SECURITY OF INDUSTRIAL & INFORMATION SYSTEMS

By:

PATRICK HOUYOUX LL.M.

SECURITY OF INDUSTRIAL & INFORMATION SYSTEM

THE IT Security encompasses both the security of information and management systems (IT Management Security) and the industrial security or the functionalities of the company or institution.

Industrial Security and IT Management Security follow different rules and industrial security must in any event be given priority because, deprived of its essential functions, an Industrial Company, Hospital, Institution or University may see its damage quantified exorbitantly and in some cases even be forced to cease its activities.

PT SYDECO, ARCHANGEL / SST and SydeCloud products, manufactured in Indonesia, are perfectly adapted to be integrated into a general security policy, acting as major components of industrial security and IT management security for any company or institution.

I propose to start by presenting the question of Industrial Security, how it looks like, how to envisage it and how to make it a success. In a second step, I will deal with the question of the Security of the management system and will end with the question of IT Security in general.

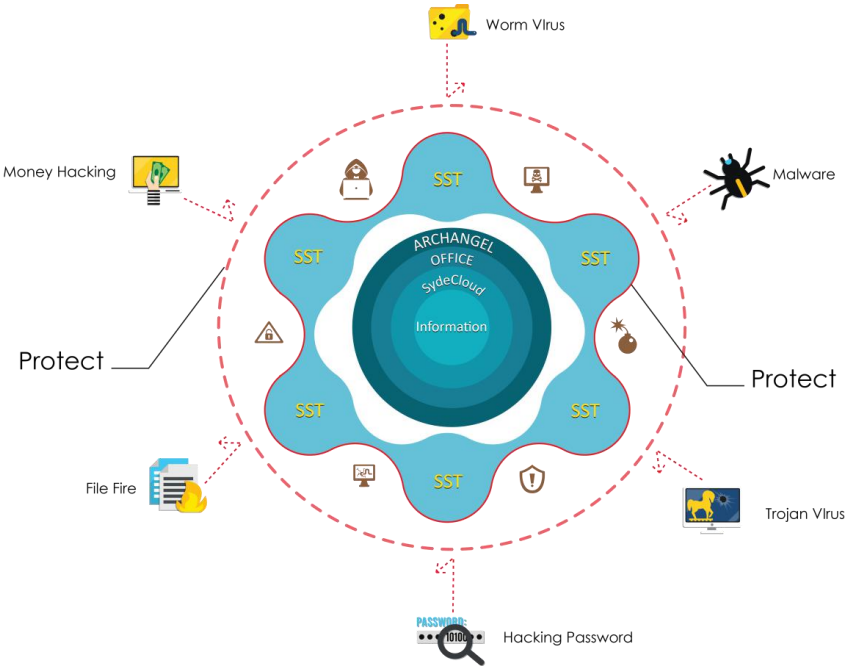

Figure 1 : The outside world is full of danger

PART 1 : INDUSTRIAL SECURITY

As said, the IT Security of the Infrastructure, taken as a whole, encompasses the security of the Information System and the Security of the connected Industrial and/or high-tech equipment (such as for example research laboratory equipment, medical equipment) or that of the functionalities of a company or institution.

The IT Infrastructure is understood as comprising all the operational elements essential for the effective, efficient and proactive use of technology in general, information and data.

The IT Infrastructure is therefore made up of visible and/or physical elements such as computers, servers, personnel, all physical installations including programmable and connected industrial or high-tech equipment. But it is also made up of invisible and/or intangible elements such as networks, data and storage, virtual facilities and software, to which must be added processes, policies, training, security, mobile and virtual functionalities.

IT Infrastructure Security is the set of means, tools, techniques, policies and methods that guarantee:

- that only competent persons or other authorized systems intervene on the system, on the physical or virtual installations and on the functionalities and,

- that only competent persons or other authorized systems have access to the data, whether sensitive or not and,

- the confidentiality, integrity and availability of such data.

