify the possible threat and then have a way of resolving it. Throughout the years, organizations like ENISA have been publishing the annual threat landscape meaning that we have the list of most common cyber-attacks, while also ranked from most common to less common that are referred to, as prime threats. The latest report we can access is the one of year 2021 which ranks Ransomware in first place, Malware in second, and Cryptojacking in third while threats like are related to e-mails, data and supply-chain follow the list.[4] In addition to that, from that report, we can observe the actual monthly timeline of those threats, with most been witnessed on July, while also, the sectors of the industry the threats were most perceiving and more in numbers, with most been witnessed in Public administrations/Government. Furthermore, there is a list of the threat actors that performed the above-mentioned attacks; more details will be explained in Paragraph 2.2.4.

There is also a global effort to distinguish and identify all the threats that are out, and for this reason, there had to be an agreement to have a common language and refer to the same threat using the same name. With appropriate terminology, threats can be categorized and characterized based on their features for a better hunting and sharing them. To this, comes to play its role, the Cyber Threat Intelligence (CTI), which acts as a database that stores information, which originated from various sources, regarding the known threats or potential threats to the organizations. Having all those information gathered, risk frameworks were created that give the organizations the ability to measures the significance of each threat and understand if it is of threat to them. About this, more details can be found in Paragraph 2.5.

In general, a threat can be any negative happening or action in the Internet world that can possibly damage any asset and therefore must be protected. The threats that we are discussing about, that are related to the information systems, can and have been classified and categorized in four different categories based on the level of detail they have and the components of them around the system they are trying to affect. These categories[5] are as follows:

Hardware Threats – Here we have attacks that are very sophisticated and need experienced attackers to perform and can cause damage to equipment such as the hardware, firmware, storage medias, circuits, etc.

Software Threats – The attacks that are included in this category are built around specific operation systems or family of systems. They are not very sophisticated attacks as they do not require special knowledge around their execution and use.

Network Threats – In this category, the attacks are affecting the communication channels of the electronic equipment by using networking protocols to infiltrate into systems that are connected to the network. These attacks are known for being easy to execute as a one of the most famous network targets is the wireless networks. The network attacks can be combined with software type attacks since they belong to the same layer.

Cyber Supply Chain Threats – When talking about supply chain, we have a series of components and sub-components we can think of, that are easy to be attacked. Any exposure made to the systems that are filled with those components can reach the personnel, the elements and the services of an organization and compromise its security. Even though these attacks can easily be customed to specific supply chain systems, there are not many attackers that try to attack them and therefore they are not considered very popular.

2.2.1.1 Hardware Threats[6]

It is in the nature and the structure of the equipment that is been used by organizations worldwide to be dependent on two essential pillars, the hardware, and the software. The hardware part is what the equipment is using to perform its operations. It is referring to the processor, the storage media, the circuit boards etc. It is all those components that are needed to have a normal function of a system and as we all understand if one component is not working properly, then the whole system does not work properly either.

Hardware issues happen at a very frequent base. Threats here, can exist at any point in the lifecycle of the systems, from the very first boot of them until the end of their life. For this reason, the list of hardware threats is huge, and it becomes very difficult to enumerate, categorize and identify all of them. But of course, we can focus on some widely accepted ones that are extremely likely to have happened to all organizations. In this effort, a crucial milestone has been played by the Hardware Threat Landscape and Good Practice Guide[7] ENISA has published in the year 2017. Below we will explain some of the above-mentioned threats and try to understand their behavior. Also note that the threats below are listed from the most severe to the least severe. Others might disagree but everyone's opinion is accepted.

1. **Legal and Compliance**

   In the era we are living in, organizations are obliged to follow specific rules and regulations around the cybersecurity landscape. In the European Union, the General Data Protection Regulation (GDPR) is in force and any organization that tries to stay away from it, will face steep fines that could influence to the worst possible extend the existence of the organization itself. The attack pattern of threat in this category is:

   (a) Violation of Laws / Regulations / Compliance

   (b) Violation of Contract

2. **Disruption**

   In this category we can witness failures, malfunctions or outages that are able to disrupt the services performed by systems that are connected to them. Even though disruptions could be done from environmental factors, this category covers only threats that could be performed by threat actors. The specific attack pattern this type of threats have, is:

   (a) Denial of Service

   (b) Vulnerability Exploitation

   (c) Communication Outage

   (d) Authentication / Authorization Failure

3. **Intentional or Unintentional Damage**

As the environment is changing, so do the extreme conditions in the pass of each season. This particular category of hardware threats consists of threats that are very difficult to forecast due to their nature. Here we have attacks by the nature itself like earthquakes, volcanic eruptions, or thunderstorms. The attack pattern those threats follow is listed below:

(a) Heating / Cooling Functionality

(b) Environmental / Man-made disasters

(c) Excessive Resource Consumption

(d) Power / Communication / Display / Audio Interfaces

4. **Man-in-the-Middle (MITM)**

The MITM term is perfectly explaining the unauthorized interference of someone or something between the two sides of a traffic transfer of communication system that could view, modify, or alter, the normal performance of it. The attack pattern this kind of threats follow is:

(a) Network Traffic

(b) Memory Bus Traffic

(c) Sensor Traffic

(d) Audio Traffic

5. **Abuse**

When we misuse a hardware asset and harm the durability of it and the services it provides, then have performed an abuse to its security. This term is used to describe threats that have managed to grand themselves unauthorized access to data or assets or gained somehow the ability to alter those data and assets without the approval of the owner(s). The attack pattern this type of threats have is explained in the following categories:

(a) Hardware / Firmware Modification

(b) Over-the-Air Update

(c) Boot Loader Modification

(d) Memory Corruption

(e) Local / Remote Management / Debug Interfaces

The threat landscape is changing, and, in my opinion, this will be the order of the threats list that will happen the following years based on the current situation. Even though Hardware abuse is very common in our days, there are many ways to counter it as security updates and fixes are happening constantly. At one point, all the "open" holes of the hardware will be patched and the interest of attackers in them will be extinct. Environmental threats will never stop existing given that the greenhouse effect and the pollution are continuing to alter the normality of our planet. Security the hardware layer in an organization, is a complex way since changes in all the layers must be done holistically.

Software Threats

Unlike the hardware that is compromised of the components of a system, the software focuses on the "how" this system is operating. It is immediately connected to the hardware while it provides the necessary processes that are required for the execution of the needed actions. Software is covering a vast domain and it can be identified by its many categories and sub-categories. It is undeniably the "blood" that runs in the inside of the systems and therefore is keen on receiving attacks that could possibly cause serious damage to the system as a whole and not only the software explicitly.

The complexity of the structure of the software is not stopping malicious actors to try and infiltrate it. Attacks here can either be forced by the human or caused by other factors that remain unpredictable. The MITRE Corporation in the Common Attack Pattern Enumeration and Classification (CAPEC)[8] they have released, is explaining threat and attack patterns that define the software threats. Below we will explain some common threats which are listed based on their severity, similarly to the list of Hardware threats in the previous section.

1. **Integrity Attacks**

   One of the elements of the triad that compromises a system, organization or entity is the Integrity. As integrity in the Internet world, we are referring to our data are being delivered intact without any change. This is why we need to be protected from attacks that try the opposite. These attacks are clever, but their implementation is easily recognizable. The attack pattern of this category is:

   (a) Software Integrity Attacks

(b) Malicious Logic Insertion

(c) Contaminate Resource

2. **Man-in-the-Middle Attack (MITM)**

Like the Hardware threats, here we have unauthorized entities that try to perform attacks on the communication media between different software within the same system or of different systems that co-exist. Threats in this category have attack pattern as below:

(a) Application API Message Manipulation via Man-in-the-Middle

(b) Leveraging Active Man-in-the-Middle Attacks to Bypass same Origin Policy

(c) Packet Sniffing and Packet Injection

(d) Session Hijacking

3. **Access Control Subversion**

Daily attacks are happening from people that are pretending they are someone else. One of the threats they pose to organizations is the Access Control Subversion which is done by impersonations of legitimate authorized users or by manipulation of existing users' privileges. Even though there are models and technics to counter this type of attack, attackers find clever ways of achieving similar actions. This type of threats follows a specific attack pattern similar to the below list:

(a) Exploitation of Trusted Credentials

(b) Exploiting trust in Client

(c) Authentication Abuse

(d) Authentication Bypass

(e) Privilege Abuse

(f) Privilege Escalation

4. **Denial of Service (DoS)**

This is a very general term that covers every threat that has as goal to exhaust the attacking system by consuming its available resources and reaching it to its limits. Hence their standard procedure, DoS attacks are relatively easy to identify in advance and prevent in time. However no complete protection against them is possible as of today. The attack pattern of this category is:

(a) Forced Deadlock

(b) Flooding

(c) Excessive Allocation

(d) Resource / Memory Leak Exposure

5. **Manipulation**

This category is comprised of a big list of threats that try to change the correct settings of a system that have originally set by the creator of the software. They act is a way so as to create sudden and unpredictable conditions that take time to resolve. These conditions could either be some unauthorized access to data or some malicious code execution. The possible scenarios are many and all have similar attack pattern as the list below:

(a) Manipulating User State

(b) API Manipulation

(c) Buffer Manipulation

(d) Shared Data / Input Data Manipulation

(e) File Manipulation

(f) Configuration / Environment Manipulation

6. **Injection**

One old-school method of achieving the leakage of information, code execution and privilege escalation without being noticed, is by injection technics. These threats may or may not be malicious, but the intention of their execution is only malicious. Injection threats follow an attack pattern similar to the following:

(a) Parameter Injection

(b) Resource Injections

(c) Code Injection / Local Execution of Code

(d) Command Injection

(e) Object Injection

(f) Code Inclusion

7. **Spoofing**

Spoofing threats are cause by malicious interactions in the case of impersonation of legitimate users that convince other users to initiate a communication with them. Users remain unaware that the other communication end is not who its supposed to be and freely exchange information that could harm the organization they belong into. A typical result of such attacks it leakage of information that could by itself result into security of privacy breach. The attack patter in this category is as below:

(a) Content Spoofing

(b) Identity Spoofing

(c) Resource Location Spoofing

(d) Action Spoofing

Network Threats

While systems and computers are perfect for processing raw data but also require a medium to transfer them to other systems and communication with other computers or equipment in general. For this process, they are using the network that can connect endpoints, makes the workflow easier and in general benefit the daily operations of an organization. Since it is connected to the hardware and software of the information systems, it also becomes a troublemaker when it comes to security. The trouble the network is creating, is not small and neglectable. On the other hand, it is extremely dangerous to the nature of the organization and if exposed, the data and assets are in great danger.

The information that is being transferred through the network, is controlled by different protocols. Other protocols are implemented for the security of a system and others for the ease of access of the users. These protocols have passed from a series of enhances and evolutions until they reached the version they have today. Networking protocols are specially designed software that undertake the transmission, processing and receiving of information between interconnected systems. The threats they are facing are similar to those of the software explained previously. Famous protocols that are keen on being attacked on a daily basis are protocols that not only organizations use but also people in their routines. For instance, when we connected to a public Wi-Fi the protocols that are been used in that, are of the Wireless Local Area Network (WLAN)[9] category such as the IEEE 802.11a or the IEEE 802.11n[10] or alternatively when we turn on the cellular data on our mobile phone, we are activating the GSM/CDMA[11] networking protocols. These are only few of the many protocols that surround the networks. Some are wireless and some are wired.

From the side of the attacked, it is not guaranteed that physical access is required as the network can be manipulated remotely. They can be located somewhere between the proximity nodes the particular network is transmitting from and to. This means that an attacker can be at another country or even at another continent. Below, there is a list of network threats that are ordered based on the future landscape they might belong into.

1. **Information Leakage**

   When dealing with the network that connects two or more systems, we are talking about exchange of information. The information that is being transferred could be important, sensitive, or public. There might be personal details of passengers of a flight or the schedule of a public transport media. Any information can be collected maliciously by two methods, actively and passively. The active approach consists of brutal methods such as Brute Force Attacks and the passive approach consists of information gathering by observation technics such as Direct Observation. The attack pattern of this threats is described below:

   (a) Footprinting

   (b) Protocol Analysis

2. **Access Control**

   Similar to software threats, the adversary in this situation is accessing data vis camouflage technics like pretending to have the identity of someone with privileged access to the organization’s systems. This way, trust is gained from the normal users of the systems and exploitation is achieved. Threats of this category have the following attack pattern:

   (a) Exploiting Trust in Clients

3. **Interception**

   When we exchange data or information with someone in the network, we do not want some third entity to participate in the exchange. Depending on the nature of the transferred information, unauthorized access can be gained by a malicious actor that can intercept the organization’s systems and resources. Due to the sophistication of such attacks, they are high in the list of most threatening attacks. The attack pattern they have is the following:

(a) Sniffing

(b) Eavesdropping

4. **Spoofing**

   The impersonation that an attacker is achieving for stealing information from a software is very similar to the technics that network scammers are using. This type of attacks can include Data Breaches and leaks in the security and privacy of the information. The attack pattern of those attacks is:

   (a) Resource Location Spoofing

   (b) Content Spoofing

   (c) Identity Spoofing

5. **Protocol Manipulation**

   Threats in this category are performed with attempts of injection information into the communication media that pass via a wired or wireless network connection. The goals of such attacks are to find exposures in the security of the organization and reveal vulnerabilities they can be used for performing attacks in the near future. Even though Protocol Analysis is a way to perform attacks that belong in this category, they differ from those of the previously discussed threats in the Information Leakage category. The attack pattern that is followed here is:

   (a) Traffic Injection

6. **Obstruction**

   This is a standard technic of denying the access of the user in the organization’s systems. The attacker in this situation, can either destroy network equipment or just lurk in the network transmission mechanisms that are been used. Depending on the type of the media the network is using we have different kind of attacks. While the signal jamming can be performed in wireless media, such attack will have no result if performed in wired media. This category has the following attack pattern:

   (a) Physical Destruction of Networking System

   (b) Route Disabling

(c) Jamming

(d) Blockage

Cyber supply Chain Threats

At any organization in the world, whether it is considered large or small, there is and should be a supply chain system. The supply chain is the connection that exists between the employees, the activities of them, the information, and the resources when dealing with parts, components or finished products so as to reach their final destination. It is a network that requires perfect coordination between all the ends. But as it is very clear and obvious, this network is also keen on receiving numerous attacks that are aiming to alter the normality of the operations within the organization.

A Supply chain system could be restricted in size to an organization in a specific area or could be big enough to cover countries. Therefore, the management and organization of it, is crucial to its reliability and security. The personnel that will be part of this supply chain system, must be well trained, skilled, and experienced enough so no mistakes happen. For that, organizations should emphasize of protecting this network on every aspect of it, whether it is personnel, business units of products.

As part of a Cybersecurity Framework, organizations can adopt a specific to supply chains system domain that is called the Cyber Supply Chain Risk Management. Within this domain, the organization will have coordinated approaches to incidents that might occur that refer to the supply chain network. In addition to that, the role of this domain might be even more important as the always changing laws, and regulations of countries are increasing in numbers. Threats to the supply chains are nothing new; they always existed, just in smaller numbers. As not much expertise in this field existed, those attacks were not understood by the organization and very rarely countered by them. And for that, the attackers decided to approach parts of the supply chains of organizations, that would be difficult to realize and counter.

The MITRE Corporation in the Common Attack Pattern Enumeration and Classification (CAPEC) repository and Supply Chain Attack Framework and Attack Patterns[12] has focused on the supply chain attacks and how they are realized. They tend to be focusing on components that are being used within the activities of an organization and if not controlled early enough, their damage could be permanent. Other attacks could offer unauthorized access to intruders to the key machines of the supply chain that for instance might change the destination of delivery of products.

Below follows a list of the attacks that are been considered as harmful with sorting based on their future impact and possibility of happening the following years.

1. **Substitution**

   One of the actions an attacker can perform when granting access to the systems of the supply chain network of an organization is that of replacing the components he finds in some points in the system with others or changing their order. The substitution is considered successful when the end product looks like the original one but with changes that are not easily identifiable but deeply can cause issues to the functionality of it. A substitution attack could be performed in all the levels that complete a product whether it is the hardware, software or firmware. Despite the aggressiveness of such attacks, the anomalous alteration of software in the supply chain is associated to specific patterns that give it away and can be identified by the security personnel and prevent the possible damage it can cause to the organization. Other ways of countering supply chain attacks are not necessarily cheap as the vis-à-vis hardware attacks can be really difficult and expensive to mitigate. The attack pattern of Substitution threats is the below.

   (a) Malicious Hardware

   (b) Malicious Firmware

   (c) Malicious Software

2. **Malicious Insertion**

   Attackers in this type of threats try to infiltrate the supply chain’s system and insert malicious software or entity, in general, without the approval of the administrators of the systems. These threats almost always end up on weakening the security mechanisms of the supply chain systems or components. Malicious Insertion must not be confused with the previously mentioned Substitution as on the first, a new part, software or component is added while in the second, changes to already existing components are performed by the adversaries. The typical attack pattern of malicious insertion is the following.

   (a) Counterfeit Hardware

   (b) Malware

(c) Malicious Software

3. **Alteration**

   This category of threats covers a huge list of them, and this is why is stands last in the list since they are not very specific at all times. The aim of such attacks is to perform a state change on the target system that comes in contrast to the security and reliability of the systems of the organization. Alterations focus on changes that have to do with the current regulations and laws that the organization is compliant with and making it non-compliant. As alteration attacks do not have an aim on gaining unauthorized access or manipulating information, the result of them could be confusing to the organization and therefore of higher severity. Hence their number and their effect on supply chain systems, alteration threats and attacks are hard to mitigate. Their particular attack pattern is listed below.

   (a) Insecure State

   (b) Cyber Espionage

   (c) Performance Degradation

   (d) Non-Compliance

2.2.2 Vulnerability

When creating or making something concrete, like a car for instance, it is obvious and in the expected negatives of it, that some parts may not be fully completed. There might be some mistakes, some flaws or even some malfunctions in the designing process that remain open even after the release of the product. These are called vulnerabilities. And like in everything else, in the cyber world too, all the systems that have been designed throughout the years, have some of them. Despite the huge effort of the engineers to patch them by introducing new supplementary systems or launching minor fixes, not all can be covered. Those cyber vulnerabilities, allow the attackers to perform their actions and possibly cause damage to the target. The total number of vulnerabilities cannot be measured as it is increasing daily and is also changing.

In addition, vulnerabilities can be created in a later time. This might happen due to improper use of the system or factors that at an instance can cause damage, like a natural disaster. The result of a tornado could be the exposure of the protective fence that surrounds a company's premises. This will create a gap that an intruder can use to infiltrate and perform any malicious actions against the company.

2.2.3 Asset

Each corporation has to defend its values, equipment or any other object that belongs to it. By the term asset in cybersecurity, we are referring to any valuable item that the organization is using to perform its daily actions. It can range from something tangible like the hardware equipment (e.g., servers, switches, routers, computers) or intangible like information the organization has in its possession (e.g., data, patents, intellectual property). The assets of a company are one of the most important objects that an attacker can steal or alter.

Therefore, it is very important for every organization to determine and categorize its assets. For some, the electronic equipment could be of higher priority than data in it. A component manufacturing company would be more harmed if the machines that operate and craft the components are damaged, while a bank would be concerned about the financial amounts that are stored in its deposits. Different priorities, means that the Security Framework each company is using, must be tailor made explicitly for them. There cannot be one particular Framework that can cover everything.

Like everywhere else, in this dissertation too, the assets that a public administration has, would influence the way of designing the suggested Security Framework.

2.2.4 Threat Actor

Behind every major or not cyber-attack, there is someone or something that creates it and if successful, manipulates the content of the actions. Like in a normal bank robbery, there are the thieves, people who illegally perform actions that have as only intention to steal money they do not own. Same way, in the cyber world, there are individuals or groups of few people or much larger teams that act the same way as the thieves in a bank. They are called threat actors. People who pose a significant threat to others. As years pass, those actors belong more and more intelligent, skillful, and evasive. They learn well how the target system operates and master the art of manipulation.

In the years of the unexpected coronavirus disease (COVID-19), many changes happened to the cyber threat landscape. In detail, ENISA, posts almost annually the Threat Landscape Report that among others, consists of the most common threat actors. The list of potential threat actors is impressively large and includes categories such as insider actors that are acting from inside the organizations. For year 2021, the cybersecurity threat actors that are considered the most harmful by ENISA are, the State-sponsored actors, the Cybercriminals, the Hacker-for-hire actors, and the Hacktivists all of which benefit from the pandemic and increase their chances of success. But what are all those and what are their motives?

2.2.4.1 State-sponsored actors[13]

The acquisition of sensitive information is of interest to nations as well. They are people who have granted the "License to Hack" by entire countries. They are employed by the governments to target other governments, organizations or even individuals and collect valuable for them data. Comparable to espionage that was especially common at the years of Cold War. They know exactly who they work for and are almost covered by them, so their motives seem harmless and since they act from their own country, they have nothing to be feared of, such as being arrested. Their patriotic believes and nationalistic attitude, make them the perfect candidate for this job.

2.2.4.2 Cybercriminals[14]

As we all are familiar with the Internet, there are parts of it that remains underground, and dark. The so-called Dark Web. Like the Internet, there must be people who "work" on it but on the malicious way. The Cybercriminals are known to access this deep web structure and trade malicious items and services such as hacking equipment of stolen patents and personal data and make profit out of it. They can pretend to be selling legal items but, they are managing to channel to the world their malicious tools and target unsuspecting individuals. The hunt of them is a very difficult job, as the law enforcement agencies that are after them need to adapt to their movements and change their approach according to them. The Cybercriminals' motives are only to make profit without caring about the result of their actions while their targets are not small groups but big entities. In contrast to the common threat actors, cybercriminals have no pattern on their actions and quite hard to counter and predict. Their target determines the way of their approach and their victims feed their actions.

2.2.4.3 Hacker-for-hire[15]

Especially in the era of COVID-19, where new trends around cybercrime arise, there is a highly aggressive and very difficult to defend threat actor group that benefits from offensive espionage. The so-called hacker-for-hire companies is a relatively new trend that offers other companies, groups, and individuals the specific capabilities that allow them to enter the target's system by developing and using malwares, payloads and command and control technics. These companies, like every other, are operating legally in the country of their target and remain untraceable thanks to the use of tools that are not very sophisticated. Their motives are solely the amount of money they are charging their clients for the particular services. Unlike other threat actors that follow standard patterns in their approach, the hacker-for-hire companies are difficult to predict due to their nature. The approach they take for every task, resembles exactly what the clients wants and in most of the cases, as they act as proxies meaning that they are authorized to act on behalf of someone else, they target cannot identify their sponsors or their objectives.

2.2.4.4 Hacktivists

Have you even heard or seen online or in the news, the group called "Anonymous"? It is perhaps the most iconic group that performs hacking actions that focuses on DDoS (Distributed Denial of Service) attacks with targets like political faces, governments, or religious groups. Like all the other hacktivist groups that operate in the cyberworld, they are using old-school methods such as the DDoS, release of sensitive data and account takeovers, and this is the reason why their numbers are decreasing through the years and their impact is minimizing. They act individually and target groups they believe are altering the proper way of things or are corrupt. In their eyes their actions are for the good of humanity, but this does not mean they are acting in a legal way. In addition to that, companies have become more conscious and protective on the way of sharing data in their platforms and as a result, this made the job of hacktivists even more difficult as they were expecting to find more open doors in systems during the pandemic. The lack of sophistications in their actions is definitely considerable but their existence is still visible. Even though hacktivists are not very common, cybersecurity frameworks, still take them into consideration when implementing a defensive mechanism.

2.3 What is a Security Framework?

Have you ever seen a money transfer truck making the delivery? Can we identify the amount of defensive equipment the security personnel are carrying? How many lines of confirmation they follow to make the transfer? All those are similar to a cybersecurity framework companies use. It is the very essential combination of standards, guidelines, applications, and options a company has in its disposal to be able to manage risks that appear in the Internet world everyone is depending on. They are key elements that know well enough the company's structure in order to have the appropriate counter measure for almost any occurrence. Almost, because as we already know we cannot be completely covered since the unknown is our worst enemy and similar to companies an unknow new threat is the worst threat.

Not only a framework, will be aware of the existence of all those elements, but it will also organize them so each one will be assigned to specific role in the case of an attack. Each framework is designed to assist the roles of the humans, and not to perform the actions themselves. They are guidelines on how to react to different scenarios. They offer a reliable, methodic, and accurate way to counter an attack no matter how composite the environment is.

2.3.1 Cybersecurity Legislation

In most of the cases, cybersecurity frameworks are mandatory, or strongly recommended since the compliance with laws and regulations, is forcing companies, to align their protective mechanisms according to the state and international regulations. Of no excuse stands the NIS Directive (EU) 2016/1148[16] which is the first European legislation that is accepted from all European countries for the protection of all the information systems and their network infrastructure in the EU. Given the continuously increasing number of incidents that are focusing on altering the services, functions, and general normality of the operations of the European organizations, it has become of high importance the application of a horizontal legislation, meaning that it applies to everyone without exception, for the common good and the boost of the continuous growth of entity of the member states. As a result, companies are forced to invest in their cybersecurity protection which includes experienced personnel and frameworks.

In detail, NIS which stands for Network and Information System is a well-organized and thoroughly planned directive that was under negotiation for more than 3 years. It is the first ever EU-wide legislation on cybersecurity and entered into force in 2016. The implementation of such legislation was a major milestone in the cybersecurity world as it signified the first time a common approach was agreed between the countries of the Union. The NIS directive is the primary component of the European cybersecurity architecture for the protection of its systems. It provides guidance to member states, so they all follow a common route of security and as years pass even countries outside EU try to accept it. Among others, it defines obligations for all member states to follow that are also behind the security frameworks they use. As another very important role of the Nis directive, we have the creation of national and European Cyber Security Incident Response Teams (CSIRTs). According to ENISA and their publicly available information, Greece has 7 CSIRTs[17], out of which only 2 have Governmental usability.

Of no surprise came in 16 December 2020 the new proposal from the Commission about new cybersecurity policy initiatives. They included as a recommendation to all the EU member states, the development or application of a Cybersecurity framework in order to achieve among others, exchange of information with the other member states. This way ENISA became the EU cybersecurity agency that is now collection the information from all countries under NIS Directive, provides support to member states, and assists in the implementation of it to European institutions and businesses.

Furthermore, in order to increase the operational cooperation within EU, comes a new act that strengthens ENISA and designs a cybersecurity certification framework for products and services, the EU Cybersecurity ACT.[18] Even though the cybersecurity frameworks do not deal with products or services, they are collaborating with the above-mentioned Act so as to handle cybersecurity incidents that happened within the European security network.

2.3.2 Types of Cybersecurity Frameworks

Choosing the right security framework for our organizations is not as easy as it sounds. It is not like picking a car that we base on our budget or our likings. People must consider it as an extremely strong tool that will assist us and be there in case of difficulty. The framework of our choice will benefit our daily work on the security part of it. Not only that but will be then more recognizable in the field of our expertise. We will prove that our work is professional and robust. On the web we can find mainly three types of security frameworks. The control frameworks, the program frameworks, and the risk frameworks. All those types perform more or less the same functions, but they specifically adjust to the company's profile they are chosen for.

- Like in the society, we have types of fuel for the vehicles, such as petrol, diesel, natural gas, ethanol etc., in frameworks, we have controls. They are the different kind of severities on risk that frameworks developing teams have taken into consideration. If for instance someone owns a diesel running car, they will pick diesel as fuel and not petrol. Similarly in security, if we are facing environmental threats, we will pick a different security control than if we were facing legal threats. This is how Control Security Frameworks work, by having different controls in their disposal, and assigning the correct one to the correct area of involvement of the company. A very well-acknowledged control framework is the NIST 800-53[19] which has categorized controls into low, moderate, and high referring to the severity of the impact they are used for.
- Another type of security frameworks is the Program Security Frameworks that unlike control ones, they focus on the proper way of dealing with threats, starting from before entering the organization and ending with the aftermath of it and how to deal with it. Taking from example the proper way of driving a car, someone can say that I will only use reverse gear and still reach my destination. It is not about being legal or efficient but achieving the goal. Unlike that, a program security framework like the NIST Cybersecurity Framework (CSF) can show the proper way of driving. First starting with the ignition and the first gear and ending with shutting down the engine and park. This is how this type of frameworks work and as we will see later in paragraph 2.4.2 and 3.1, we need to have a correct approach rather than just having an approach.
- What happens when we drive a car and suddenly, we are unable to move? A possible scenario is that we run out of fuel because we did not check the fuel tank and we did not calculate that option. Like so, Risk Security Frameworks, are planned so they can identify that we are running low on fuel and focus on finding the closest gas station. They prioritize the risks that might appear in the organization they are used for and find a solution to those risks first before other. If they identify a leak of information from a specific account in accounting department, they will focus stopping it rather than dealing with a tornado that is

about to hit the relevant location area of the premises. Examples of such frameworks are NIST RMF[20] or ISO 27005[21].

2.4 Threat Taxonomy

When dealing with threats, there are numerous differentiation that define them. There are perspectives and dimensions that make on threat different than some other. But they all start with a small question: Is this malicious? For the ease of this clarification, big organizations have spent enough resources to suggest a proper way of understanding each threat which they called threat taxonomy.

The non-stopping development of IT systems all around the fields of processes and information, has assisted in the introduction of many weaknesses. Like in real life, it is in the nature of someone to envy what is not his, similarly in the Internet world, there are entities that put a lot of effort in trying to steal valuable assets from others. State-sponsored actors, cybercriminals, hackers-for-hire, and hacktivists are threat actors we have already talked about in Paragraph 2.2.4, that are only few that complete this list. They attack the systems and try to achieve their goals in different ways. Since this is not a new issue, many organizations need to have a common understanding with others when dealing with cyber threats. For that they have adopted the Cyber Threat Intelligence (CTI), a way of sharing information with other organizations, more of which we are explaining in Paragraph 2.5.

However, as the defense around cyber threats increase, so do the threats themselves. Threat actors are adapting to the situation and become more advanced, but we should not forget that the source of the IT threats all around the world is not only made by humans, but it can also be accidental, environmental, or political. For that it comes to the leading personnel of each organization to assess the possibility of the occurrence of a threat event. Therefore, they can use the specific categorization other risk management professionals have created, in benefiting to the common understanding around cyber threats. That is no other than the threat taxonomy.

Each taxonomy has its own hierarchy and levels, providing additional terms and details. In addition, there are definitions and categories so the decision makers in the organization, can select a particular cause of action to deal with the threat. A threat taxonomy can improve that communication between the decision makers of the organization and the threat taxonomy is two ways. First, the communicating threat language and second, the order of the taxonomy structure the organization will use. Threat language is the terminology around the threat landscape that help organizations communicate with the same terms in the case of failure in a system of at a data breach. Taxonomy structure is the analysis and assessment in multiple aggregations in the overall threat landscape which means that the correct categorization of the threat will lead to the correct choice of course of actions.

2.4.1 Complete Threat Taxonomies

A taxonomy is like the cars. It is ordered like the car manufacturer Mazda, as Mazda 1, Mazda 2 etc., and classified as small, sedan, SUV etc. In the taxonomy there are tiers similar to groupings which have "parents and children", meaning that some are supervising others. Each threat taxonomy is using different terms for its categorization but in the end, they all serve the same purpose. In the top levels of the taxonomies, we might see terms such as top-tier or high-level, while on lower tiers of them, terms such as family or subclass.

Many teams have developed their own threat taxonomy that is applicable to the IT systems and organizations can adopt them. The taxonomy itself will not be enough, hence some work is needed by the responsible personnel of the organization. Without any human intervention, the organization will only have a categorization of the threat events and for that, they require activities from both human and environmental sources. This is why, subcategories need to be included in the taxonomy which will add more detail. The professionals who will be working with the particular taxonomy must be aware of the definitions of all the threat categories since they will prove a valuable part of the unity of the team. For this reason, the threat taxonomies are designed mainly for organizations with threat intelligence capabilities that can provide estimations of how probable a threat is about to happen. Having that said, let's take a closer look at some of the threat taxonomies organizations can choose from.

Open Threat Taxonomy (OTT)[22]

OTT started as a shared and complete set of information system threats that exist in the Internet world and may affect organizations worldwide. The first version of OTT was released in October of 2015 as an open-source tool from the company Enclave Security. The owners and authors of OTT believe that one can understand more about the threat from the components it consists of. And for that, OTT is designed to lay down the components of a threat as agent, threat action, threat target, and threat consequence. Also, in the structure of the OTT we can see a ranking system of threats based on their actions. This ranking system will prioritize threats based on their rank and focus them first.

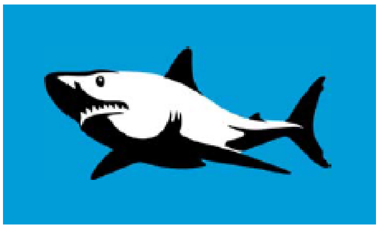


Figure 2: Open Threat Taxonomy logo

The Open Threat Taxonomy includes in its categories of threats the most common and widely acceptable ones without leaving behind non-technical dangers. The categorization is made based on the nature of the threat and by how much they influence the CIA Triad of the information systems. The taxonomy has four main categories of threat with a total of 75 threat actions. Out of those actions, only six are ranked with the highest possible threat rating of 5.0 and 16 with rating of 4.0. Some of those threat actions and their category can be found in the table below. Note that the rating in the OTT is subjective and therefore could be different from organization to organization.

Threat Category	**Threat ID**	**Threat Action Name**	**Threat Rating**
Physical Threats	PHY-001	Loss of Property	5.0
Physical Threats	PHY-002	Theft of Property	5.0
Resource Threats	RES-004	Disruption of Electrical Resources	4.0
Resource Threats	RES-006	Disruption of Communications Services	4.0
Personnel Threats	PER-001	Personnel Labor / Skills Shortage	5.0
Technical Threats	TEC-013	Escalation of Privilege	5.0
Technical Threats	TEC-022	Maintaining System Persistence	5.0

Technical Threats	TEC-031	Application Exploitation via Input Manipulation	5.0

As we can see, OTT covers a lot of information systems threats that can be valuable to the risk comparison an organization will perform. If the OTT is combined with a risk assessment framework, the organization explain what threat it is facing and at the same time understand how harmful it can be.

ENISA Threat Taxonomy

Only few months later than the release of the first OTT, in January 2016, the European Union Agency for Network and Information Security (ENISA) published their first threat taxonomy. The ENISA Threat Taxonomy (ETT) is dealing with threats in a different way compared to OTT. ETT keeps a more neutral posture of providing details for the threats with less consistency and more blurriness unlike other taxonomies. In total, ETT has included in their taxonomy 75 threat actions, a number same as of that of OTT but with alterations. They classify the threats in levels with the high-level ones being the most dangerous to organizations.

With deep emphasis in the details of each threat included in the taxonomy, the ETT is agreed to be one of the most detailed ones in the Internet world. It includes features such as details of how the threats are implemented, description of them, their trend compared to previous years (stable, increasing, decreasing), or if they are included in previous lists of ENISA. The high-level categories of ETT are eight in number and in some version of ETT nine. From the number of categories itself, we can understand the detail in this taxonomy and thanks to that, we can relate with higher detail to one of them in case our organization is a victim of a cyber-attack. One very important part of the ETT is the addition of the Legal category of threats which means that ENISA in not neglecting the General Data Protection Regulation (GDPR)[23], despite the fact that the GDPR came to implementation almost two years later than the first version of ETT, in May 2018. Having a category that deals with the legal threats, can be considered a milestone in accepting an organization as serious and law abiding.

From the 75 in total threats included in the ETT, only 8 have a trend of “Increasing” which means two things. First, organizations have finally realized how important is to have a means of protection against malicious actors. And second, the global effort in countering threats and attacks has been more experienced by either the resources used to that cause or by understanding more and more the structure of the existing attacks. If we now compare that report of 2016 with the threat landscape ENISA published in 2021, we will be able to compare the findings and conclude if the estimation of 2016 was correct.

Just as a reminder, the ENISA threat landscape of 2021 reported as prime threats, meaning that they are the most important ones, the Ransomware, Malware, Cryptojacking, E-mail related threats, Threats against data, Threats against availability and integrity, Disinformation - misinformation, non-malicious threats, and Supply-chain attacks. While if we examine further the estimation of ETT of 2016, we will see some differences in the predictions made around the threats. In order to properly understand these differences, one must take a close look into both the ETT and the landscape.

For instance, in the category of “Nefarious Activity/ Abuse” of the ETT 2016, we will see some extensive attention placed in threats that have to do with “Malicious code/ software/ activity”. This kind of threats are very dangerous to organizations and can cause serious damage on the infrastructure of it. Attacks such as “Exploitation of fake trust using social media” can manipulate data found in the organization but if we compare to what 2021 ENISA suggested, we will see few to none references on similar attacks which means that either the security of software has increased and this way people do not fall into the trap of the social media, or preferably, the personnel has been trained enough to deal with such cases.

As we can see, there is an extreme amount of information that ENISA has been collecting from sources all over the world while tries to benefit the organizations realize at which extend their premises and resources are in danger. The previous example was only one of the threats that shake the world daily and according to the ETT their increase in numbers, or severity and aggressiveness might alter the threat landscape to the core. Having that said, if an organization wants to investigate into the security protective mechanisms, it can study the ETT as it is a highly valuable taxonomy.

Sum-up of Threat Taxonomies

As more and more threats were emerging to the surface into the Internet world, the need for threat taxonomies emerged too. There are plenty of different threat taxonomies published that support different roles. Others are created for adversarial threats, others for intelligence sharing, and others for more human-centric roles. One thing is for sure; there is not only one available taxonomy that is perfect for every kind of organization. For the organization to benefit from a taxonomy it has two options, with one being more costly than the other. The first is to spend resources, time and effort on creating its own threat taxonomy that categorizes completely all the possible and previous threats that occurred or will occur against its infrastructure and systems. And the second, which is by far the easiest and fastest to implement, is to adopt one of the already existing threat taxonomies. But even though the cost of the second is very low, the organization should keep in mind that no specification was made when the particular taxonomy was published, meaning that some micro-managing edits to the taxonomy need to be performed so it covers the organization's needs at a big percentage.

Without analyzing more into the subject of threat taxonomies, we need to point out that when an organization feels the need to benefit from a taxonomy, there are plenty of different ones out there that will be of good use for them. Never forget that each threat and each organization is far more divergent than others. Each one has its own character and point of view so it can identify as unique.

2.5 Cyber Threat Intelligence (CTI)

Almost every threat that has caused damage to organizations, either directly or indirectly, has been recorded and its details have been included in its spot on the Threat Intelligence storage. Given the increase in number and variety of cyber-attacks and malwares the job of forensic investigators and security analysts, has become much harder through the years. Now using the CTI, cyber security personnel, has immediate access to the collected data and can create counter measures to incidents that consist of already known attacks with higher speed and better efficiency.