The security of industrial and/or high-tech equipment or the security of the functionalities of a company or institution differs from the security of the Information System because it requires the implementation of different means and measures of protection, among which the following can be mentioned:

- Prevention and sensitization of operators and stakeholders to good practices,

- A thorough knowledge of the Industrial Network Infrastructure to detect potential faults (mapping),

- The implementation of a continuous monitoring approach for industrial systems and flows,

- Constant monitoring of threats and vulnerabilities,

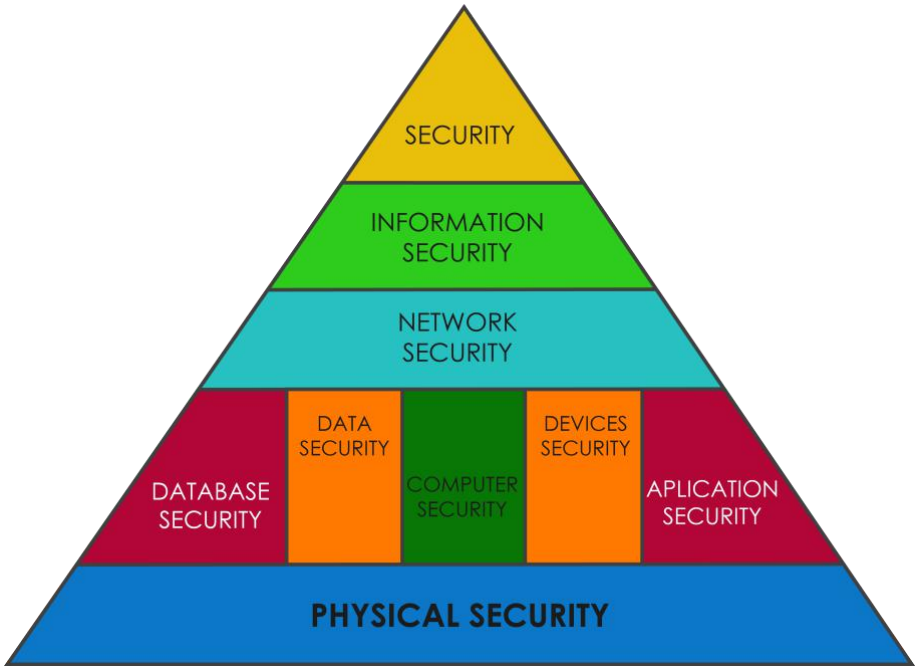

Figure 2: IT Infrastructure

The objective of the security of industrial and/or high-tech equipment or the security of the functionalities of a company or institution is to reduce risk areas without harming business objectives.

Thus, we will use a:

- Physical access control,
- Intrusion detection,
- Use of industrial components and equipment integrating authentication or trade protection systems,
- Updating of supervision software solutions (SCADA) to benefit from the latest developments in safety,

However, there is no point in rushing to these means of protection without first carrying out a risk analysis.

In order to draw up the impact analysis, those affecting the infrastructure and production capacity (more or less long interruption), people (injuries, deaths) and the environment (pollution) must be taken into consideration, without omitting the impact on the national economy.
It is not our intention to reproduce, summarize or paraphrase the new ISA/IEC 62443 standard (series ISA-62443-4-2, *and* ISA/IEC 62443- 3-3) which specifies security capabilities for control system components that provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs) but simply to draw your attention to what seems to me fundamental and especially what are the minimum but indispensable protection steps to be taken to ensure the safety of industrial installations.

For the sake of clarity I will use indifferently the terms institution or company to refer to a company or institution that owns an industrial installation or high-tech equipment. I will also use indifferently the terms assets, device or institutions when speaking about an industrial and/or high-tech equipment.