2.5.1 Cyber Threat Intelligence origin

Every company has access to the Internet in order to perform its daily operations, but at the same time, it becomes exposed to possible threats. For that, there must be a continuous defensive mechanism for at least identifying the threat and knowing how to react over it. Those threats do not just happen once, but if the company is in the target area of the malicious actors, there is a possibility of multiple future attacks. The attackers are very keen on achieving their goal which is to infiltrate into the target's system and manipulate any assets they find. This signifies the origin of the data collected by any CTI[24].

2.5.1.1 Internal

If the internal IPS of the company manages to include in its report the threat, then internal data are collected and are included in the CTI of the particular attack. This intelligence is not easily visible to analysts but may assist in identifying some other attack. Information like IP addresses, domain names and ports are shared through this source.

2.5.1.2 Community

“There is power in numbers and there is power in unity”, as Dr. Martin Luther King, Jr. said and explains perfectly what the second CTI source of data is all about. Not all companies are attacked the same way, and for that, there exists a category that includes CTI that is shared between organizations that either share the same interests in some field or belong to the same group of organizations. There are community groups that take actions in cooperation to each other when facing attacks.

2.5.1.3 External

This category includes both public and private CTI collected from areas that do not exist inside the organization or inside the community group. They can be feeds that are available for no cost that are called public and can be feeds that in order to acquire them a specific fee must be submitted. Both have their pros, and their cons. Public external CTI are free but how can do not guarantee data integrity and quality and private external CTI offer levels of data quality but are only available after subscription.

2.5.2 Cyber Threat Intelligence approach

In order to acquire data that feed the list of information around a threat and in extend an attacker, specific tools must be used[25]. Examples of tools are the Traffic Light Protocol (TLP), the Managed Incident Lightweight Exchange (MILE) and the Open Indicators of Compromise (OpenIOC) framework. These tools are immediately connected to types of threat intelligence. Some focus on information selection, some in knowledge analysis and others in intelligence utilization. Based on their actions, they are split into 4 types explained briefly below.

2.5.2.1 Strategic Threat Intelligence

Strategic intelligence focuses on the who and why of the threat. It provides information on how to treat attacks by answering those questions. If we manage to identify who performed the attack and what their motives were, we will easily manage to find clues around the future of their operations and their approach. What their intentions are, and our organization is within their scope of attack. This intelligence has long-term use and is considered high level as the collected info is used by high-level personnel such as IT managers and CISOs. Examples of information we find using this type of CTI are the possible trends of threat actors or statistics that refer to similar attacks on the global grand total.

2.5.2.2 Tactical Threat Intelligence

Tactical intelligence focuses on the what of the threat. It holds information about the Tactics, Techniques, and Procedures (TTPs) of the attack. It assists the personnel to how the attacker is expected to perform a future attack and distinguish what kind of information is most likely about to be leaked. With tactical intelligence, we understand more about the technical expertise and goals of the attackers while also the attack vectors. This intelligence has long-term use and is considered to be low level as the collected info is used by cyber security professionals such as IT service managers or network operations center (NOC) employees. Examples of information we find using this type of CTI are targeted industries, geographical areas of operations and the major TTPs of the attackers.

2.5.2.3 Operational Threat Intelligence

Operational intelligence focuses on the how and where of the threat. It offers information about the context of the attacks like previous malicious activities insight in the methodology of the attack of potential risks. It has to do about incoming attacks to the organization that have been identified in the past. This type of intelligence has short-term use and is high level as it is used by security managers, security forensics personnel of fraud detection groups. The collections of such data are originating mainly from social media and real-world social activities that include many people. The analysis of human behavior or the actions of threat teams feed this intelligence. Examples of information of this type of intelligence are Obfuscation Tactics, Incident Response or Vulnerability Management.

2.5.2.4 Technical Threat Intelligence

Technical intelligence is the basis of analyzing incidents of attacks. It provides information around the indicators of attacks of the proof of them. When trying to find suck information, analysts must take close look to Indicators of Compromise (IOCs), command and control channels and other similar tools. This type of intelligence has short-term use and is considered to be low level as it is used by SOC personnel and Incident Response teams. They particularly break down, suspicious phishing email content and addresses, malwares or reported URLs. It is of high importance for technical intelligence analysts to collect data at the correct time. If they miss some content of a bogus URL, the higher-level analysts such those of operational intelligence might not be able to identify the incoming attack. Examples of this type of intelligence are domains used by malicious endpoints and hash checksum.

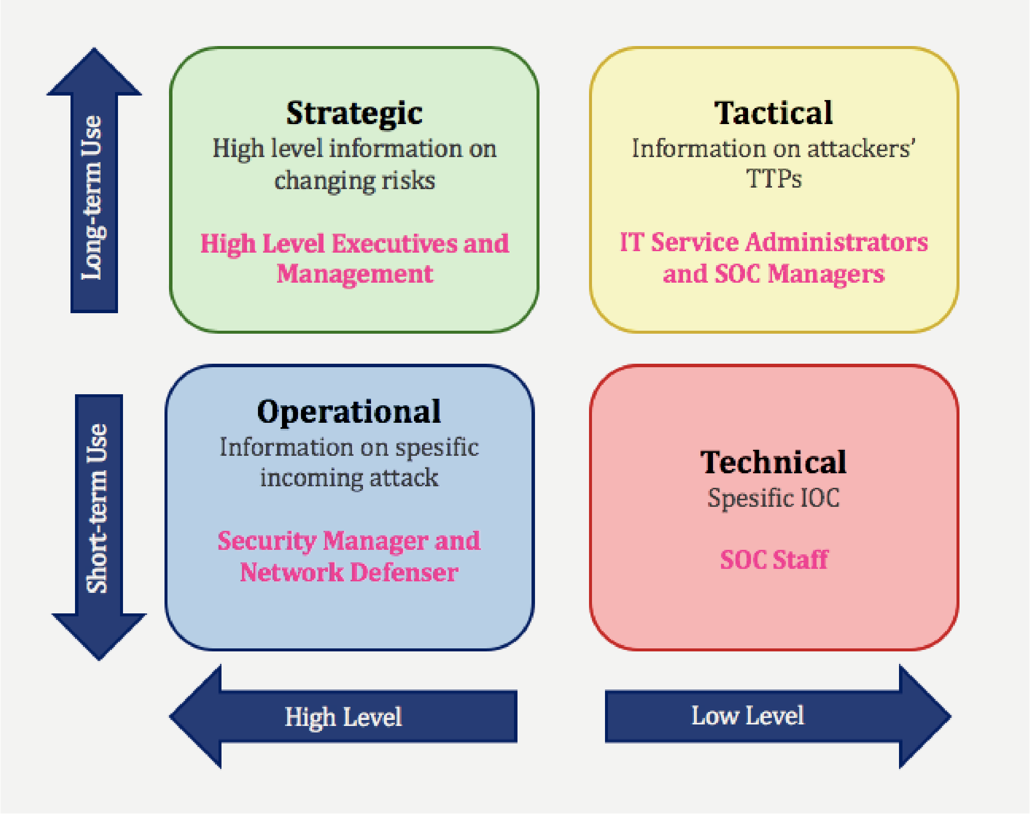

Long-term Use
Strategic
High level information on changing risks
High Level Executives and Management
Tactical
Information on attackers' TTPs
IT Service Administrators and SOC Managers
Short-term Use
Operational
Information on spesific incoming attack
Security Manager and Network Defenser
Technical
Spesific IOC
SOC Staff
High Level
Low Level

Figure 3: Comparison of 4 types of Cyber Threat Intelligence

2.6 Current state of Security Frameworks

As of now, there are plenty of security frameworks and that for, the choice of the best one exists. But organizations need to understand that it is not about picking the best framework, but it is making the choice of that suits my company best. And this is how there will be higher possibility to face the upcoming threats.

2.6.1 ISO/IEC 27005

One of the most recognized and up-to-date information security risk management standard family that belongs to the third type of security frameworks we previously mentioned, are the ISO 27000 series standards. In order to reach its current state, this framework has passed through numerous updates and revisions that as for now, has included all the options an organization can follow to counter possible risks and treat them accordingly. These standards were first published but the International Organization for Standardization (ISO) on the year 2011 and since then they have been accepted by many commercial enterprises, government agencies and non-profit organizations. As we understand risks have no boundaries and can influence any organizational structure.

The referring standards, belong to a family of standards that explain and allow the owner to implement an information security risk assessment, management, and management systems to its organization by offering guidelines, sets of specifications (ISO 27001) and codes of conduct (ISO 27002).

In this family of standards, exists the ISO 27005[26] which focuses on the risk management process which got included in the ISO 27000 family of standards on the year 2018. Differently to other very popular risk management standards this ISO 27005 is flexible enough to allow organizations to select the particular approach of their liking on how to assess the risks they are facing. This is all based on the specific business objective and way of acting. In detail, a six key component procedure is offered as follows.

1. Context establishment
2. Risk assessment
3. Risk treatment
4. Risk acceptance
5. Risk consultation
6. Risk monitoring and review

In order to properly implement this standard, the organization needs to which resources are available, what scope the contribute to and what are their boundaries. Also, an understanding of the critical systems and processes need to be done as long as which assets are supporting the critical systems and processes. Finally, any possible constraint to the organization will influence the outcome of the standard and this is why the organization need to evaluate those too. All those can be described in one scheme as below:

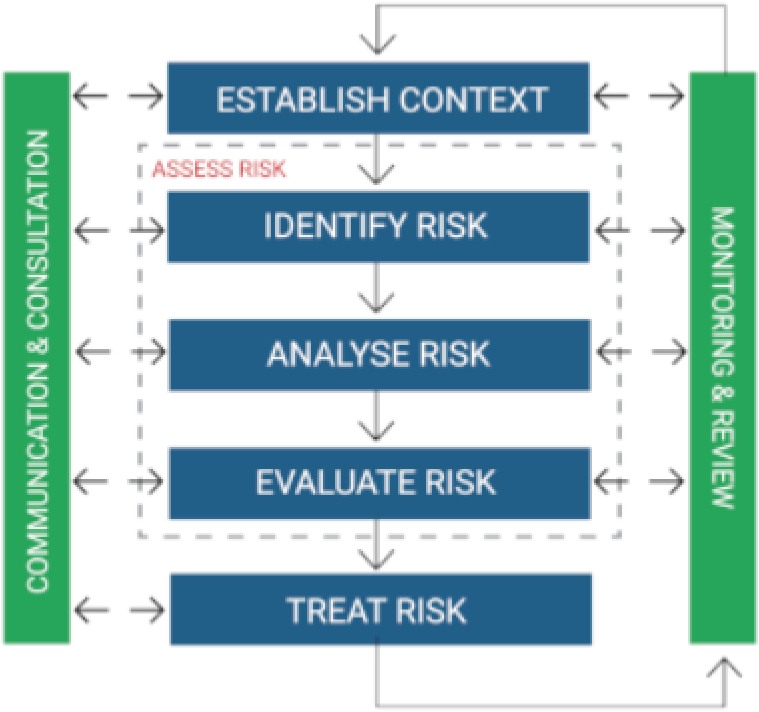


Figure 4: ISO 27005

The very first step of the implementation of ISO 27005 is that the organization sets the appropriate criteria and terms of how they identify the risks, the responsibility for them, the impact they will have to the CIA triad of the information of the organization and how the calculation of the risk impact and likelihood. This step is outside of the boundaries of the actual risk assessment, but it does not mean it is not necessary. On the other hand, it resembles the core of the structure of the standard.

On the second step, the organization must make some calculation in order to identify which threat is applicable to each asset for which information has been compiled in advance. Then from the impact and likelihood calculation of the first step, the resulted values need to be assigned to the assets. An evaluation of each risk is following but in cooperation to the predetermined acceptability levels of the organization in order to conclude with the prioritizing of the acknowledges risks.

In the middle of the total process, come the treatment of the risks, which procedure can be performed with four different ways. Some of which might be linked to each other. The easiest way is to completely avoid the risk by eliminating it. Some other way is to modify the risk, but in this case, another standard needs to be applied to the organization

(ISO 27002) that will apply specific security controls. If the organization does not have the required means to perform the first two ways, there is the option to share the risk with a third-party authority that will deal with it and send back the results. And last but not least, If the risk is withing the acceptance criteria that the organization has already set, then it can be retained.

For an organization to proceed to the fourth step, it must first define and therefore follow the acceptance criteria that are considered when dealing with a risk. Here, policies, goals and shareholder interests are considered and contribute to the implementation of the standard.

Dealing with a risk is not an easy task. Those who are certified and experienced in such actions, need to take many things into consideration such as the interests of the stakeholders of the organization. This communications between them, must be a continuous process that is been done prior and after dealing with a risk. It consists of the fifth step of the implementation of the standard and stands at a crucial point in emergency situations where a specific plan tailored to one risk has been agreed.

Having done all the previous steps is not enough to guarantee that the organization is safe from the risks. After the first five steps, a recap needs to be performed. Since it is in the nature of all the risks to alter at any time without any notice, the organizations need to continually monitor them and keep an eye for any changes on them. A proper risk monitoring completes the implementation of the standard with also includes new threats to the organization, and data received from other sources about new risks.

2.6.2 NIST Cybersecurity Framework (CSF)

In the top of the list of the world’s best security frameworks, stands the very well-known and strong framework of NIST[27]. This is a framework capable of improving the critical infrastructure of cybersecurity with aiming in increasing the organization’s readiness when dealing with cybersecurity risks by applying standard practices and processes. It is a framework whose structure and application has been the basis of many other frameworks since its robust and comprehensive. NIST CSF, as it is called, has become very flexible throughout many updates leading to a complete guide of cybersecurity activities an organization can use whichever its field of expertise is, from agricultural organizations to even federal ones.

Despite the fact the NIST CSF was originally designed in the U.S. for the U.S. organizations, it is now widely accepted from the entire world. Even entire countries have adopted this cybersecurity framework as it is covering their needs to the maximum. Such countries are Italy, Israel, and Uruguay. This framework is so high-profiled, that even laws were suggesting it. To be exact, during his presidency, President Trump released the Executive Order 13800[28] in May 2017 which was called “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”. This order was almost forcing federal agencies in the U.S. to use this particular framework customed to their needs in order to manage their cybersecurity risk and provide the necessary risk management report to the Secretary of Homeland Security and Secretary of Commerce. The report that the secretaries submitted to their President included findings around the cybersecurity image of the country. In detail, the United States was requested for immediate improvements in its cybersecurity workforce, hired specialized in cybersecurity teachers for the primary and secondary levels, staff for the higher education and training instructors and forced the personnel of non-cybersecurity fields to receive relevant training. This means that every body requires having a guideline on how to react to threats and governmental bodies are no excuse.

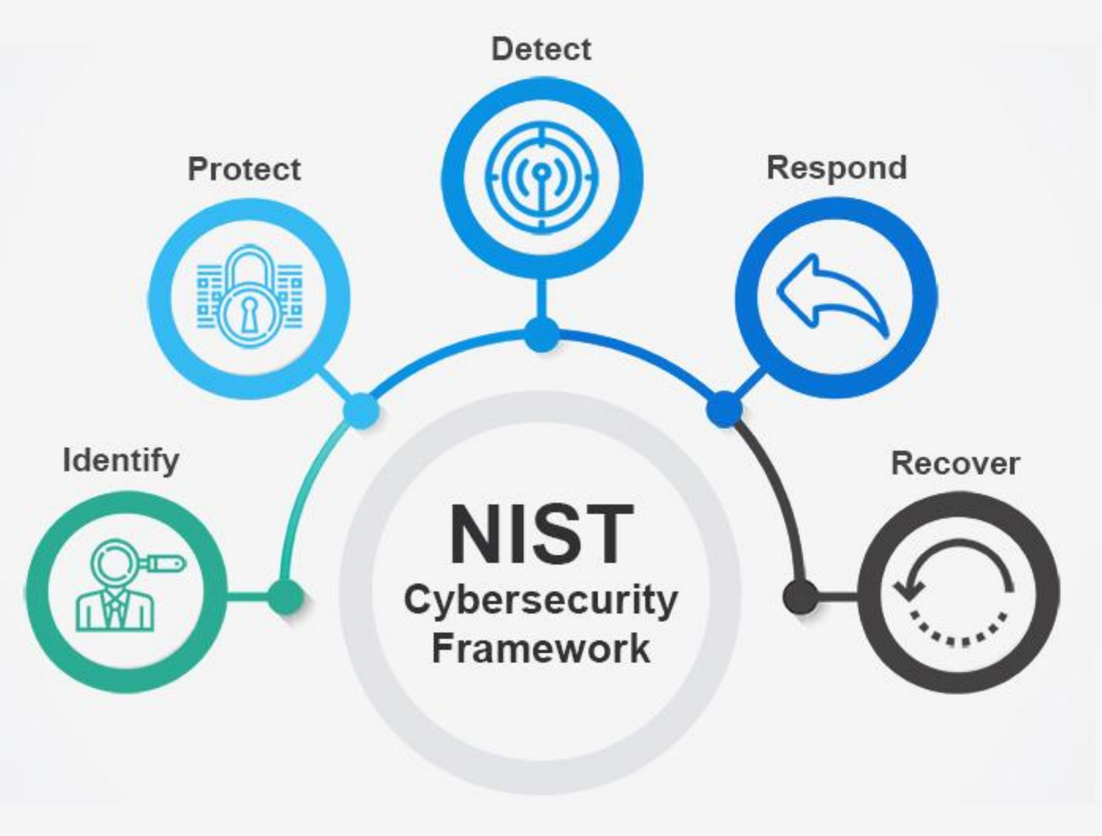


Figure 5: The NIST CSF

NIST stands for National Institute of Standards and Technology of the U.S. Department of Commerce. They designed a framework that is voluntary meaning that in can give to a business an outline of what choices to make in the process of deciding where to focus its time and resources in the case of an emergency cybersecurity event. The structure of it is like other frameworks but this one holds the crown of being the first to implement this specific structure. In particular, the Core of the NIST CSF is based of the five-element principle of Identify, Protect, Detect, Respond and Recover, more of which we will explain in Paragraph 3.2. For every organization the detail of each element differs based on its needs but what remains the same is the categories of the elements. There are in total 23 categories with each having numerous subcategories that, they construct the right approach when dealing with an incident.

The NIST CSF focuses on giving to the organization's personnel an idea of what the upcoming attack looks like, how to react, which decisions to make and what to prioritize. The framework also assists to the learning process of an incident that has become a valuable addition to many organizations all around the world. This way, every incident, harmful or not, trains the victim and contributes to the very precious knowledge list one needs.

At the "depths" of the framework, we have a maturity levels feature or as defined by NIST, implementation tiers. The basic idea behind this process is that the more additions you make to each capability of the framework, the higher the maturity level the specific threat is. The levels are not numbered but labeled meaning exactly what they are starting from Partial, going to Informed, to Repeatable and concluding to Adaptive with the last being the top of the top which guarantees that the program is the best possible. As a very important role in the part between Repeatable and Adaptive levels, play the knowledge shared with other companies for the similar incident, the so-called Cyber Threat Intelligence (CTI).

When talking about how to implement this particular framework, one must take a close look at the Identify element. It is not only the first, but the most important element that will guide the whole process and lead to a successful implementation of the CSF. Here the organization, will realize the existence of the incident, check its details, and coordinate its sequence of actions on how to deal with it and hopefully disable it. Once the Identify element is mastered, then and only then, the organization can proceed to the implementation phase of the Protect and Detect elements.

An organization must never overestimate the program it is been using. It is almost guaranteed that at some point of time in the future some of the enterprise's components and processes will be breached and then we should hope the damage will be small. For that, it is very important to be certain that we will discover the breach and be able to restore the influenced systems back to their original state before the incident happened so in short, properly implement the Identify element.