Risk analysis in the field of industrial and/or high-tech equipment or risk analysis of the functionalities of companies or institutions such as that those active in the Energy, High Tech Industry, Mining, Metro and Railways, Construction, Laboratories, Medical and Paramedical, Data Center, Telecommunications, Research, Banks, Education sectors...can start by drawing up a list of assets to be protected classified according to their order of importance for the activity of the company or institution or the country, followed by an analysis of the impact in the event of a loss. But it is usually said that this analysis can also start by drawing up a table of risks which will be sorted according to their level of dangerousness and the probability of their occurrence.

For me, the probability aspect of the occurrence of a cyber-attack is of secondary importance, even meaningless. Indeed, the consequences of a cyber-attack can be disastrous even if the probability of its occurrence was low. As an example, hadn't we foreseen a disaster scenario for Covid-19 in Africa that didn't happen? Better not to play Russian roulette.

But in any case, the parameters to which most attention should be paid are the degree of importance of the assets (installations) to be protected for the company's activity and the consequences of a cyber-attack depending on the aim (threat) of the cyber-criminal, who may be seeking easy gain or acting with the simple

intention of causing harm, or may still be acting in the context of industrial espionage.

Let's not forget that we are dealing with industrial protection and not with the protection of the information system of the company that has these programmable devices. Therefore, except in the case of devices whose purpose is to collect information (I am thinking here of programmable and connected medical devices or those used for research purposes), we should not concern ourselves with the confidentiality, integrity and availability of the data collected.

The establishments that have such devices can be classified into three categories according to the place these devices occupy in the company's activity.

Thus we will have in:

CLASS 1: Companies which consist of only one department with a single programmable installation or which have several departments with such installations which are interconnected and for which this installation or these installations constitute(s) the main activity.

CLASS 2: Companies which comprise more than one department and whose connected and/or programmable installations are not interconnected with each other but for which such facilities constitute the principal activity.

CLASS 3: Companies that have one or more departments with facilities that may or may not be interconnected, but where these facilities do not constitute the main activity.

The danger of a cyber-attack, depending on the goal pursued by the cyber-criminal, can also be either (1) destruction of the installation or encryption of the data that it has collected if the cyber attacker is pursuing easy gain or simply intends to cause harm, (2) deprogramming of the installation if the cyber attacker is pursuing the same goal, and (3) theft of the collected data if the cyber attacker is in the business of industrial espionage.

The impact on the company can then be considered as being:

- **MAJOR** if the company is class 1 regardless of the purpose of the cyber-attacker,

- **MAJOR** if the company is class 2 and the cyber-attacker is pursuing easy money or industrial espionage goal,

- **MEDIUM** if the company is class 2 and if the result of the attack is the deprogramming of an installation,

- **MEDIUM** if the company is class 3 and the goal of the cyber attacker is the destruction of the installation and,

- **MINOR** if the company is class 3 and the goal of the cyber-attacker results in deprogramming or industrial espionage.

It is therefore obvious that the greater the impact on the company, the more serious should be the protection of its installations.

The next quadrant represents the need for protection of an installation with respect to the threat it may face where the **RED** color indicates that the installation requires the maximum security, the **ORANGE** color indicates the need of a medium level of security and the **GREEN** color indicates that the installation requires a standard security.

Installation / Threat	Deprogramming	Destruction Ransomware	Espionage
CLASS 1			
CLASS 2			
CLASS 3			

Figure 3: Quadrant of the impact level of an attack

This quadrant is very useful to determine the type of protection the installation needs to counter a cyber-attack.

In order to determine the type of protection that the installation to be protected needs, we must situate it in its environment and analyze the type of interconnections that exist or are envisaged for it.

Indeed, interconnections are an important source of vulnerabilities and, before interconnecting two networks, it is imperative to carefully consider the risks that may result.
There are several types of interconnections.

Let us consider for the purposes of this presentation that the installation to be protected is part of a network that we will call "Industrial Network". It is quite obvious that this Industrial Network may include one or more installations that each requires protection against cyber-attacks.

The installation can therefore be interconnected either in the same network to another installation, or with a public network such as the Internet or telephony, or with an information and management system or another industrial network of a different class.

The fundamental rule to be observed in interconnections between different networks is PARTITIONING, regardless of the type of network to which the industrial network must be interconnected.

But this partitioning must be unidirectional in the case of an installation of class 1 from the industrial system to any other network, including another industrial network of the same company or institution, whether of lower class or of the same class.

This partitioning must also be unidirectional in the case of an installation of class 2 from the industrial system to a public network or to another industrial network of class 3.

The partitioning of the industrial network of Class 3 must not be unidirectional.

The best way to partition a network is to protect it with a firewall, but not with just any firewall.

This firewall must in fact be able to withstand increasingly sophisticated attacks, even those carried out from a quantum computer, and must be able to protect the

data collected by the installation if it has this effect, and above all it must be unidirectional when it comes to protecting an installation of class 1 or 2.

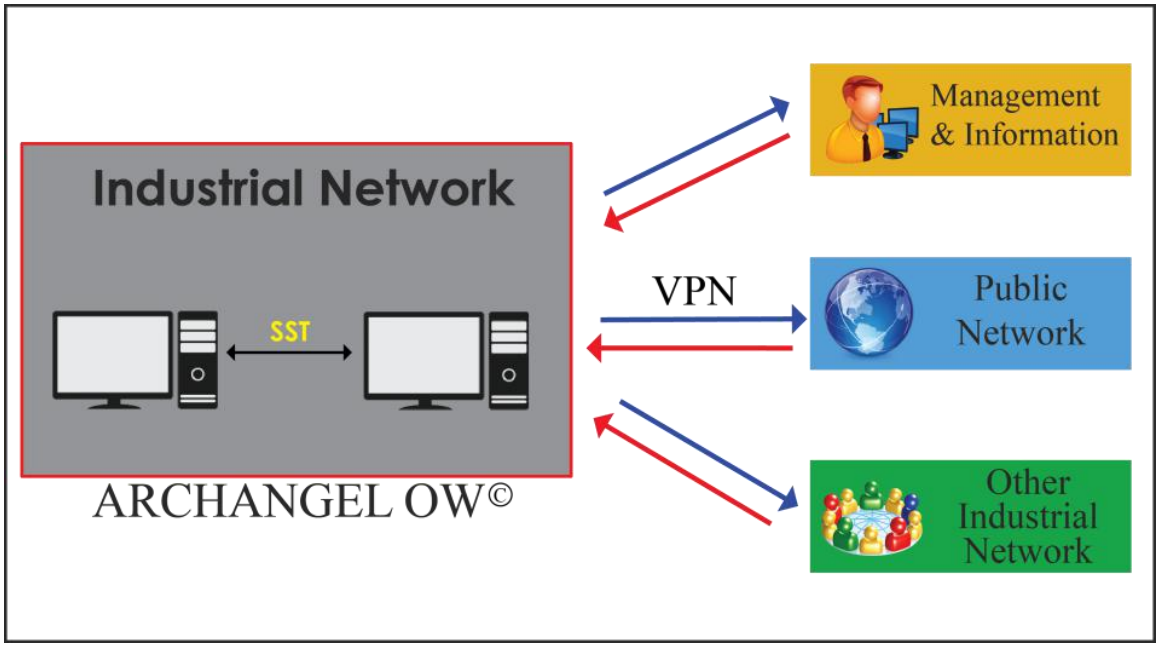

Figure 4: Interconnection of Installation Class 1

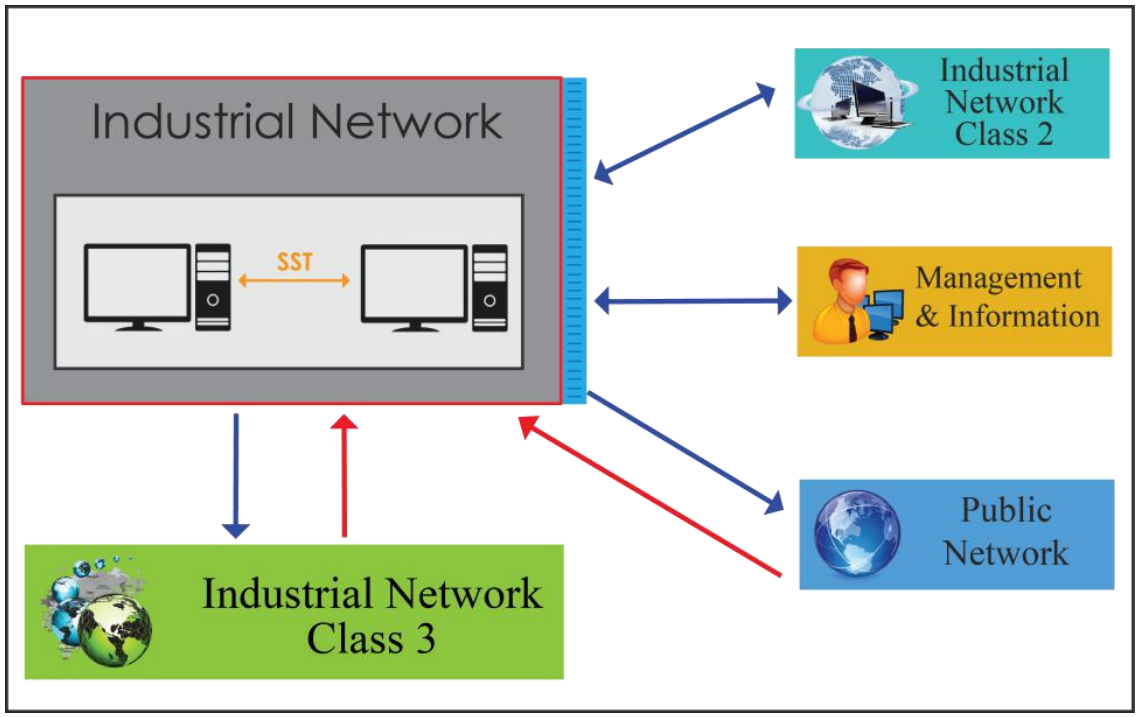

Figure 5: Interconnection of Installation Class 2

The system developed by PT SYDECO, **ARCHANGEL OW©**, meets all these requirements in that it allows the unidirectional and is completely impermeable to the attacks led even by a quantum computer because its protection and that which it provides are not based on theory of numbers.

For multi-directional protection, **ARCHANGEL©** will be chosen.