Overall, it all comes down to how an organization can use this CSF. Before doing that, the organization needs to first look at the history of the cybersecurity issues ever existed or continue to exist nowadays and might be of importance to it. Such issues could be not knowing what risks and vulnerabilities might arise to the surface that are hidden or having a vast number of assets you need to protect but you do not know the way for that. Other could be not having experienced enough personnel to deal with incidents and therefore end up spending serious amount of time and money in chasing items that in the end, have minimal to no impact to the organization instead of focusing on real risks that are harmful. Therefore, an organization needs to have the NIST CSF in its arsenal. It is built in focusing on helping organizations prioritize any cybersecurity-related decisions and helps in putting the organization back to a safe way of existing in the Internet world without the fear of getting trapped in it.

2.6.3 Australian Signals Directorate (ASD) Essential 8

As part of its defensive program against attacks that have to do with the Information Technology field, the Australian government has created a team that is facing the country's cybercrime as its first line of defense. The [29] is aiming in defending Australia from global cyber security threats. The ACSC has, through the years, distinguished 8 essential strategies that can defend targeted attacks with a success rate of 85%. This has come to conclusion of suggesting a baseline security framework that is capable of incidents using a unique approach that corresponds to three maturity levels using the above-mentioned strategies. The Essential 8 is using the maturity levels as indicators of how the organization's risk profile can customize the framework upon its implementation.

The flexibility of the Essential 8 is making it perfect for fitting to the needs of an organization no matter its size. It does not only effect big businesses with thousands of personnel, but also small businesses with just few hundreds of them. Especially when dealing with attacks on targets of small to medium businesses, either they are Hacks with outcome of stealing or selling information, or Impersonation of identity with result in paying the attacker financial amounts, the threat is real and exists. Threat that is capable of causing financial damage to the organization that it will not manage to overcome. Also, in case of an attack there is the possibility of damage in the reputation of the business which might be even more serious than just financials costs. This is why, while implementing the Essential 8 framework inside the organization, the maturity level of it will increase and hopefully lead to a cyber threat awareness which comes with the creation of cyber defensive mechanism.

Figure 6: The Essential 8 logo[30]

The Essential 8 uses a maturity model as a measurement baseline to compare the organizations maturity against each of the 8 controls. With 3 maturity levels, the organization will eventually go from the 1st level to the 3rd, meaning that it will start from being the least secure to very secure. By reaching the third level, the organization is now completely aligned with the plan of the mitigation strategy created from the framework. But this alignment does not only need to be performed once, but instead, performed in a frequent basis so as the organization keep its maturity level and not drop out of it which will lead to an open door form an attacker to act. When talking about maturity levels, a very easy example is the frequency of backups with the 1st having them done monthly, the 2nd weekly and the 3rd daily.

The 8 strategies within the implementation of the framework are categorized into three categories for a better classification and understanding. Some strategies or controls could be placed in other some category too such as the Multi Factor Authentication that is belonging to the category of Limiting the Extent of the Attacks could also be part of the category of Preventing Attacks due to its nature. For a better understanding of the categories, we should first briefly explain them.

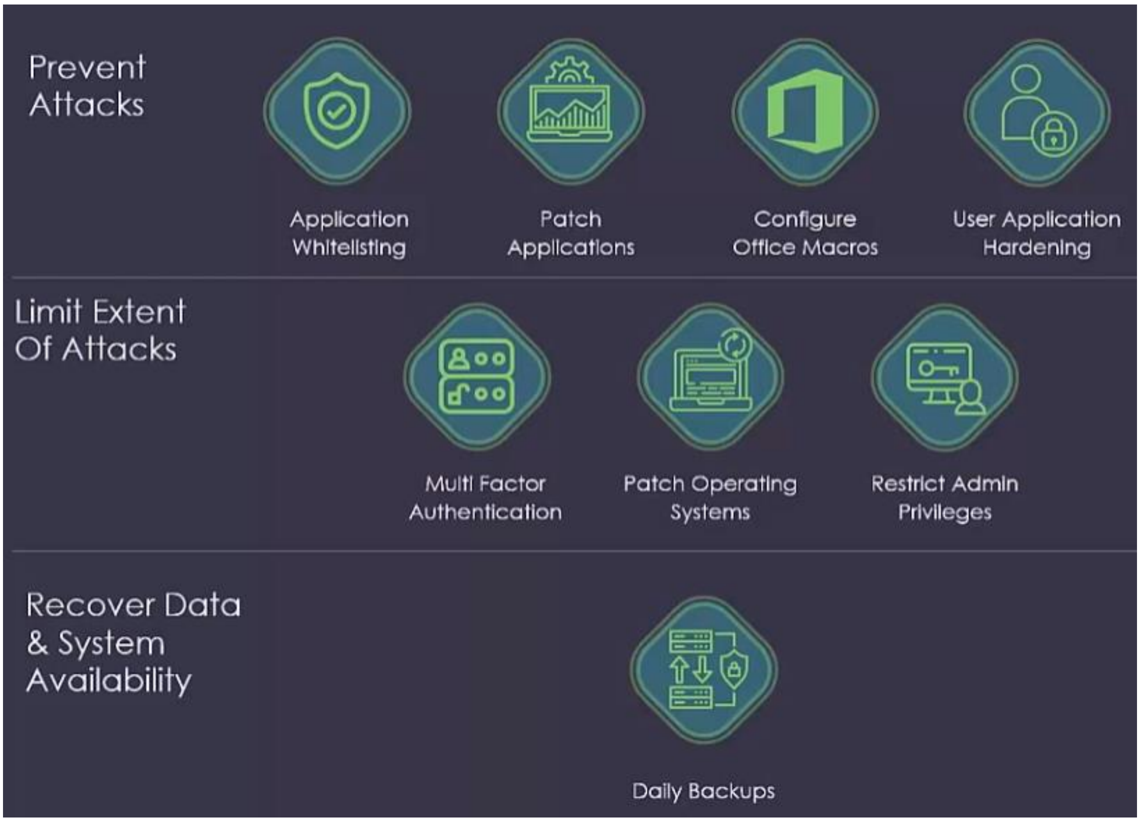


Figure 7: The Essential 8 strategies into categories[30]

The first category of strategies is the one that deals with the Prevention of Attacks by either fixing software and updating them or by increasing the user application. In this category we have Application Whitelisting that in few words, gives the permission to applications to be approved or trusted so as to run on computers. It is like giving the driving license to someone before he is able to drive a car. In the IT worlds, it refers to the actions an IT administrator performs to software such as the allowing the use of Microsoft Outlook or Microsoft Excel, or whitelisting them, and everything else blacklisting meaning that no user is allowed to use them. This way an organization can decrease the chances of malware, ransomware, and viruses to be inserted into the system.

Another strategy in the first category is the implementation of Patching of the Applications. In common words, apply the updates that are released for 3rd party software that is commonly used such as Google Chrome for browsing or Microsoft Office for documents and tables. Given the fact that updates are being released by the developers of the software to cover some “holes” found in the software, when applying them quickly, we decrease the time we give to malicious actors to perform their actions to the specific software.

Moving to the third strategy of the first category, we have the Configuration of Microsoft Office Macros Settings that is there to block macros from running that were included in the Microsoft Office by non-trusted entities. Macros are small amounts of coding strings that are built into documents to allow the user to automate some tasks. But since the macros can hide malicious code in their strings, it becomes very easy for an attacker to insert the malicious code into the system, and therefore a strategy against that is crucial.

Last strategy that can implemented as part of the first category, is the Hardening of User Application. This can be performed by either uninstalling add-ons on browsers or disabling features from web browsers, PDF viewers or Microsoft Office. Think of that an attacker can obfuscate the malicious code into the above-mentioned configurations of applications so the user can accidentally activate them as easy as just launching the application. Also note that the majority of such attacks are coded using the programming language of Java which is also used for creating applications such the ones previously were mentioned.

On the second category of Limiting the Extent of Attacks we have one of the most important strategies that is so easy to be implemented and yet provide a high percentage of security to the organization. This no other that the Multi Factor Authentication (MFA), which can not only stop hackers getting access to our systems, but it can also limit the extent of an attack in case the first stage of the attack is met. MFA is a security mechanism that requires the user to authenticate himself before gaining access to the system. It is an additional piece of evidence, besides the username and password, that makes sure that the user who tries to log into, is the one he is supposed to be. When talking about attacks, and the attacker has managed to find the username and password in order to enter the system, he will come across the MFA mechanism which will make it very hard and maybe impossible, for him to gain access. The nature of the MFAs is based on encrypting algorithms that are for now impossible to crack in specific amount of time. For instance, we have Google Authenticator which is using the HOTP[31] algorithm which uses a shared secret key of at least 128bits of length, that makes it enough so an attacker cannot crack it, with the nowadays known ways.

In addition, the second category hosts the strategy around Patching the Operating Systems. Similar to the Patching of the Applications strategy in the first category, we have the constant update of the operation systems this time such as Windows, MAC, or Android. It can be considered as double strategy as this strategy not only covers patching systems but also keeping up with life cycles. This is one of the hardest strategies for an organization to meet from the framework, as ASCS accepts a level 3 maturity level of an organization in this strategy by having a patching sequence of less than 48 hours. But since the patching versions might not be stable at that time, most of the organizations, do not manage to meet the frequency due to the non-stability of the patches.

Last, on this second category, and organization is requested to perform the strategy of Restricting the Administrator Privileges based on the user duties to the operating systems and the applications. This is a process that is required to be regularly revalidated and decided the need for privileges. Privileges can be taken or given so easily that an organization should think well prior to granting them. Attackers count on the privileges they will find on admin accounts since they usually have the most of them in an organization.

To conclude, we have the category of Recovering Data and System Availability with the only strategy of Daily Backups. In this third category, we have a way of “saving” the organization if the backup is set on time. As maturity levels go up, the frequency of backups is increasing, and thereby a daily backup plan is setting the organization as very mature on this category according to ASCS. In case a cyber security incident occurs, and we have loss of data or unauthorized access to the systems, but with a fresh backup we can restore them and ensure that the malicious actions have been stopped.

After this small introduction into the Essential 8 we can understand how helpful is for an organization to use these guidelines that the ASCS has provided. The cyber-attacks are real, are happening in a very frequent basis and sometimes can cost a lot of money. The maturity level of an organization does not completely determine how secure the organization is against attacks, but it is only an indication of how and where the defensive mechanism can be boosted. Of course, the higher the maturity level on each strategy, the better.

2.6.4 Baseline Cyber Security Controls from the Canadian Center for Cyber Security

Figure 8: The Canadian Center for Cyber Security logo[33]

Following the other famous cybersecurity frameworks, and similarly to the Australian government that implemented their own framework focused mainly for the Australian organizations but also for other country's ones, the Canadian Center for Cyber Security[32], designed their own cybersecurity Framework. It is categorized as a baseline cyber security controls group that is applicable to small and medium size organizations. In the beginning it was destined for organizations within the Canadian borders that having understood the country's laws and regulations, it provides recommendations in order to help to the improvement of the resilience through cyber security applications. This means that organizations that follow these controls, will reach a level of certainty when dealing with cyber threats.

The first release of this framework was made in March of 2019, few months before the outbreak of Covid-19, and without knowing the upcoming situation around the health landscape of the entire world, the Canadian Center of Cybersecurity managed to implement a solution for possible threats that were including also the new trend of cyberattacks that this pandemic gave birth to. The second release occurred few months after the pandemic, in June of 2019, when the framework tried to cooperate with the need for more security around the degree of protection for the companies that started been targeted with covid related attacks. In February of 2020 came the final release, so far, that provided minor updates to the control of the framework and for now has been used by companies.

On the core of the Framework, we have a big list of baseline cyber security controls that aim to provide small and medium size organizations with the appropriate practices when dealing with cyber security incidents. Even though this framework is based on the NIST Cyber Security Framework, it focuses on a different approach that requires a smaller amount of the needed funds to initiate such protective actions, but with the same results. In the end, it all comes to how ready organization is when making such steps, and how aware it is when realizing the severity of the dangers that exist in the Internet world.

Before an organization starts implementing the controls of its choice, there must be a process of understanding of the capabilities of the organization and a calculation phase of which of the controls are suitable for the current business profile of it. For an organization to be eligible, meaning that the controls of the framework will manage to protect it against cyber threats, the size of it should not be exceeding the 500 employees. This does not restrict the use of the framework from larger organizations, but as it is obvious, more employees mean more possible threats, with more weaknesses and therefore more advanced and expensive frameworks should be used. Then the understanding process begins, with the organization selecting its assets and choosing if and how many are needed to be protected, so relevant controls are used. The organizations never secure 100% of their assets since it becomes very difficult to evaluate the equipment used from computer to servers or from mobile phones to company vehicles and tend to be forgetting them or choosing to do so as they are not that important to the it. In addition, the organization must understand the injury degree of any possible attack might result to the systems and assets. For this, a proper assessment for the injury level of compromise of the CIA triad of the organization must be done, so different types of assets are distinguished, categorized, and finally protected. If an asset will be marked with high injury grade, then the potential negative effect of an attack might be very severe and possibly unpredictable and inevitable. Continuing with the initial stages, the organization must understand what kind of sensitive information it possesses and how likely they are to be threatened. Different emphasis is placed if the organization is dealing with sensitive personal information of citizens or any intellectual property. Finally, any organization that is choosing the Canadian Center Baseline Security Framework needs to be prepared so capable and experienced employees undertake security related tasks with a proper plan for improvements and scaling. All the improvements need to be performed in a timely manner that will first be aligned with the budget of the organization and the capabilities of its employees and then with the final goal around the strengthening of the security.

After the Organizational Controls, or in short OC.x.x (each “x” signifies a number), have been considered, then the organization needs to discuss and choose as many of the Baseline Controls it can. The BC.x.x as they are referred inside the framework in short, are spread around 13 different categories, with each having equal importance to the reducing of the possible risks of the organization, but also to provide an appropriate response mechanism to incidents. Of course, the Baseline Controls are designed for an organization to implement them all but since the target group of this framework is that of small and medium size organizations, some can be either implemented in a smaller degree or just left aside; all because of lower budget.

First, the organization must accept the fact that an incident will occur either they want it or not, either they are prepared or not. Therefore, this framework has as first control that of the development of an incident response plan. This can be covered by tools that help in the process of detection, prevention, and mitigation of incoming attacks. But since such tools can be very expensive to both own or assign to outsourced agencies, the best things to do is in first place, have a written plan on every reaction that has to be done. Written plan means also that the organization has responsible persons who will deal with the handling of the incidents by performing actions that cover communication with stakeholders or any affected persons. In addition to that, it is highly recommended to have a cyber security insurance policy suitable for incident response and recovery actions.

Then a series of controls can be applied that benefit the organization on the software security. In more details, it is highly recommended that no software remains out of dated. This means that automatic patching should be enabled or alternatively, develop a management system that controls the patching. In addition, if some software is needed for the processes of the organization but is old and no automatic patching is in place, then administrators should patch the software manually. As another way to strengthen the software security, anti-malware solutions are highly needed that will scan the systems automatically in coordination with an active firewall, in the form of a software, that will protect each device separately.

Users can also be secured using some controls that are inside the Framework. To achieve that, organizations could configure the devices with actions like changing all the default passwords, removing unnecessary features, and activating other security features. Also, two-factor authentication is highly suggested especially for important users that have privileged accounts. Such authentication is not enough and therefore organizations should persist in frequent password changes and have definite policies around the combinations of passwords. All of that are not enough if the personnel are not aware of the dangers of the Internet and for that, the organization must invest in awareness training for the employees, so they are in position to understand how the Internet works and how to use it without compromising the organization they work for.

Backups were always a point where the organizations could return when they experienced any loss of data or alteration in the configuration of the systems. Now it is more important than ever that organizations control their backups to ensure their recovery mechanisms are up and running. One of the strongest ways to protect data in backups is by having them in offline mode at a secure location preferable far from the main area of operations. Furthermore, the frequency of the backups is also very important while also the encryption of the backup itself.

Combining user security and software security, organizations need to take care of the mobility securing process. Mobile devices used by the employees need to have restricted access making them only suitable for work and not for personal use while also be in an encrypted state. There are enterprise mobility management solutions that allow organizations provide visibility, secure access, and data protection to all the devices. Caution needs to be taken when accessing public networks, unknown Wi-Fi networks or when NFC transactions are performed and for that each employee must be in position to control the use of their devices.

On the business aspect of the protection mechanisms an organization can implement using this Framework, stand the perimetric defensive ones. Such are the dedicated firewalls that control the traffic between the corporate network and the outside Internet with focus, if possible, to next-generation firewalls. DNS firewall for the outbound DNS requests to the internet, VPN connectivity and multi-factor authentication for all corporate

IT devices and implementation of DMARC on the organizations email's services are only few of possible enhancements an organization can benefit from.

If the IT services the organization is offering have been altered lately to cloud services, this means that the organization is increasing and follows the standards that will accompany the next years. Having secure cloud services is of high importance while the target surface that is left online becomes bigger for malicious actors to benefit from. To help that, organizations can outsource some of their IT services, but they need to do that with caution. First, they need to evaluate their comfort level and then decide how much access they can give to the outsourcing company or what legal jurisdictions their outsourced partners use and store.

Another very interesting control an organization can use is the regular control and evaluation of rights the users have. The users must have permissions to use the resources of the organization they are requested for and not have more that needed. This means that administrator accounts should be few and only if needed as not majority of the employees needs to have access to administrative activities. Also, if permissions have been given for specific amount of time, the administrators must be aware of the times and retain the privileges when the users have no use for them. Last, if the organization can implement a centralized authorization control system, then one user will have access to all the needed applications or websites with the use of the same credentials from any location.

Finally, organizations need to find a way to prevent unauthorized access to portable devices that are ownership of the organization. Talking about USB flash drives, portable hard drives, or SD cards, we are only talking about easy ways of exfiltrating data out of an organization. For this reason, a way to prevent that, is first to have strong control of who and how uses such devices and second, if these devices are not needed any more, how their destruction process is been done. Of course, locking USB ports on every single computer is an option but a very restricting one.

Having all that said, we can see that the possible implementations of protective mechanisms the Canadian Center of Cyber Security suggests, are many and have different parameters. As previously said, it is in the competence of the organization to choose which control to use. But the more the controls an organization is using, the higher the security it is ensured.

2.6.5 Center for Internet Security Critical Security Controls (CIS)

With one of the most if not the most interesting structure, come the CIS Critical Security Controls (CSC) [34] cybersecurity framework. The main goal of CIS is by giving the CSC to the organizations, they will better be able to defend themselves against know and future attacks by a unique way of choosing the appropriate key security concept, from a big list and turn it to a mechanism that will achieve the selected defensive task. The unique structure of the CSC is help in the core of the framework, where CIS decided to be categorized into three categories the suggested controls. Those are the basic, the foundational and the organizational. In addition to the categories, the CSC is designed with three Implementation Groups (IG) which refer to the size of the organizations they target. But on the version 8 of the framework, the categories were removed, and emphasis was placed on the Implementation Groups

In the most recent version of the CIS CSC, which is the iteration number 8, organizations can find eighteen controls each including cyber defense safeguards, each for every implementation group. In detail, the IG1 which is also referred to "Basic Cyber Hygiene", holds 56 cyber defense safeguards, IG2 holds 74 and IG3 holds 23, all summing up to 153 total safeguards. Furthermore, the implementation groups are a perfect example of how a cybersecurity framework can be applied to any size of organization, no matter how much IT personnel they have or how much money they are willing to spend into the defensive mechanisms. The first implementation group is designed for small and medium-sized organizations that most likely have limited IT and cybersecurity personnel and expertise to focus only on the tasks around protecting the assets of the organization. The second group is made for organizations that do have experienced personnel dedicated to managing and controlling the IT infrastructure and possibly support the needs of big enterprises with many departments in different locations. Finally, the third group should only be applied to organizations that belong in specialized fields around cybersecurity with experienced personnel and sensitive systems that also perform tasks for other organizations such as penetration testing.