Within the same industrial network, each installation must be protected by a system that is not an anti-virus that is incompatible with programmable High-Tech devices, but by a highly qualified protection system such as **SST©**, Secure System of Transmission, another product of PT SYDECO, that scan then translate into alien language any data, not using any key, and convey them in the form of waves.

We therefore highly recommend protecting the industrial network within the company or institution by means of the unidirectional firewall ARCHANGEL OW© or ARCHANGEL© as the case may be and, within the same network, to protect each connection between installations by means of SST©.

We also advise not to connect a class 1 network, which requires the greatest vigilance, with a public network except, in case of absolute necessity using the **VPN**, such as the one created by ARCHANGEL and which does not call for the intervention of any third party.

Engineering stations that contain software for configuring industrial equipment and for programming High-Tech machines or even source codes, are vulnerable points and must be totally isolated from both industrial installations and information systems. This isolation will be done by means of unidirectional firewall in the direction starting from the stations with a connection protected by SST. They are indeed an open door to the control of the system by hackers.

These engineering stations are part of **class 1** in our company classification system.

RECOMMENDATIONS

FIRST FOR ALL CLASSES:

- Create a map of the industrial system by making inventory of the installations,

- Verify the class of the company and determine the protection required by its installations according to the class to which it belongs,
- Create a map of the connections and interconnections of the machines to be protected. This is optional for companies belonging to class 3.

- Establish a continuity plan and define preventive measures,

AFTER INSTALLING FIREWALLS:

- Manage the access of users which must be limited to their presence in the premises,
- Create strong passwords and protect them with SST,
- Hierarchize access to different accounts and programs,
- Do not allow any file sharing that would use third party technology such as GOOGLE, and other GAFAM,
- Process a daily backup of the data and keep it in a specially dedicated server for this purpose itself protected,
- Perform a regular safety audit of the installation,

These recommendation constitute a minimum. They have to be strictly followed by companies belonging to classes 1 and 2.

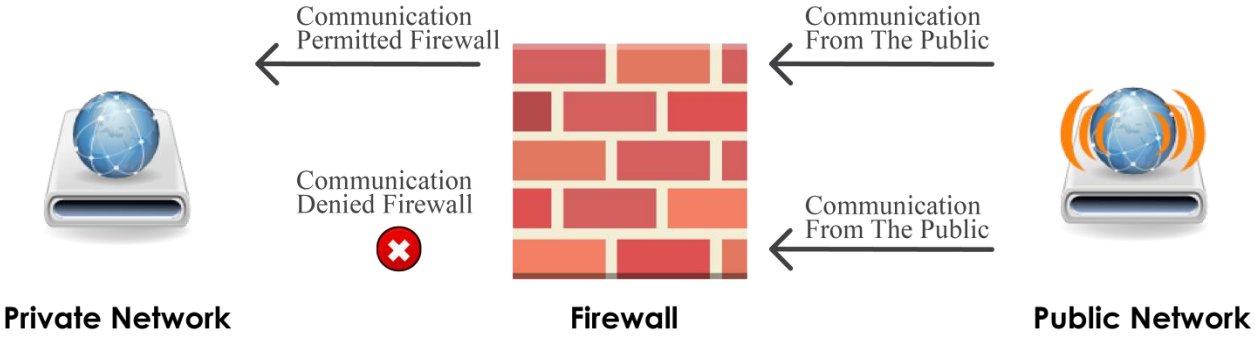

Figure 6 : Protection from the outside world

PART 2 : INFORMATION SYSTEM SECURITY

The information system of a company consists of all the data and the hardware and software resources which enable these data to be stored or conveyed. It is an essential asset of the company or of the institution. The information system must be protected against any degradation, theft or loss of its data and that of its customers or partners which would lead to the degradation of the institution or company's brand image.
Not to mention the disruption in its operation and possible financial losses.

The current trend is to consider IT security as one of the criteria for assessing a company when it comes to choosing a partner.
We can then talk about cyber security rating of the company or institution which will be added to the control of its solidity and the quality of its services to determine the level of confidence that can be placed in it.

It is therefore essential for a commercial, industrial or institutional establishment to protect its information system, especially when it is accessible by a third party who may be a teleworker, a client, a partner, a citizen or student.

I - AN INFORMATION SYSTEM MUST BE SECURE.

Then logically come the following 4 questions:

- What is "to be secure"?
- Against what should it be secured?
- What are the causes of insecurity?
- How to secure it?

And once we find the answers to these questions, we can develop the best way to protect the information system keeping in mind the fact that there is no one-size-fits-all solution. Each information system requires its own protection, taking into account its own causes of insecurity.

This is what our next developments will focus on.

A) WHAT IS "TO BE SECURE"?

It can be said that an information system is secure when it fully guarantees 1) Confidentiality, 2) integrity and 3) the availability of the data or information it processes or stores.

1) CONFIDENTIALITY occurs when data or information cannot be disclosed without the authorization of the only person(s) who has (have) the authority.

2) INTEGRITY occurs when data or information cannot be altered or modified without the authorization of the only person(s) who has (have) the authority to do so.

3) There is AVAILABILITY when the data or information is at any time and without delay accessible by the only person(s) who has (have) the power to access it.