If we take a closer look at the controls, we will see that some are very expensive and difficult to achieve if the organization is small or medium-sized. Therefore, the organization can choose which control it will use and align it to the needs it. Example of controls that is impossible to achieve is CIS Control 16 which deals with the Application Software Security and all the safeguards around preventing, detecting and remediating cybersecurity vulnerabilities that could possibly infect the organization. Another example of control is the CIS Control 18 of Penetration Testing where an organization is testing how effective and strong is against any potential malicious activity that is trying to infiltrate its premises. The simulation of such scenarios requires experienced personnel, time, and money, which small organizations do not freely dispense.

Since in our case we are mostly dealing with small and medium size organizations, it would be good to focus on the controls that the CSC can offer and can be applied to such size bodies. For that, CIS has allowed organizations to filter the controls that belong to the 8th version of the framework and check if the suggested actions refer to something that is manageable by the organization's resources. For example, when talking about the Data Protection, which is part of the CIS Control 3 of the framework, some encryption of data on end-user devices or the establishment and maintenance of data processes, are easy safeguards to implement and can immediately elevate the security posture of a small-sized organization.

When a small organization is choosing to implement the CIS framework, most of the controls are available and there is always the opportunity to choose the exact approach on how to perform this control. It is known that the Audit Log Management is not an easy task as the collection of detailed audit logs and their retaining is not as easy as just establishing the entire audit log management process and ensuring the appropriate storage for them. These safeguards will distinguish the Implementation Group and maybe even classify the organization as more secure.

In comparison to other cybersecurity standards, we find the CIS CSC as a starting point for organizations that want to have a complete and detailed approach as on how to protect their data and assets. Later, when the security posture of the organization is hardened enough, a more complex cybersecurity framework can be implemented but then the emphasis will be in the details but crucial if the company really wants to invest in its protection.

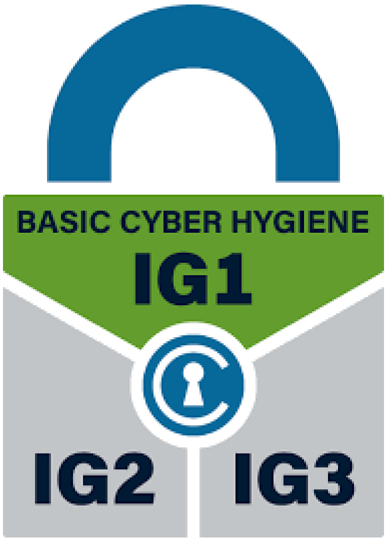


Figure 9: CIS CSC Implementation Group 1[35]

2.6.6 Comparison between the frameworks

Almost every country in the world is trying to protect its assets, either they are related to people or not. As it is obvious, huge amounts of money are spent in this effort and this created and continues to create comprehensive cyber security frameworks that undertake the role of a “guardian angel”, if one can say, against the possible threats that lurk in the Internet world. Unfortunately, the threats are only in increasing in numbers and severity. Other target specific people, other entire organizations and other whole countries and governments. Without a doubt, some countries have suggested more complete frameworks that are released to the public for the common good. Countries such the United Kingdom, Canada and Australia have offered extensive protection mechanisms that all have some common points.

In a short comparison between the available cyber security frameworks, one can see that even though the use of the frameworks is said to be general, deeply, it is customed to fully cover each country’s threats and vulnerable points. But at the same time, since the cyber-attacks can affect different countries, the mechanisms that are suggested can be widely accepted. Let’s take for example the case of the United Kingdom, that during the Covid-19 pandemic saw major vulnerabilities and security flaw around the health sector with around 20% of the organizations been linked with it. Having so big threat surface for attackers to use, the UK government dealt with 777[36] significant incidents only in the year 2021, which roughly translates to that attackers go along with the everyday changes. As a result, frameworks that originated from the UK shifted their approach to cover more health incidents than before. This is only one of the many examples of improvements the cyber security frameworks have to offer.

With a different approach comes Canada that decided to focus on the digital economy since that was the field that showed increase both in finances to the government and increases to the numbers of jobs. Therefore, from one side we have the economic growth but on the other hand, we have a much larger target surface with numbers talking about a 78% affection percentage of successful cyber-attacks to Canadian companies. This also explains the shift in actions and controls inside the Canadian framework that focuses more on the financial factor rather than the health factor as the UK one did.

To conclude, the reasons and circumstances that push a company to develop or change its framework, are highly affected by its immediate environment, no matter if it is related to finances, health, or any other field. For that, we cannot expect one cyber security framework to be designed for every single organization in the world. Based on this, a smart approach from countries would be, to pick the framework of their choice and alter its parameters so it fits, to the highest degree, the needs their direct environment has.

3 Properties of a Security Framework

In order to fully understand and then develop our own Security Framework, we first must understand the architecture and structure of them. Similar to the cars that have a set of wheels a frame and an engine, frameworks require parts, so they operate in harmony.

3.1 Components of Security Frameworks

Like every other defined element in the Cybersecurity world, every Framework is constructed based on three main components.[37] The Framework Core, the Implementation Tiers, and the Profiles. All those components and strictly connected to each other and based on each other for a proper and smooth cooperation.

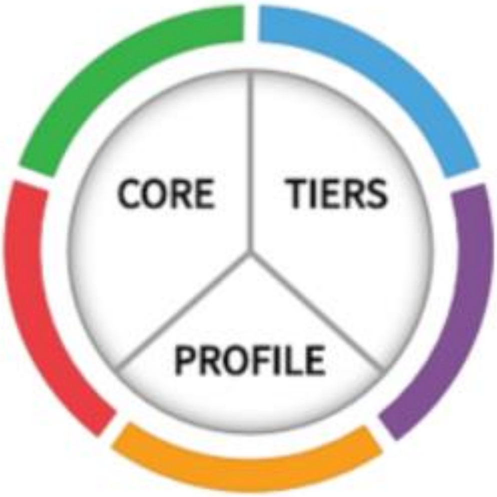


Figure 10: Components of Security Framework

Framework Core

Here lie around the standards, the guidelines and the practices that are presented in an understandable manner and language. This way it allows the communications of cybersecurity activities and outcomes across the organization from the executive level, which is the highest level, to the implementation or operation level, which is the initial level of an organization. Basically, the framework core, guides the organization and the management of security keeping the boundaries in place and reminding at any time that the organization has some specific rules to follow. This part needs the most of time to organize and fulfill since, any digression of it might influence the overall character of the organization. Following the core, the connection between overseeing and decreasing of any cybersecurity chances, is guided in such way that it adds to the proper implementation of the cybersecurity and risk management processes.

Framework Implementation Tiers

In this component of security frameworks, we have the "user manual" of the conduction of the assessment process and planning of cybersecurity activities in the organization. The tiers describe attributes to consider when creating a target profile or completing a current profile. It helps in a way that the correct settings are applied on the point of view of the cybersecurity risk management from an organization. Using the implementation tires, organizations are assisted in deciding the suitable level of completeness for the cybersecurity program of choice. Those tiers can be used as specialized tool that can deal with functions like arranging the spending plan of the company or the categorization of the mission needs of it.

Framework Profiles

The framework profiles represent the outcome based on business needs that an organization has selected from the framework categories and subcategories. The profiles can be characterized as the alignment of guidelines, standards and practices that were chosen and are part of the framework core in a particular implementation scenario. In other words, it communicates the cybersecurity requirements because they are used to recognize and organize the openings in an organization so as to enhance the Cybersecurity.

3.2 The Five Elements of a Security Framework

NIST describes the Cybersecurity Framework using five elements or functions.[37] They provide a general understanding of the structure of the frameworks since many are designed based on these elements. The basic functions are included within the core of the framework, and each consists of different categories, subcategories, and informative references.

3.2.1 Identify

In this first element the organization must establish the framework and fit it to its current needs. The framework has to be suitable for future cybersecurity-related measures taken by the company. The company's personnel must identify which dangers exist, what is their likability to occur or what outcome the attack might have, all of which must be included in the framework. Only then the framework will have the correct settings that are immediately connected to toe company's profile and are tailored to the current dangers. This part is of critical importance to the framework's success. From the category level, that comes after the Function level, out of 23 the 6 categories, are part of the Identify Element. They are covering a broad field of objectives that have to do with the initial steps in the implementation of a Security Framework such as Asset Management and Risk Management. Their managerial nature stops them from being very strict unlike the next categories that follow. For this reason, they can be used in both cybersecurity risk management and in risk management in general.

In the public sector, which is our field of interest, the element of Identify can be fitted in the cyber security Governance processes that public service bodies have. In the public sector agencies, it is of high importance to have the roles pre-defined and clear, so the personnel are aware of their responsibilities for managing cybersecurity incidents. People in supervising position need to be designated so a point of contact is nominated. If the management of the public organization is not strong, neither is the overall accountability of it.

In addition to the responsibilities the personnel must have in the public infrastructure, the staff must receive constant and thorough training around the current Cyber Security Baseline Standards. As of now, NIST has organized a platform with relevant training material named One Learning. There, the staff can train themselves and pass from assessments and benefit from the knowledge the platform has to offer, increasing their cyber awareness and guaranteeing their position in the line of defense of the public sector. But when talking about experienced IT personnel, this training must be mandatory. Regular updates in the policies, procedures, and roles of the sector the belong in, need to be included in the awareness training of the staff. For them the training should be not only web-based, but hands on as well in case of cyber-related threat which is not web-deployed.

Since the public sector has immediate connection with third party entities that are needed for the correct operation of the ICT systems in the sector, the organization's cyber security obligations need to be shared with them. When the third party is entering the premises that belong to the public body, they should be aware in advance of what they are about to face. Such third-party entities can be internet of cloud services providers, power and communication technicians or suppliers. In a way of controlling the managed physical and environmental access, of the public sector, every cyber security requirement, must be included in agreements with the third parties. Furthermore, a documented responsibility agreement between the public sector and its providers, must be made in order for both sides to be aware of their responsibilities and in case of improper fulfillment of the services, blames should be given to the correct side.

Another very important managerial category of the Identify element, are the access control procedures that if they are correctly implemented, systems are ensured that no unauthorized access has been given to users and therefore, no unwanted settings alteration has been performed. This stands as a very strong security measures that decreased the chance of human errors that can manipulated maliciously the core of the framework and in extent, the public body itself.

3.2.2 Protect

Moving to the second element of a Cybersecurity Framework, we have the shields of the framework against malicious activities. This element represents the ability of the framework to mitigate any potential cybersecurity instance. Same as the Identify functions, 6 categories of the total 23 are fitted to the Protect functions some of which dealing with the Data Security and the Maintenance of the organization. They are here to offer options of defensive mechanisms in order to contribute as a second layer of defense to the organization. In the public sector, bodies shall have implemented safeguards to protect and guarantee the delivery of critical infrastructure services that are designed for them at that moment.

It is very important, especially in the public service bodies, to have individual authentication and identification of all authorized users that can connect to the organization's network and possibly manipulate the data and assets of its databases, that most likely store information of citizens and are considered by the GDPR sensitive and therefore limited to few. Therefore, everyone who can access personal data must be documented and be appropriately authenticated. A very common way of authentication is the multi-factor authenticator. This way if some malicious actor manages to get access to the organization's network, he will be prevented from entering into applications of computers or even to databases.

Besides the restriction of access, the electronic equipment that the public sector ahs in its disposal, is by itself a way to an intruder to perform malicious actions. For this reason, all hardware and software should be documented, reviewed, and updated in a constant basis. All those Digital Resources that the Asset Register of the public sector will have, will be a record of what computer has been purchased, which operating system it is running, which applications are installed in it and who has access to them. This way, if a malicious actor has managed to install a keylogger on a computer or a well obfuscated malware, on the next review and update of the Asset Register from the IT personnel of the public sector, the computer will be set in quarantine and as a result the mechanism will be perform its job as intended. Additionally, the constant update and upgrade of the electron equipment will offer an extra protection feature for the organization. Obsolete computers and systems are most likely to have many known threats that cannot be countered. If a patch on the system is not available, then the only option is to upgrade into a new one.

Since the human error is one of the possible threats of an organization, no other than the daily used Email service should be protected. To protect email, the public service bodies should implement Transport Layer Security (TLS) between the sending and receiving email gateways. The encrypted now emails will be transferred over the network with much more security and much less fear to be manipulated. But if the equipment of the body is old and not upgraded to newer yet, then the TLS might not be a viable option since it is not supported by older systems. To add to that, the implementation of Sender Policy Framework (SPF) might be a good protective mechanism against email spoofing attacks. This way the receiver will have some email information about the email he is about to receive as of how legitimate and therefore secure it is. Last, when citizens are requested to present sensitive information to the public service body, but need to send them electronically via email, then the body must ensure that they are protected wit encryption or strong passwords which is of course shared via other means of sending.

These all are not enough by themselves if the IT administrators are not well trained. They hold important roles in the line of defense of the public sector as they have access to infrastructures such as networks, user end point devices of servers. They must be trained and preferably certified that they can have security roles and for that, are encouraged to engage in a continual professional development. Administrators must be able to understand and identify any anomalies in the systems they are operating. This comes only after training and experience, and this is why they are a very important component of the human part of the security framework.

3.2.3 Detect

Just the protecting mechanisms are not enough for the security of an organization. There also needs to be a way of detecting the incoming attack and the possibility of cybersecurity incident. Here stand all the exercises to recognize the event of a cybersecurity occasion meaning that we have a more active way of dealing with threats. As part of the Detect element, we have 3 categories of the total 23 with them been the Anomalies and Events, the Security Continuous Monitoring, and the Detection Processes. These categories are explaining the job of an Intrusion Detection System (IDS). In the public sector, the bodies need to detect the cybersecurity incidents before they enter the organization and cause their damage.

Using proper equipment, when an incident happens and a malicious actor is entering the system, a relevant log is created. This log can be later evaluated and analyzed so the organization will now know how to react to any similar future events. The public sector should have appropriate levels of logging information that hold the logs for a specific amount of time until a fix has been found or an upgrade to a more secure system has been done.

Thanks to the existence of Cyber Security Incident Response Teams (CSIRTs), organizations can now share their log of the incident to them and receive any information around it. This way they will have a fast and most likely complete way to counter the specific attack and if reacted immediately, no harm will be done.

As it is obvious, not all infrastructures of a public service body have the same importance and therefore, there must be a clear documentation of them sorted based on their prioritization. Some systems are more important than others, taking as example the more important citizen information database versus the Christmas preparation list. The bodies need to define which assets and systems are necessary for the proper functionality of the services on a daily basis and which ensure that the state continues to function as intended. This documentation should be continuously updated, have a level of importance, and define dependencies between the different components of all infrastructures of the public sector.

In the detection mechanism of the framework’s core, the anomalous activity detection should also be included. As technologies changes, so does the threat landscape worldwide. With the expansion of services comes the enhancement of attacks. In a way to deal with that, incident monitoring systems can be implemented within the infrastructure of an organization that will track the movement of a malicious activity, how it reacts to the current defensive mechanism, what it targets and maybe what is its outcome. This is done by taking a closer look into any unusual patterns of network traffic those activities follow, any changes in settings of installed applications, standard signs of attacks like trying to switch between networks of run software with privileged access, or any retrieval of essential information from the contents of the attack’s infrastructure.

3.2.4 Respond

After having done all the previous steps, now we know how the attacker is acting and more or less are able to react to the attack. In the Respond element of the framework’s core, we have the proper activities which are prioritized through the risk management process, that the organization is following in the event of a cybersecurity occurrence. The Response Planning and the Improvements are few of the 5 categories that this element has. In the public sector, there must exist a cyber incident response and management plan that will help dealing with attacks. Like any other similar plan, the actions, the roles, and the responsibilities of the people that deal with it have to be clearly defined in advance because if a wrong approach of the response process is followed then the incident will be countered.

If the public service body wants to have an incident recording process, it should have a Cyber Incident Response Plan (CIRP) that will guide the organization of how to respond to all cybersecurity incidents. More details on CIRPs will be given on Paragraph 3.4.1. Also, in case of an incident the public service body must have a Communications Plan that will be linked to the CIRP. This plan will include details of the stake holders with whom communication must be kept in case of an incident. The team that is dealing with the incident must also be part of this plan alongside the senior member with their contact details. In extreme situations, the communication might need to be established from a cloud-based system in the case of disability of the primary means of communication. Often neglected, the Communication Plan is an essential part in the event of a cybersecurity incident.

In the correct and legal way of responding to an incident, the organization must take into consideration the current Data Obligations that follow the legal guidelines such as the GDPR regulation. For that the Data Protection Officer (DPO) is responsible to explain to the organization what legal steps should be followed. In the instance of a data leak, the organization needs to know from the DPO, that the individuals whose data are leaked must be informed. These legal obligations also extend to the post-incident sharing. After the occurrence of the malicious event, all the mitigation measures that were followed, need to be shared secretly and evidence of their use should be collected and maintained. When the incident happens, some steps must be taken so the organization understands its root causes and make sure that not similar event will happen in the future. If the incident if web related, internet providers and service providers might need to be informed. But in order to do that, the public service body needs to have a classification policy for the incidents. If it does not have any, it can consider the sharing information based on the Traffic Light Protocol[38].

Before the organization is ready to move to the recovering process from the incident, it must first understand and accept the lessons it learned. This is a way to improve and strengthen the Respond function by learning from what went wrong when dealing with the incident. Of course, the stake holders need to be part of this process because without their acknowledge, no lessons will be learned, and the result will be same as not having any framework at all. A review of the lessons can be valuable to the public sector as it will show the effectiveness of the CIRP.

3.2.5 Recover

In this final element of the Framework’s core, the organization is now able to come back to the regular daily activities. Here we have the operations the organization is performing to keep things up and running or return to normality which the cybersecurity event influenced. The Recovery Planning, the Improvements and the Communications are the only 3 categories that are part of this function. For a public service body to recover, it needs to implement, identify, and test likelihood mechanisms.

Within the public sector, there must be several Recovery Points Objectives (RPOs)[39] which will be there for all the systems of the organization ready to be recovered in case of need. They define the time when data must be backed up in a way that they can be used for this recovery process. These points will assist the organization in the situation of a disaster or failure of a system between specific amounts of data. Meaning that, the RPO sets an amount of data and the aging time of it and when needed it provides the maximum amounts in the backup storage. For instance, if a disaster occurs and the RPO of the public service body is set to 48 hours, and the last available good backup is from 40 hours ago then the organization is covered. If the last available good backup is 49 hours ago, then there might be a partial or complete loss of data because in the 48 hours period an attacker will easily be able to manipulate his findings.

Furthermore, it is necessary for a public service body to have a complete and strong Disaster Recovery Plan (DRP)[40] that will be ready to react to any cybersecurity incident. A DRP will organize the approach a body has to take on how to restore a system access in a standard amount of time that will be updated from the previous four elements of the Framework’s Core. The DRP makes sure that in the event of a cybersecurity incident, the right personnel and processes will react as planned to counter the threat. The Incident Response Plan (IRP)[41] they will utilize, will provide a targeted response to the specific threat to not only counter it but eradicate it too. Even though DRP and IRP are not the same, they are strongly linked to each and to the organizations business plan and emergency management plans to totally support the necessary resources for the functions of the applied framework.