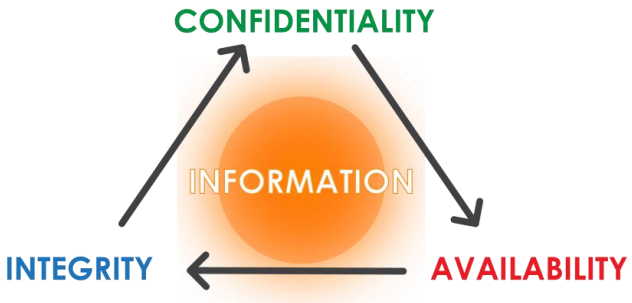

Figure 7: CIA: Confidentiality, Integrity, and Availability

Some authors add to these 3 fundamental criteria two others which are the authentication of users by an access control and the non-repudiation of transactions by the person who is the originator.

Personally I cannot agree to the addition of these two conditions because they are in fact the consequences or requirements and not a criterion of the security characteristics: User authentication is the condition that must be fulfilled by the only person(s) who has (have) access to information. User authentication is in fact part of the security requirements to be put in place so that the only authorized person has access to information. The same applies to non-repudiation, which does not concern the security of the information system but that of transactions

But the security of an information system is not limited to that of its data or information. In order for these data or information to be always confidential, not

altered and available, it is necessary that the devices that process them or keep them or convey them are themselves protected against any risk of attack (threats) or loss (accidental or voluntary).

B) AGAINST WHAT SHOULD IT BE SECURED?

The answer to this question can be found in the very definition of computer security that we have just given: The information system must be protected against any threat or attack against confidentiality, the integrity or availability of the information and data it processes, stores or convey.

In computer security, a **threat** is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either "intentional" or "accidental" or otherwise a circumstance, capability, action, or event. (Wikipedia).
An **attack** is the work of a hacker who can, as we have seen for the industrial system, pursue a goal of quick gains (ransomware, sale of stolen data, etc.) or, being animated by an intention to harm, destroy, render ineffective the system or take control of it. It can also, for espionage purposes, steal information

But the system, in order to fulfil its function properly, must also be protected against any interruption of operation that would occur following a power failure, or a natural event such as flood, earthquake or volcanic eruption.

C) WHAT ARE THE CAUSES OF INSECURITY

These causes are to be searched in both the human side (the users) and the one of the protection tools used or to be used. They can also been found in the environment where the information system is located.

On the human side:

The cause may result from the user’s lack of knowledge of the security means in place or, even though he knows these systems, from his lack of knowledge of their functionality.

It may also result from the carelessness or dishonesty of users or access to the information system by a person who is not authorized to do so.

This is why a security policy must be drawn up and made known to all staff.

On the material side:

The insecurity of the information system can also result from the absence of firewalls or anti-virus, from the absence of their updating or from their insufficiency or inadequacy or the absence of protection when data are in moved.

This is why a global architecture of the IT infrastructure has to be developed

On the environment side:

It may result from a local power failure or internal network failure, flooding, or an act of nature and whose risk is linked to the location of the establishment.

This will be part of the security policy as it will be the duty of the dedicated staff to monitor these elements.

D) HOW TO SECURE IT?

The information system must therefore be secure to respond effectively to threats that may come from these different sources.

We have just seen that the response to be given will vary depending on whether the vulnerability turns out to be behavioral, environmental or in terms of data protection.

The study of how one can protect the information system from sources of insecurity from the human or environmental side will be the subject of a separate examination because it concerns the security of both the information system and that of the industrial system. This study will lead to the development of a security policy which is in fact a document that contains a set of rules relating to what must be done or what must be avoided by the staff in order to guarantee the security of the IT infrastructure of the establishment. This security policy must be known by all the actors involved and must regularly, at least once a year, be reviewed and the appropriate case readjusted to deal with new situations.

We are now going to explore how we can protect the information system from deliberate attacks against the data it processes, guards or carries.