As part of the DRP, the organization must ensure that they have assigned the role of activation of the DRP to experienced and capable personnel of their team. They will be the first to call when the event occurs, and they will be those who will initiate the DRP. All their details must be documented and available throughout the entire time the incident in happening. These authorized personnel will also be part of a recovery team that have to maintain the set of recovery procedures the organization has predefined that will be executed during the event. Not to be forgotten, the public service bodies might be dependent on third-party entities. It is essential to include them too in the documentation process of the recovery plan and if possible, review and confirm their existence constantly.

When recovering from an incident, an organization must never forget the technical equipment they have in their disposal. That equipment must have a technical protection that will cover the network, the systems, and the services the organization offers, while vulnerabilities that lead to the cybersecurity incident must be identified and a plan of their eradication must be executed. This is a process to ensure that the same issue will not happen again or if it happens, the personnel will know how to react fast enough to prevent any damage. In case some vulnerabilities in the equipment cannot be mitigated, the organization must accept the corresponding to them risks and inform the management team on how to deal with them.

An incident does not only cause damage to an organization if it is successful. It also provides the organizations and of course the public service bodies with valuable information and lessons that complete the Lessons Learned Process. This process is a review of the overall incident handling process and is a key component to the improvement of it. New approaches and better practices can outcome from this process while the organization becomes “smarter” and more experienced in similar situations. To enhance that the public sector can organize meetings that will include many different bodies with different approaches and different experiences. The information gathered from those meetings can add to an overall upgrade of the elements of the framework the public sector has adopted.

3.3 Information Security Management System (ISMS)

While a Cyber Security Framework can suggest measures to counter threats and deal with security processes in general, an organization can use some additional “weapons” to its “armory”. Such is an Information Security Management System or ISMS[42] in short. An ISMS is sometimes a requirement for a company to use a framework or can be separate part of the defensive mechanisms. But what is an ISMS and how can it be implemented in an organization?

An ISMS is a collection of policies, procedures, guidelines, and activities that an organization is dealing with, in order to protect its information assets and data. It consists of a systematic approach for protecting, adding, and editing an organization’s information security to reach business objectives that is based on the risk assessment and the organization’s risk acceptance levels. For a proper and successful implementation of an ISMS, some fundamental principles need to be followed while also some points need to be clarified so no confusion is created.

To begin with, an organization must understand why it needs to implement an ISMS because otherwise it will fall into the trap and myth of that such system refers to specific kind of organization with focus on the technological field. Since the information is one of the most important assets of an enterprise, it should be protected. This means that any organization can benefit from and ISMS as there is no difference between an IT organization, a pharmaceuticals organization, or a furniture manufacturing organization. Additionally, such a system is not defined by technical security requirements and companies should fear it. Last, the use and implementation of an ISMS is not controlled from the organization's security department, but on the contraire, only the original steps are coming from it, while the development, the use and the compliance with an ISMS can only be controlled by the executive management.

Specifically, the executive management of an organization should follow basic principles that are needed to for the success of the ISMS of their choice. The must have awareness of the need for information security as the consequences of losing sensitive data can be catastrophic not only for small but also for big organizations too. There needs to be an assignment of responsibility for the information security since some organizations need to have a formal DPO (Data Protection Officer) appointments. On the other hand, it is better for an organization to instill the importance of cyber security responsibility into every member that belongs in it. Furthermore, the management can incorporate commitment and interest of the stakeholders because they need to be aware of the potential consequences of inadequate cyber security measures. For instance, many big organizations do not have a proper incident response plan in case of a data breach. Embedding cyber security is also an essential security measure throughout the organization's IT systems and processes, not only as an add-on, while the nature of the projects and the teams of each organization is different. Last, the continual reassessment of the information security plays an important role to the successful implementation of an ISMS. As seen worldwide, the rate of increase of cyber attacks means that the systems must constantly be tested and strengthened.

Following these and many other principles, organizations can benefit from the managerial security of their assets. When they choose a cyber security framework, they might be requested to also use an ISMS, similarly to the ISO 270001. As described, each of these steps above are a good practice for an organization even if it is not seeking accreditation against the ISO standard.

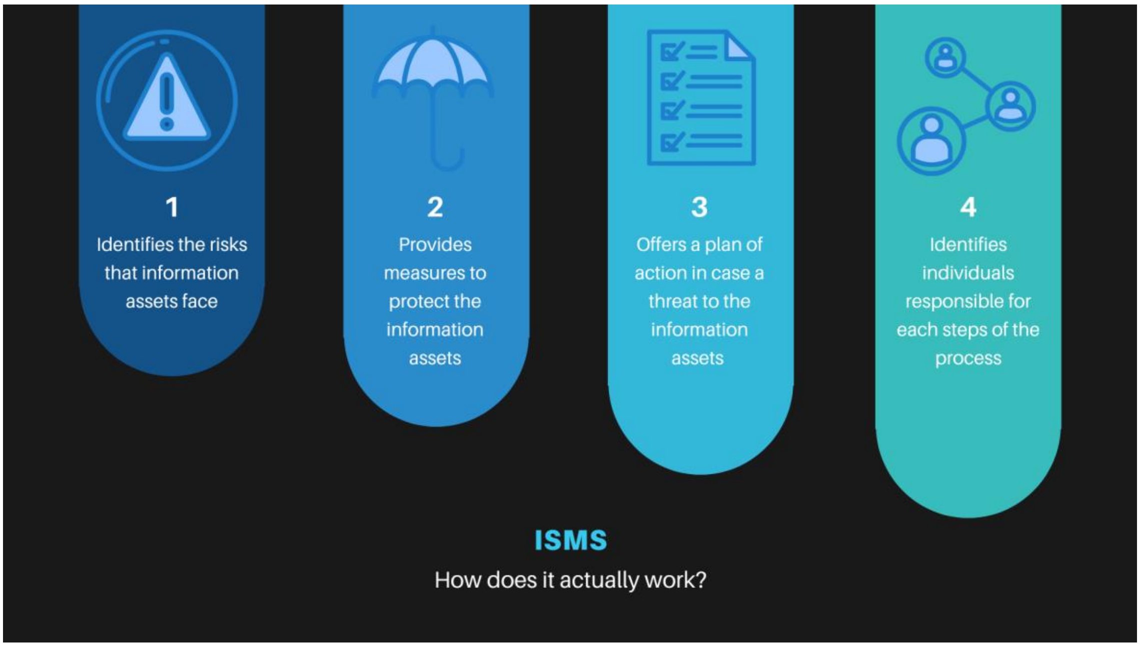

1
Identifies the risks that information assets face
2
Provides measures to protect the information assets
3
Offers a plan of action in case a threat to the information assets
4
Identifies individuals responsible for each steps of the process
ISMS
How does it actually work?

Figure 11: How does ISMS work?

3.4 Cybersecurity Incident Response Plan (CIRP)

When an organization has chosen the Cyber Security Framework of its choice and Information Security Management System[41], it should also include a specific document that will provide the IT and the cyber security employees all the necessary instructions on how to react to important security incidents like data breaches, data leaks, malicious attacks or even loss of sensitive information. This is no other than the Cybersecurity Incident Response Plan or in short CIRP. This document will cover every step in the incident response path, from the preparation before it happens until the recovery and post-actions after it occurs.

An organization needs a CIRP form few reasons. First reason is that when an incident happens no matter how severe it is, the security team will be able to understand the attack and respond in time. If there is no plan to follow and everyone acts on his own, making actions that are helpful, the outcome will not only be the incapability of reacting and eradicating the threat but also resulting into huge financial costs. Especially now that laws and regulations have been voted worldwide, and especially in Europe with the GDPR, companies may face significant financial fines if they don’t protect the sensitive information they store in case of an attack. If the organization does not have a CIRP in place, then it will expose itself to further fines and legal action.

Second reason is that in case of an incident the organization will have a way to investigate the incident from the internal. This means that no external investigation or audit will be needed which might also expose the organization even further. This is why many industries are forced to follow standards that require them to have an incident response plan. For instance, in the US, the California Consumer Protection Act (CCPA) which is a data privacy regulation requires an incident response plan or if an organization is pursuing ISO 27001 certification and does not have a CIRP it will not pass the audit.

3.4.1 Example

As already said, a CIRP can either be a separate framework by itself, like the NIST Incident Response Plan[43], or a template which a company can use. These templates offer a detailed approach that an organization can use to start off with its incident response planning. Some of the completely free templates are the TechTarget's incident response plan template[44] and the California Government Department of Technology incident response plan[45]. CIRP templates offer a complete guide of actions that an organization can use immediately but of course can change it based on its needs. After all it is just a document, that does not force the organization to spend big amounts of money to implement just plan the steps of reaction against an attack in advance.

4 Cyber Security in Public administrations

Like every organization in the world, public administration bodies operate as one too. They have the structure of an organization of the private sector with specific leadership positions, exclusive personnel to key positions, trained professional, tools and equipment to use for their daily activities. The only difference is that the funds that are needed for their daily operations, come from the state and any actions that require money needs to be authorized first.

4.1 Information gathering from public administrations

For the purpose of this Dissertation, information was gathered by all the publicly available information from the online resources of the Greek public bodies while emphasis was placed in the existing legal framework that surround them. Such information is forming the structure and the practices that are used by public administrations all around the Greek territory. Due to the huge amount of different administrative bodies in Greece, the type of data each is controlling, differ from one another and therefore each public administration is using a different approach around their cybersecurity posture. Some administrations deal with sensitive data of the citizen, and other with information that are immediately connected with the economy of the country.

4.1.1 Public Administration 1, part the of Ministry of Education

The first type of public administration body that was examined in this Dissertation was that of the Ministry of Education which includes both Primary and Secondary Education where the responsibilities of the personnel in this public administration body are restricted to all the actions that have to be done around the movement of teachers, organization of secondary education system which holds records of all the students that belong in the prefecture, records of all the teachers that are currently active in schools, applied for position or are about to be moved to other. The administration also takes care of affairs that have to do with the payroll procedure of substitute teachers, the pension plan, and other educational matters. The main concern in this public administration body is that there is no clear definition of the security related responsibilities and the protective mechanisms have witnessed small alteration from the initial instructions the body received from the government.

To begin with, we have the preventing mechanisms this public administration is using but as we will see there is not a central protection, and everything is user coordinated. What does this mean? Each user has access to specific websites, links and portals based on their position. The body is dealing with applications, and user restrictions centrally with corresponding blacklisting. This is applied only to the ungraded network that allows users to use the Internet for general use. On the graded network, each user has his own named account for each platform.

The application settings and restrictions that are installed in every user's computer, are configured by the personnel who followed the instructions as to what to allow and what to deny. Even though a general approach is suggested, there might be changes to each department of the Ministry of Education as it is individually controlled. The users or each computer, should not have full privileges into their computer such as installation of applications, deletion, and updating of them. If someone wants to install a new application, there should be restrictions against it and only possible with the appropriate authorization. If for any reason this public administration has given more privileges to users, the dangers of possible human error and the exploitation of the organization are increasing. Since the employes in this type of public administration body might come from fields that have nothing to do with cybersecurity, the bodies, should follow the instructions, which are also documented in the National Cybersecurity Strategy 2020-2025[46]. As additional enhanced security requirements, this type of public administrative bodies, should be provided with the corresponding protection around their network which consists of firewalls, DMZ, remote access, and VPN. Furthermore, it is common for the public administrations to have additional software firewalls that are installed in each computer. This provides extra user protection against the web but needs to be constantly updated.

When we talk about the strengthening of the users, especially in the case of the Ministry of Education where the employees have access to e-platforms, it is suggested to have a password change at a very frequent basis as with no proper change of them, an attacker can have access to the personal sensitive data of teachers and students. This type of platforms could be the “myschool”[47] which is a unified information system that assists school units and administrative structures of education in the Greek territory and also requires named account to access it. This is on the most important requirements the Hellenic Ministry of Digital Governance has asked to be implemented by the public administrative bodies and therefore should be followed strictly. It is in the hands of each body to enforce this kind of changes with a way that is not causing any confusion to the users.

How does the public administration limit the extend of attacks? When we talk about physical and environmental attacks, there are protocols that originate from the Ministry of Climate Crisis and Civil Protection around the plan that public administrations are forced to follow in case of fire, flood, earthquake and even war that include emergency contact numbers, disaster prevention equipment (fire extinguishers), and responsible personnel. These protocols have reached every body in Greece but they remain at the competence of each body's administration to put them to use and force them when time comes.

As it also suggested, the teachers and the employees that need to connect to platforms of the Educational System use Multi Factor Authentication (MFA) which is a very targeted protective mechanism. These platforms are "myschool", the payroll system and the teacher allocation platform. The reason behind the implementation of MFA is that since the GDPR regulation, came to effect, all European organizations that were dealing with human, and not only, sensitive information, had to show the protective mechanisms they have. In our case, the administration is dealing with sensitive information of teachers, students, and schools.

Moving on to the user privileges, we have already mentioned that each user has full privileges to his/her computer. When we talk about the platforms the employees need to connect in order to perform their daily tasks, the account are as normal users except some few that have administrative privileges. For the protocol platforms that store all the documents that include the laws, regulations, changes, and implementations the body has done in the past, the public administration must also have accounts with administrative privileges. As a result, there is strict restriction of user privileges in the administration body which is resulted from the security policy that the body has selected which also abides with the current security situation of the Greek territory.

Last, as the most important mechanism the public administration has implemented is the frequent backups for the important assets of the body. It is obvious that some servers require more frequent backups than other due to their severity and sensitivity of their assets. Each public administration is choosing the right approach which is following the instructions and of course any legal restriction too.

4.1.2 Public Administration 2, part of the Ministry of Environment and Energy

The second type of public administration body is one which is part of the Ministry of Environment and Energy. This Ministry has many employees of different fields who work in positions related to the Energy, the Forests, the Mineral Raw Materials and of course, the Electronic Governance. By the size of this organization, we get a clear idea of how most of the Greek public administrations work and have issues with, while anything that affects this Ministry, it most like affects any other body in Greece.

As we move to bigger public administrations, we see more complex and secure configurations. The Ministry has implemented security mechanisms that follow the instructions that have been given to them. Here, since we have many employees, it is easier to have a positive effect of training of the personnel. This mechanism is strongly suggested and is mentioned in the National Cybersecurity Strategy. It consists of actions that the public administration can take to increase the knowledge of the employees which will result in less human errors. The different fields of expertise all the employees have, makes the Ministry open to threats that have to do with human interaction. By implementing a training plan that will increase the awareness of the personnel in areas that they have never studied about, is key to the elevation of the security posture of the body.

Every computer, server and any relevant software that are used for the daily activities of the Ministry, have original Windows OS while also original licenses for Windows Office which achieve a high level of protection against identified vulnerabilities. Due to the original licenses, the organization receives the updates in a regular basis and keeps the entire body secure. It is also suggested the public administration bodies should minimize the number of legacy systems that remain outdated and pose a threat to any infrastructure. But sometimes we can all understand that it becomes really difficult to exchange an old system with a newer one when the appropriate personnel are missing. All the bodies are aware of such system and indeed try to make changes whenever they can.

As the employees are many, so is the network traffic that is been created by and to them. Therefore, it is very important for the public administration to have mechanisms that will fitter and block unwanted traffic flowing through the network. For that, it is suggested to have a central Firewall appliance with functions that block malicious activities and an Antivirus that will detect and block the incoming virus to the network and potentially exposing important information.

The Ministry is using the “Syzefxis” system for their mailing, which provides a secure solution for the entire Greek territory. On the negative of this, if this mailing system gets inactive, approximately 95% of the Greek public administrations has no mails, or maybe 80% of the telephony is not operational, due to the efforts of interconnecting networking with telephony. This though, creates many problems when trying to move one protocol of a specific Ministry to the new Ministry it got combined with. The protocol is a filling system of all the incoming and outcoming messages that is stored in a tree-like network. Therefore, is very difficult to cut a branch from one tree and paste it to another. This is how such platforms are structured in the Greek public administration, but this is no concern of the body itself as it is controlled by a mode general entity, which also applies to other Ministries.

4.1.3 Public Administration 3, part of a Municipality

The third type of public administration body in this Dissertation is one which is part of a Municipality and more precisely with a department that deals with Technical Services. The building of this public administration hosts one of the 2 datacenters of the Municipality. The second datacenter is located inside a second public administration of the same Municipality and is used for redundancy reasons. Here, the body can establish a very secure way of preserving the data it is holding, due to its multiple locations. In case of natural disaster where one location is suffered, the other one is holding the backup of the first.

The role of this public administration is crucial to the protection and preservation of the assets of the Municipality. This public administration is controlling data protection mechanisms that protect the personal information of the citizens of the Municipality. These mechanisms must follow the GDPR and all that this entails since the nature of the data is sensitive. Any action that violates these regulations might be catastrophic with severe consequences both financial and political.

At the current state, the Municipalities, like other public administration bodies in Greece, use the Syzefxis communication program for the protection of the digital data. Right now, Syzefxis remains in upgrading process to the Syzefxis 2 which includes the purchase of newer equipment, more secure protocols and an overall strengthening of the telecommunication needs of the public sector on both voice and data. For now, and until the public sector receives the upgrade, this public administration is responsible to control all the security protocols and provide the necessary traffic filtering actions to a big amount of the data that are daily transmitted to the Municipality.

After research that was done around the municipalities in the Greek territory, around the total amount of employees, there are users with various permissions all of which are changed in a regular basis. A central database of the exact parts and equipment each employee is using is kept, which include the serial numbers and the purchase date, for better and faster troubleshooting services. This assists the role of a monitoring system which is in place and filters the incoming and outgoing traffic with the help of highly sensitive and accurate sensors. As a further detection mechanism against threats, stands the public Irida system which besides assisting the electronic management of documents and tasks, it is also used for threat and virus detection. It is another platform the Greek public administrations use and for each Ministry or municipality, the users have specific named accounts. Additionally, the Municipality has in its disposal the Diavgeia system which is one more platform of this structure.

From the beginning of the Pandemic of Covid-19, the Municipalities and almost all the public administrations in Greece, have coordinated the remote access for the employees where it is possible. To support the fast implementation of a platform for remote working, the employees could use various clients and if the body had in its disposal specific firewalls, the connection could be done from it with also having multiple MFA mechanisms. There was no clear instruction from the government regarding the way and the tools that remote working should be implemented and therefore every body chose the one of their likings.

In the past, the only source of attacks the municipalities have received in the Greek territory, were minor phishing attacks which did not cause big damage and got countered fast. Furthermore, the websites of the municipalities, if they have any, are getting compromised which is resulting into loss of significant amounts of data and ever since, the control, editing and the management of them has been done by an outsourced partner to the municipalities. Similar attacks were published on governmental websites and the details that were gathered from them as to the way the attack was performed or the tools that the attacker used, were used to edit the instructions that the public administrations received. Having now know the specific attack and its pattern, public administrative bodies can protect themselves from it. And since the Greek government is using tools that are widely used in its network, the sharing of needed information was done.

4.2 SWOT Analysis for public administrations

As we have seen from the research around the public administrative bodies, each one is acting separately from the other even though they all belong to the same country and receive money from the same treasury. Each one is strong in some mechanisms and weak in others. Below follows a general view of the problems, and issues that are identified for the public administrations that cannot speak for the entity Greek territory but can be a good referencing point.

STRENGTHS

Due to the nature of the public administrations, which include manipulation and holding of personal, and in some cases, sensitive information of the citizens, there is the need for having defensive mechanisms against cyber related attacks. Below is the list of things the public bodies control and do well in.

1. Password change which is suggested but not forced
2. Blacklisting of bad websites and whitelisting of good websites
3. Regular Backups
4. Use of secure governmental programs for file sharing and communication
5. Multi factor authentication
6. Firewalls and Antivirus
7. Awareness training to the personnel

WEAKNESSES

It is not easy to first coordinate and then implement actions and measures if you do not have the full control of them, something common for the public organizations. Below follow, what public organizations lack in or things they have not been implemented yet.

1. Sometimes the Firewall and the Antivirus is not centrally placed but only locally
2. The permissions of the users are not well coordinated and given

3. No restrictions when accessing the Internet from the work environment
4. Use of MFA only on some occasions
5. Sometimes few to no awareness training of the personnel
6. No existence of CIRP and DRP
7. Lack of personnel but in numbers and experience

OPPORTUNITIES

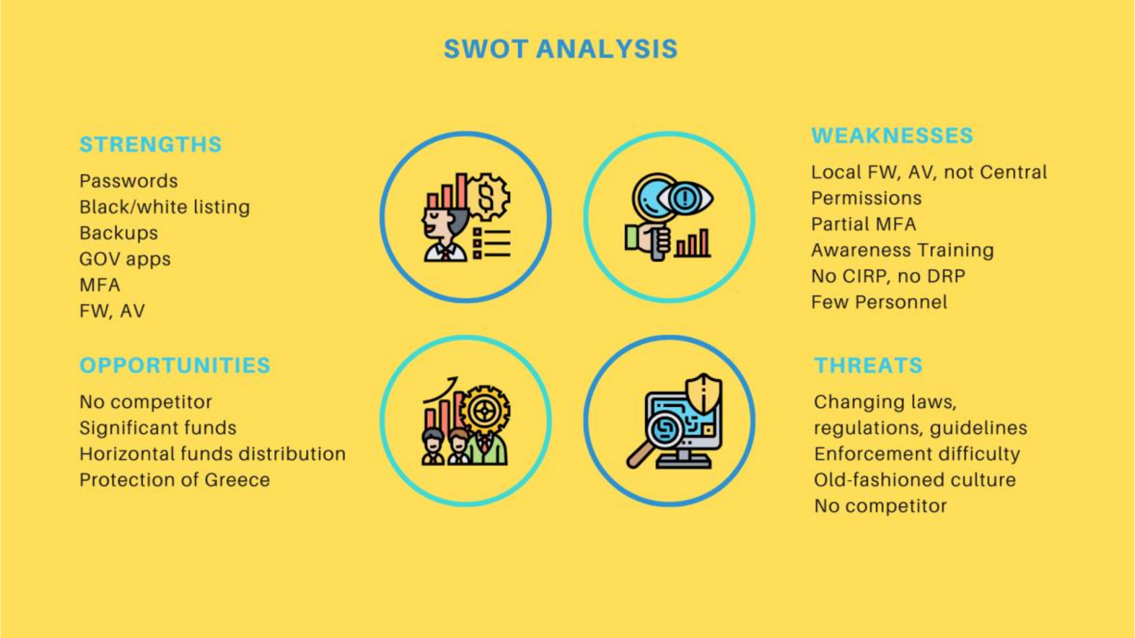
Like other governments all over the world have done, same can Greece. Following the steps of Canada or Australia, the Greek government can detect the opportunities it has been given due to the financial growth and technological advancement it has seen the past years. Since we are talking about a government coordinated organization controlled by a single point using a single treasury, Greece can benefit from not having any competitors within its territory and expand in terms of cyber security defense. Below is a list of some potential reasons why the Greek public administrations can excel in the field of cyber security.

1. There is no competitor
2. With coordination and correct distribution of funds the growth can be horizontal
3. Protect the entire greek territory

THREATS

With every good comes a bad also. When one tries to advance there will always be a drawback that might stop or slow down the advancement. Similarly, the Greek public administrations will face threats and might not be able to achieve their goals. When trying to control your organizations' threat landscape, it is not an easy task. Below we can see some possible threats that Greek public administrative bodies might face.

1. Regulations, and guidelines
2. Difficulty to enforce the frameworks
3. Old-fashioned culture
4. No competitor and therefore no challenge to advance and improve



SWOT ANALYSIS

STRENGTHS

Passwords
Black/white listing
Backups
GOV apps
MFA
FW, AV

WEAKNESSES

Local FW, AV, not Central
Permissions
Partial MFA
Awareness Training
No CIRP, no DRP
Few Personnel

OPPORTUNITIES

No competitor
Significant funds
Horizontal funds distribution
Protection of Greece

THREATS

Changing laws, regulations, guidelines
Enforcement difficulty
Old-fashioned culture
No competitor

Figure 12: SWOT Analysis of public administrations

5 Choosing the right Framework

When it comes to the choice of the correct and more accurate cyber security framework, there is no clear and definite answer. Some would say choose one that is very popular and has been accepted by many countries or organizations. Some other will say try combine many. None of those options are neither correct nor wrong. It all comes to what the organization wants to achieve, what budget it has and how willing it is to make changes. With all that said, below follows a detailed approach of a Baseline Cyber Security Framework customed to the needs of the Greek public administrations. To avoid any confusion, it must be noted that this is just a suggestion that is not based on extensive checking with professionals or is accepted by known cybersecurity guides worldwide. The below suggestions are an outcome of close examination of the current situation of the Greek public administrations that is affected by the needs of them while also the current health situation that exists in the world regarding the pandemic of Covid-19.

Overall, the Greek public sector is divided into numerous ministries, each having under its jurisdiction an even larger number of directorates, divisions, and departments. As it is perfectly normal, within the Greek territory, we will see small, medium, and large sized administrative bodies. Since we would like to suggest a cyber security framework designed for the entire public sector, we choose a versatile approach so it can be used from any size body but with higher focus to small and medium-sized ones. So here follows an 8-step guide which any public administration body is free to use if they feel it will be of help when dealing with cybersecurity threats and what they entail. The steps are not mandatory, and those of the 3rd phase of implementation of the framework can be skipped, or if they are already implemented, they can be modified.

For assisting the designing of the guide, the Cybersecurity Handbook from the National Cybersecurity Authority of the Hellenic Republic, the CIS Controls v8 and the ENISA Cybersecurity guide were considered. The aim of the guide is to be specific to the needs of the Greek public administration and the steps that are suggested are targeted to them.

5.1 1st Step, Prepare the ground

Before an organization starts implementing and applying all the defensive mechanisms it has chosen, it must first prepare the ground for them which also signifies the initialization of the 1st phase of implementation of the suggested guide. This means that all the parts that form an organization must be ready for any future change. Parts can be the building itself where the organization is located into, the employees that have to complete the daily tasks, the equipment that is used for the daily tasks, the services it provides and the status it has in the general landscape. Undoubtedly, the people are the key component for completing the daily tasks. But people are not enough; they also need to be well-structured inside the organization while having specific roles and tasks. For that, all the organizations have higher ranking personnel, who take care of the smooth operation of the organization. When also talking about cybersecurity, someone or a small group of people must be in position to know how to react in case the organization is under attack or is generally exposed to some threat. They are the first who will know how to react, decide what is the right option to deal with the threat and take the responsibility for any positive or negative outcome. Before the incident, they will be those who will know and suggest which is the correct and appropriate equipment the organization must purchase, what skills to look to the new employees that will be hired, what will the training procedure be for the old and new employees, while also for the effective development of the policies that are accompanying the cybersecurity framework.

Within the organization, the communication of the employees must be achieved clearly. It should not create any confusion and should abide with the laws and regulations, while it also protects the rights of the employees. All these can be included in the ruleset that the responsible for cybersecurity matters personnel will enforce to the organization and will provide the organization with the appropriate employee buy-in. These rules should be outlined in the framework’s cybersecurity policies and be mentioned and become understood by the entire employee list. Then, they will know what is correct and what is wrong and of course what are the consequences someone will face if the policies are not followed as intended. Obviously, the cybersecurity policies must be constantly reviewed and updated as the goal of the organization might change as it continues to operate. By organizing the above-mentioned rules, the organization is preparing the ground for the application of the suggested framework.

All the rules that are explained in this 1st step, must never be opposed to the current data protection regulations. Since Greece is part of the European Union, it must follow the GDPR regulation to the exact. Especially for the public administrations that store, process and maintain personal data of the citizens, the framework must ensure that no security control is skipped, and the protection of these data is in place. Personnel with appropriate knowledge and experience should be checking if everything is working as it is intended to and not against of any change of the legal landscape of the country. Sometimes this job can be undertaken by third parties that have a contract with the Greek government and will take care of the GDPR related actions.

Everything must be checked, verified, updated, and controlled. If the initial step fails to be met, then there is no point in even thinking of implementing a cybersecurity framework neither its defensive mechanisms. This task is not easy and must be dealt with clarity and without any influence as it holds the key to success of the framework.

5.2 2nd Step, Have what is needed

For a public administration body to implement the framework of choice of the Greek government, the needed parts must be there. Those parts are no other than the personnel, the equipment with its software and applications, the organizational procedures, and the security policies. If the organization has prepared the ground, it can then control its employees and its equipment which will perform the daily tasks. Since we are referring to a public organization that cannot take decisions that affect no other that its body, each public administration must understand which of the mentioned parts it can get, change, or upgrade in order to complete this step.

It is also noticed from the research that was done with some public administration bodies, that the Greek public sector is lacking experienced personnel. This can be done by 2 ways, and it completely remains to the liking of the Greek government, as it is the one who hires personnel and not the public bodies themselves. The first way is to open positions for people who already have enough experience to undertake tasks such as dealing with threats and incidents, know how to react to them, apply the defensive mechanisms that have been chosen and know how to operate maintain them in working order. As it is obvious, experienced personnel is hard to find and even more difficult it is to find one that is also experienced to the defensive mechanisms the organization is using.

- **Personnel Training**

For that, it is better to move to the second way which is training the personnel that is already employed. This process is slow and might end up in errors and difficulties, but it is worth the try. The training is not one, but it can be of many levels and specifications. The public sector can choose some basic awareness and expertise training courses for every employee and more specific and advanced ones for each department. Some fundamental training courses that can significantly boost the initial defense, should be those of introduction to GDPR, phishing awareness, and remote working. Later, or if needed, the personnel can be assigned to more advanced trainings which in the end, will be the first line of defense of the public sector against threats.

- **Equipment**

The second part is that of the required equipment. The public sector must provide the correct and the secure equipment that the administration bodies will use. This equipment is the computers the users use, the servers, switches and routers, the engineers operate, and the software that is included in those devices that assist the role of the framework.

- **Third-party vendors**

In addition to that, the Greek government must make sure that the third-party partners also abide with the government's security levels with emphasis to the sensitive personal data of the citizens. The agreements between the public administrations and the third-party vendors must be strict and precise because the Greek government is allowing access to entities outside of its control to sensitive and highly classified information. The vendors must also pass a certain set of approvals and meet the necessary levels of security. And keep in mind that the vendors are outsourced entities that grand access to the organization's assets, therefore the agreements with them must be checked and modified in frequent basis since the landscape around cybersecurity is changing in the blink of an eye.

- **Organizational Procedures**

Even though some procedures are common to every public administrative body in the Greek territory, each public administration, can choose some specific ones that will better organize it locally. These procedures must consider the amount of personnel the body has while also the equipment it has into each disposal. For example this could be referring to the distribution of laptops that the body can provide to the employees who travel around the municipality and perform their daily tasks.

- **Security policies**

Organization cannot exist without the rules that define it. Sets of rules must be there that will control the correct and smooth operation of the daily activities of the public administration no matter its size. Such security rule can be as simple as knowing that every employee of the administration must not freely give away the personal data of the citizen whose data is storing.

5.3 3rd Step, Know how to Respond

In most of the cases, a company neglects its defenses and relies on pure luck if an incident occurs. But then it will be too late, since the damage that will be caused it could be irreversible. When sensitive data is in place, and are compromised, they first are unpredictable and second, hard to restore. Therefore, it is of high importance, for an organization, especially a public administration body to develop a way to know how to respond to any malicious incident. This is made through a Cyber Incident Response Plan (CIRP); a formal document that has included all the possible guidelines, roles and responsibilities that will be needed in case of an attack. Then the organization will know how to react, who will take actions first, and in general, avoid any confusion.

- **CIRP**

A CIRP is a very important part of implementing a cybersecurity framework and therefore it comes in the first steps in our guide. If the organization first develops the controls that form the defensive mechanisms and later develop a CIRP, then it will be like buying the fuel for the car before you buy the car itself. We cannot find the best CIRP for an organization, but we need to modify the CIRP based on our needs, and this will make it the best for us.

Every plan is different than the other, as every organization prioritizes different assets and protection approach. This plan does not have to be very big with many subcategories. Since many Greek public administrations do not have many employees in the IT department, then the roles in this plan will be very specific. Few people will take the actions when the cyber incident occurs. With this step we conclude the first phase of implementation of the suggested guide for the Greek public administrations.

5.4 4th Step, Secure Everything

Moving to the second phase of implementation of our suggested guide, a Greek public administration, must secure some important parts of it. They are not only the basic devices and networks but also the access to them. Having known the popular attacks that lurk on the Internet and target organizations regardless of their size, a public administration, can start improving its posture by doing some relatively easy tasks. Those tasks require time and effort so they are not done in a hurry but correctly and as a result ensure that the outcome will only be helpful.

- **Up to date systems**

Starting off, the responsible personnel must make sure that the operating systems that occupy the devices that are used, while also any software that is install in them, must be up to date with the most recent patch. Additionally, the organization must keep track of legacy systems that are still using and migrate to newer versions that receive updates. Those updates are needed as most of them refer to vulnerability fixes that resulted from relevant attacks. To this task, the enabling of automatic updates for the devices that is possible, can save some time from the employees' job especially if the list of devices is big.

- **VPN**

During the last years, many transfer and network protocols have moved to their secure version which allows encryption and therefore less chance to be vulnerable when moving from one node to another. Nowadays, portable devices like mobile phones or laptops are very often used and since they might get connected to public Wi-Fi networks, their encryption, offers security to the users. Additionally, a public administration can utilize Virtual Private Network (VPN) tunnel for employees that decide to work remotely or employees who need to travel. The use of such tunnel offers secure connection to the government's sites using secure connections formed by SSL/TLS protocol.

- **Anti-virus**

Updating software and using secure tunnels is not enough when talking about incoming to the governmental network traffic. To protect against viruses, the public administrations can install centrally managed anti-virus software or hardware that will undertake tasks as filtering the traffic and protect all the devices that are immediately connected to it. For extra protection, every device in the premises of the public administration must ensure that the local to the computer anti-virus is up-to-date and the traffic that ends up here is clear of viruses.

- **Firewall**

In the securing process, the network security plays the most important role. Here all the traffic that passes to and from the public administration is exposed to attackers who will benefit from open doors left behind. To prevent any malicious actions, the Greek government can provide with firewall solutions to all its departments that will be deployed in such areas where systems play critical role as for instance the citizens' personal information databases. Higher emphasis should be given to the incoming traffic from the outer Internet to the internal of the organization's network.

- **Secure access to devices remotely**

As we already know, the recent pandemic of Covid-19 forced many organizations to shift to a remote access solution so the employees can work from home without fearing from their health. On one hand, we have tools that can help this need, but on the other, we have many open doors for attackers to use and infiltrate the public administration systems. For that, the tools that are used for remote access must be secure, utilized through a VPN tunnel, up to date, include multifactor authentication and ensure that their monitoring and alerting is up and running so when suspicious activity is noticed, the responsible personnel is aware of the exact threat and what to focus on while trying to react to it.

- **Secure Credentials**

Last, knowing that the human error causes a high percentage of problems in organizations that end up in compromise, it is highly needed to have secure access to the systems. Every employee needs to be aware of the equipment they are using and not pose a threat to it by not knowing how to operate them. For this, Greek public administration should demand a frequent credentials change with more complex structure than just letters and numbers. More numbers, letters and special characters make the passphrase harder to crack by the current cracking tools. Additionally, reuse of passwords for other platforms of software is good to be avoided, while also sharing of them to others.

These are simple actions that will elevate big a lot the security posture of the public administration body and strengthen the overall Greek landscape around cybersecurity.

5.5 5th Step, Harden the Physical Protection

Nobody will know what happens to his/her device if left unattended. Same goes to the situation of a working environment such as public administration where daily, numerous devices portable or not, are being used. It is very important to make the employees be aware of how they can physically protect those devices by a very simple action. This is no other that locking their device when they need to leave it on the desk, or in some meeting room, or in general somewhere that it can be manipulated by unauthorized people. This is also an extension of awareness training programs that will create the stimulus to the employees of locking their devices.

- **Auto-lock of systems**

Luckily, there are automated applications that can undertake this task if forgotten. Auto-lock functions can contribute to this task regarding the digital information that can be seen or manipulated. Same can happen to documents, since a public administration in Greece is using printed documents for various operations, there must be a way to secure them if left behind. People cannot always carry those documents with them and for that they need to be stored away securely. When talking about documents, the sensitive information of the citizen might be included and can be used against them if fallen into the hands of any malicious actor. Their storage can be in special containers that can be opened using passcode or alternatively a key.

- **Physical Security**

Physical security does not stop here. If the public administration has in its disposal remaining funds, those can be spent into the hiring of experienced security guards that can provide the extra sense of security especially to bodies where they are really needed. This can be very costly and is not always chosen but nevertheless, when a security guard is in place, people react differently and immediately the security posture of the agency increases significantly. Another possible physical security mechanism could be the installation of double doors to the exits of the building which will act as a barrier in case someone tries to steal devices or documents from the public administration. Special locks can be set up in various location, preferably close to senior personnel, that can lock the doors if needed.

Overall, the physical security is the extra protection an organization can implement and should not count on it completely. Even though there are so many actions that can be taken into consideration, some are good to be performed in a daily basis, like the locking of the device when left unattended.

5.6 6th Step, Backups

As we have understood by the meeting with the different public administration bodies, all of them know how to perform and need to have the ability to restore and recover information in case of a misconfiguration, cyber-attack of physical disaster. This recovery can be done via the Backups. In some cases, they need to occur in a more frequent basis than in others based on the severity of the data they control. Different organizations have different servers, and different servers store different data. For that, the public administration must understand and acknowledge the severity of the data and plan the backups accordingly.

While having a backup is one side of this step, the other is the rules that the backups need to follow. Those rules consist of parameters that need to be taken into consideration for the better storage of data. In short, backups need to ne regular and when the device, system, software allows it, to be automated, which will require less human interaction and therefore less potential human errors. Additionally, the storage of the backups must never be in the same area where they were taken from. For instance, if the public administration has 2 building in different location, one can be used as the storing of the backup of the other and vice versa. When the backup is getting transferred from one location to another, their encryption is mandatory to ensure that no alternation ahs occurred. Last, the responsible personnel must frequently test the integrity of the backups and perform tests whether they can be restored, how fast they can be restored and how easy that process is.

It is left into the needs and capabilities of each public organization to choose the frequency of the backups for their devices but as it is clear, the more frequent the backups are, the less work is lost in case of restoring. It is not the same when you restore a month-old document and a day old one.

With this step, the second phase is also completed. From now one, the organization can elevate its security posture extensively and differentiate from other similar organizations in both size and field of action.

5.7 7th Step, Reach the sky

Some mechanisms are easy to be met even for the smallest organization with the least possible amounts of money. But some require special preparation and specific focus in order to be achieved. The third phase of the implementation of the suggested guide is referring to the next level of security mechanisms a Greek public administration can reach and is easier to be achieved when we are talking about big entities. This consists of actions that have to do with the elevation of the security and the network posture of the administration by engaging it with the cloud. This process is very risky but highly rewarding in the end.

- **Cloud solution**

If the public administration will not pay attention to details, when picking cloud-based solutions, then the risks that it might face, might result into severe consequences. But there is no need to be scared of the cloud since there are free online guide that can provide the public administration with key steps in migrating to a cloud solution. Such solution can be met either locally, in the premises of the administration, which will be more costly, or with the support of external cloud providers, which will easier and cheaper. Here though, the regulatory frameworks should be met to the maximum degree as, the cloud provider will have access to sensitive information the public administration controls and keeps of the citizens. And for that is the EU GDPR which stands as a protective mechanism to actions around sensitive information.

With the elevation of the organization to the cloud, the opportunity to increase security in every online site is there. A cloud solution can be extended to degrees that not only storage comes in place, but also firewalls, monitoring systems and online platforms. Configurations that maintain the security of data that are distributed through the network of the administration are highly important with reference to credit card data of financial details of the citizens. Furthermore, by using cloud solutions, automation comes with security tests against the platforms that the public administrations use, that will then provide with all the necessary information to the responsible personnel who can review the findings and make any changes ensuring this way that the operation is updated and working as intended.

5.8 8th Step, Share the knowledge

As we have already explained, the existence and importance of CSIRTs in the global security environment, is crucial as to the seeking of knowledge and sharing of acquired information. Every organization, including the Greek public administrations, can share their information about new or old threats or incidents with others. This way in case some organization faced a threat which resulted into loss of data, the knowledge around how to react is shared to others and will then prevent any similar malicious activity from happening to their assets.

- **Greek public administration incident response team**

A suggestion around this mechanism of sharing data, could be the creation of an internally coordinated by the Greek government platform, where all the Greek public administrations can access and finding solutions around known threats. It can be the storing place of a database which will be slowly build with the help of the CSIRTs that operate in Greece and the entire world too. The constant update of this database could prevent alteration of existing threats or their elevation into more severe ones.

Last, using the public administrations network which already brings all the bodies together, can be the point of contact when something new happens. Either it is a solution behind a threat or if it is a new virus that hit a big organization in the UK, as for instance. The public administration then will also feel safe in a larger group of bodies and fell also that they contribute to the general good behind the Greek cybersecurity posture.

5.9 Summary

To conclude, in this dissertation, an 8step guide is suggested. It is split into 3 phases with phase having some of those steps. To sum-up, the 1st phase of implementation of this guide consists of the 1st step of preparing the ground, the 2nd step of Having what is needed, and the 3rd step of Knowing how to respond. The 2nd phase of implementation of the suggested guide consists of the 4th step of securing everything, the 5th step of hardening the physical protection mechanisms and the 6th step of backups. Last, the 3rd phase of implementation consists of the 7th step of reaching the sky and the 8th step of sharing the knowledge which both are optional. The above steps can be better explained in the below diagram.

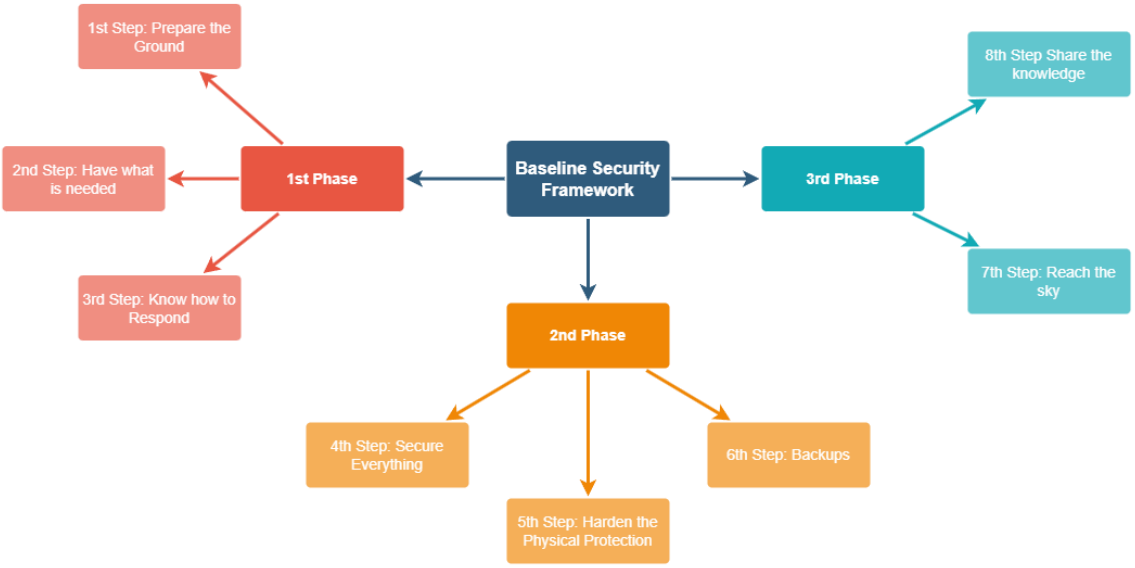

1st Step: Prepare the Ground
8th Step Share the knowledge
2nd Step: Have what is needed
1st Phase
Baseline Security Framework
3rd Phase
7th Step: Reach the sky
3rd Step: Know how to Respond
2nd Phase
4th Step: Secure Everything
6th Step: Backups
5th Step: Harden the Physical Protection

Figure 13: Baseline Security Framework

6 Implementation of the suggested framework

Each organization and public administrative body have in their disposal a huge list of security frameworks to choose and use for their needs. If a public administrative body choses the suggested Baseline Security Framework that is provided in this dissertation, it remains into their capabilities to perform all the steps as they like. The order plays an important role as the needs of the Greek public administrations focus on specific security points, but this does not restrict them to do so.

The phases are there to coordinate the overall implementation and to help controlling the actions by the responsible personnel. Within each phase, the steps can be split into many custom sub-steps that the public administration can choose to create as not everything is as easy as it seems. Each step might hide obstructive points to the general completion of it, which the body comes to solve by itself.

If some other security framework is already in use and the public administration chooses to alter its approach to a way that follows the suggestion in this dissertation, it is free to do so or result in a combination of both. This baseline security framework can be also used as supportive mechanism in the strengthening of the security posture of the organization. To the extend if this, the public administration can choose some steps that it has not yet performed that sound appealing and believe that can help in the security and implement them separately.

Furthermore, the steps are there as a general stepping point of choosing the path into securing a specific part of the organization and can be user partially. By implementing a step of the framework, the public administration might realize that it first needs to perform other actions that will be the starting point in implemented the particular step. For that, the administration must well coordinate its approach which decide how to act. This is something that cannot be explained within this dissertation as it is fully customed to the needs of each organization.

6.1 Possible scenarios

Let’s assume that the public administration has decided to follow the steps of the suggested framework, but the implementation of the chosen steps has not completed, and the body is under cyber-attack. What will then happen? Or what if the implementation is completed but incorrectly and insecurely completed? Will the public administration not be exposed to threats? At this point we can examine some possible scenarios that cover potential issues that will be created while the framework is or has been implemented.

6.1.1 Scenario 1

Scenario Name

A public administration other than ours, was recently under cyber-attack and the attacker managed to steal sensitive information of citizens.

Results

1. Citizens were angry not knowing which of their data was stolen.
2. The public administration body does not know how to recover the lost data and is facing legal penalties.
3. The Greek Government is in the difficult position of being tagged as insecure.

Summary

Such an attack could be the result of many things. Could be the result of an employee opening a phishing email from the organizations computer, letting this way the attacker infiltrate the network of the public administration. Could be the old operating system that is used in some machine in the public administration with many known open vulnerability points. Or could just be the unauthorized access of someone inside the premises of the public administration’s server room.

But just mentioning only few of the possible explanations, we can understand that the public administration had not implemented any security protection mechanism or had not correctly implemented one. The public administration body was lacking awareness training of the personnel and especially around the matter of phishing emails, was not keeping the systems up to date, and did not perform enough physical security protection actions. All those could have been prevented if the body had followed just some easy steps of the suggested framework.

Now the personnel of the public administration do not have a way to retrieve the data that has been lost and need to face the financial penalties which are the result of not following the GDPR. If the backup was made recently, then there is a chance to retrieve some lost data, but the damage is already done. By the penalty from GDPR it is unsure if the public administration will be able to repay the full price and not result into firing of personnel, decrease the salaries or other measures. For their good luck, the Greek government must coordinate the recovery method and reinforce the defenses in the public administration's behalf but still the prestige of not being secure will be there.

If one the other hand, the suggested framework had been followed, then the potential human error would have prevented since the employee would have receive relevant training around security matters like phishing emails and how to protect from them. Also, if the systems were up to date, then the vulnerabilities would be less or at least the vulnerability that the attacker used, would not be there. These protective measures are easy tasks for a public administration body to preform and are of course included in the steps of the suggested framework.

Comments

Small implementations of the suggested steps can prevent threats that might end up as catastrophic to the public administration. Everything needs to be at a good level of security in order for the organization to be feeling safe, unlike the situation of the first scenario.

6.1.2 Scenario 2

Scenario Name

Our public administration employees of the department of IT noticed some weird traffic flowing through the network. After a small investigation, they found out that an employee whose contract was for limited time, allowed the connection with an outside system and was manipulating documents that were crucial to the administration.

Results

1. Important information was leaked.
2. The security posture of the public administration was lower than expected.

Summary

Even though the public administration had implemented some defensive mechanisms against cyber threats, there was some open hole in the systems that allowed the malicious connection. When the IT personnel noticed the activity immediately informed their supervisor who then fired attacker and issued legal restrictions to him. Then the attacker's computer and devices were confiscated for further examination. Then procedures such isolating the system to a sandbox were performed in order to identify the origin of the attack, and then decide how to recover from the attack.

All those steps only cover the aftermath of the attack, with the damage already been done to the organization. But should happen so that the public administration never gets similar attack from the inside? First order of business is to re-implement each step of the suggested framework. Then the vulnerabilities will be detected and patched. The IT administrators will evaluate the permissions that are given to the employees of the public administration and categorize them based on their needs and not based on the easiest way to grand them. Then possibly some backlisting of websites, software and applications will be made resulting into the restriction of access to the Internet. Backups will be considered in more frequent basis and hardening procedures of the physical security will be done immediately. If the last backup was made recently then the recovery of the lost data will be good enough. Last, the DRP of the administration will be reconsidered and hardened, while also the public administration might offer further awareness training to the employees.

If the previously mentioned procedures were followed while the cybersecurity framework was first implemented, then the attack might have been prevented or at least caught earlier decreasing this way to extend of the damage that it caused. When dealing with cybersecurity, patience needs to be the key to the success. No organization can become secure from one day to the next, but slowly and steadily, its security posture will increase.

Comments

Now the public administration will have a more secure environment for both the systems it is using and the working area of the employees with them feeling even safer. In the future, the knowledge that the administration gained around this particular attack, can be shared with other public administrations around Greece and hopefully never happen again.

7 Conclusions

The field around cybersecurity and its defensive mechanisms will always be a very interesting and intriguing point in the study of the Internet world. The use of new systems, applications, devices, methods, and techniques will change the threat landscape day by day. Nobody can be sure of how it will be in the next years, months or even weeks. The changes occur very frequently and the ongoing process of securing the infrastructures will never stop. In this dissertation, the reader can understand the basic terminology that constructs the cybersecurity field with emphasis in the ways of protecting it in the particular example of the Greek public administrations. Their needs constructed the baseline security framework that is suggested and stands as an important part of the security hardening of them.

For achieving the completion of the suggested baseline security framework, known methods of protective mechanism were taken into consideration, but were modified into the appropriate custom approach for the Greek public administration. The combination of existing protections that are currently used and the missing points in the structure of the public administrations, were the key to combine the suggested implementation.

As mentioned before, the suggested framework cannot be used at this stage. It requires a solid testing and official work to be done by an authorized team so it can be offered to the public. But it can always be the point of brainstorming when a Greek public administration or a small company wants to elevate their security posture and find new defensive mechanisms against the aggressive threat landscape of the Internet world. To conclude, the recognition of the fact that no systems is completely secure, makes us understand that we need to do our best to achieve the highest degree of security before we fall into the trap of a cyber-attack. The coordination of all the parts of an organization with the current known defensive mechanisms will be the key to success.

8 Bibliography

1. *Cyber Defense & Response—Who We Are | Cyderes*. (n.d.). Retrieved July 10, 2022, from https://www.cyderes.com/company/

2. Team, C. (2021, August 18). *What is The CIA TRIAD & its Importance for Cybersecurity*. Website Security Store. https://websitesecuritystore.com/blog/what-is-the-cia-triad/

3. Editor, C. C. (n.d.). *Cyber Threat—Glossary | CSRC*. Retrieved August 2, 2022, from https://csrc.nist.gov/glossary/term/cyber_threat

4. *ENISA Threat Landscape 2021*. (n.d.). [Report/Study]. ENISA. Retrieved July 12, 2022, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

5. N. Mahalle, P., R. Shinde, G., Dey, N., & Hassanien, A. E. (n.d.). *Security Issues and Privacy Threats in Smart Ubiquitous Computing* (1st ed. 2021). Springer.

6. DaBoss. (2013, March 7). *Hardware Threats*. Computer Knowledge. https://www.cknow.com/cms/vtutor/hardware-threats.html

7. *Hardware Threat Landscape and Good Practice Guide*. (n.d.). [Report/Study]. ENISA. Retrieved August 31, 2022, from https://www.enisa.europa.eu/publications/hardware-threat-landscape

8. *CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)*. (n.d.). Retrieved August 31, 2022, from https://capec.mitre.org/

9. Wireless LAN. (2022). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Wireless_LAN&oldid=1121357118

10. IEEE 802.11. (2022). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=IEEE_802.11&oldid=1125038376

11. *What are Phone Bands (GSM, CDMA) and Why Do They Matter?* (n.d.). Verizon.Com. Retrieved September 1, 2022, from https://www.verizon.com/articles/Smartphones/what-are-phone-bands-and-why-do-they-matter/

12. Miller, J. F. (2013). *Supply Chain Attack Framework and Attack Patterns:* Defense Technical Information Center. https://doi.org/10.21236/ADA610495

13. *The Nation State Actor*. (n.d.). BAE Systems | Cyber Security & Intelligence. Retrieved July 14, 2022, from https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor

14. *Cybercriminals—Definition*. (n.d.). Retrieved July 15, 2022, from https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals

15. *ENISA Threat Landscape 2021.* (n.d.). [Report/Study]. ENISA. Retrieved July 15, 2022, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

16. *NIS Directive*. (n.d.). [Topic]. ENISA. Retrieved July 27, 2022, from https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

17. *CSIRTs by Country—Interactive Map*. (n.d.). [CSIRT Inventory Tool]. ENISA. Retrieved July 27, 2022, from https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map

18. *The EU Cybersecurity Act | Shaping Europe's digital future*. (n.d.). Retrieved July 27, 2022, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

19. Force, J. T. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

20. Computer Security Division, I. T. L. (2016, November 30). *About the RMF - NIST Risk Management Framework | CSRC | CSRC*. CSRC | NIST. https://csrc.nist.gov/Projects/risk-management/about-rmf

21. 14:00-17:00. (n.d.). *ISO/IEC 27005:2018*. ISO. Retrieved August 1, 2022, from https://www.iso.org/standard/75281.html

22. Open Threat Taxonomy. (n.d.). *AuditScripts.Com*. Retrieved August 30, 2022, from https://www.auditscripts.com/free-resources/open-threat-taxonomy/

23. *General Data Protection Regulation (GDPR) – Official Legal Text*. (n.d.). General Data Protection Regulation (GDPR). Retrieved December 3, 2022, from https://gdpr-info.eu/

24. *Tools and Standards for Cyber Threat Intelligence Projects | SANS Institute*. (n.d.). Retrieved July 20, 2022, from https://www.sans.org/white-papers/34375/

25. Panhalkar, T. (2019, December 5). Types of Threat Intelligence. *Infosavvy Security and IT Management Training*. https://info-savvy.com/types-of-threat-intelligence/

26. *ISO 27005 | IT Governance UK*. (n.d.). Retrieved December 3, 2022, from https://itgovernance.co.uk/iso27005

27. Cybersecurity Framework. (2013). *NIST*. https://www.nist.gov/cyberframework

28. Executive Order 13800: Growing and Sustaining the Cybersecurity Workforce. (2017). *NIST*. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800

29. *Essential Eight Maturity Model | Cyber.gov.au*. (n.d.). Retrieved September 14, 2022, from https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

30. *Essential Eight Maturity Model—AlltasksIT*. (2020, September 12). https://alltasks.com.au/essential-eight-maturity-model/

31. View, M., M'Raihi, D., Hoornaert, F., Naccache, D., Bellare, M., & Ranen, O. (2005). *HOTP: An HMAC-Based One-Time Password Algorithm* (Request for Comments RFC 4226). Internet Engineering Task Force. https://doi.org/10.17487/RFC4226

32. Security, C. C. for C. (2020, February 18). *Baseline cyber security controls for small and medium organizations*. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

33. Canadian Centre for Cyber Security [@cybercentre_ca]. (2020, April 23). *The Cyber Centre is working with its partners to keep Canada safe during #COVID19. Today @ciranews launches #CanadianShield—A free DNS service with threat protection enhanced by our data: Https://cyber.gc.ca/en/canadian-shield-sharing-cyber-centres-threat-intelligence-protect-canadians-during-covid-19 https://t.co/0aTcREMIDe* [Tweet]. Twitter. https://twitter.com/cybercentre_ca/status/1253297593590984704

34. *CIS*. (n.d.). CIS. Retrieved November 26, 2022, from https://www.cisecurity.org

35. *CIS Critical Security Controls Implementation Group 1*. (n.d.). CIS. Retrieved November 26, 2022, from https://www.cisecurity.org/controls/implementation-groups/ig1/

36. *Compare United Kingdom, Canada and Australia: EU Cyber Direct*. (n.d.). Horizon. Retrieved October 23, 2022, from https://eucyberdirect.eu/atlas/country/united-kingdom/compare/canada/australia

37. Says, K. (2018, June 28). Cybersecurity Framework—Types, Components and Functions. *Edureka*. https://www.edureka.co/blog/cybersecurity-framework/

38. *Traffic Light Protocol (TLP) Definitions and Usage | CISA*. (n.d.). Retrieved August 23, 2022, from https://www.cisa.gov/tlp

39. Recovery point objective. (n.d.). *Metallic.Io*. Retrieved August 25, 2022, from https://metallic.io/knowledge-center/glossary/recovery-point-objective

40. What is a Disaster Recovery Plan? Definition and Related FAQs. (n.d.). *Druva*. Retrieved August 25, 2022, from https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs/

41. Cassetto, O. (2022, March 8). *Incident Response Plan 101: How to Build One, Templates and Examples*. Exabeam. https://www.exabeam.com/incident-response/incident-response-plan/

42. Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31. https://doi.org/10.1016/j.istr.2005.12.001

43. *NIST Incident Response Plan: Building Your IR Process*. (n.d.). Cynet. Retrieved August 25, 2022, from https://www.cynet.com/incident-response/nist-incident-response/

44. *Ultimate Guide to Cybersecurity Incident Response—TechProspect*. (n.d.). Retrieved September 10, 2022, from https://tech-prospect.com/security/cyber-security/ultimate-guide-to-cybersecurity-incident-response/

45. California, S. of. (n.d.). *Security Policy | CDT*. Retrieved September 10, 2022, from https://cdt.ca.gov/security/policy/

46. *Κυβερνοασφάλεια | Υπουργείο Ψηφιακής Διακυβέρνησης*. (2022, November 24). https://mindigital.gr/dioikisi/kyvernoasfaleia

47. *Myschool*. (n.d.). Retrieved November 1, 2022, from https://myschool.sch.gr/