And for that, the best is to proceed to the development of an architecture of the information system of the establishment, development which cannot be done without knowing beforehand the mission or the object of the establishment and without having drawn up a detailed inventory of all the elements which form part of this infrastructure, having classified them according to the importance which they have with regard to the mission or the object of the establishment

This architecture of the information system will allow the establishment to take concrete measures to secure its data and IT equipment.

The different stages of the creation of an IT Architecture

The development of an IT architecture is in fact the final step in a reflection, a work of research and analysis that covers the whole institution without being limited to the information system itself, which is only a part of a whole.

1. PREREQUISITE

Thus, in a first stage that I call the PREREQUISITE, first we will focus on the mission, the object and the core business of the establishment in order to obtain a clear and precise image of it.

This approach will allow us to identify the IT infrastructure needs of the institution and then the security needs required by this information system for the establishment to fulfil its mission. It will also allow us later to identify within this infrastructure those elements that require a higher degree of security.

This approach proceeds from the same spirit of classification of companies such as we explained it in the first part of this study for the industrial network, except that this time, it is no longer a question of classifying the institution but well the parts of its IT infrastructure according to their security needs to allow the establishment to fulfill its mission or its core business.

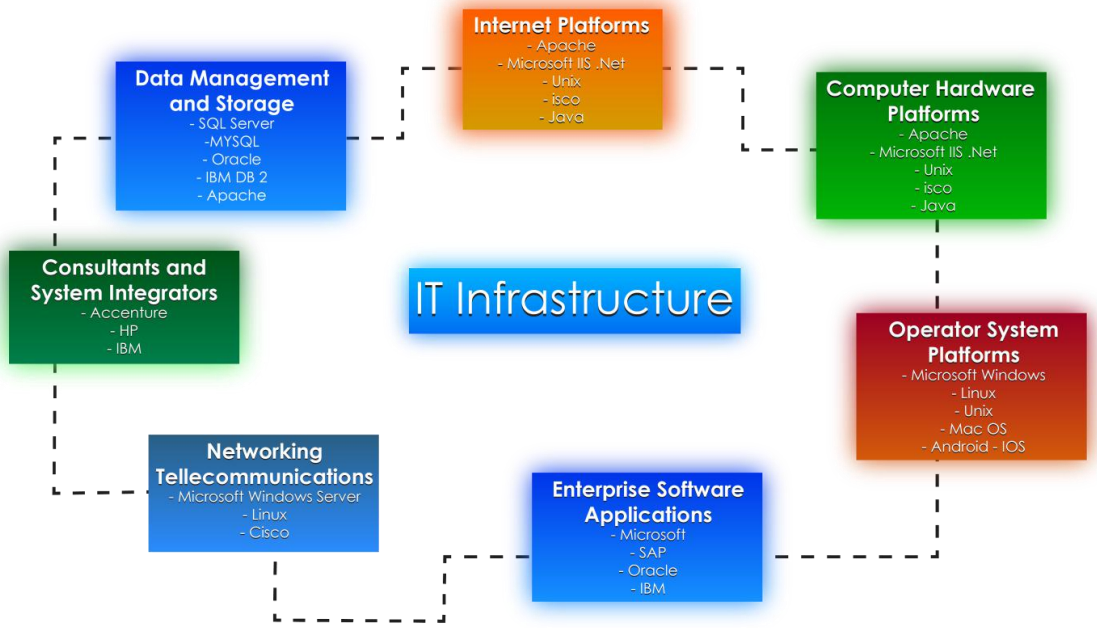

Figure 8: Analyze and inventory

Then, comes the time to draw up an INVENTORY of what exists or what is necessary in terms of:

- Computer equipment,
- Energy needs, connections, interconnections

This inventory will, in the light of what we have learned when studying the infrastructure needs and the degree of security of its components, serve as a basis for researching threats, vulnerabilities and security needs.

2. SEARCH FOR VULNERABILITIES, THREATS AND SECURITY NEEDS,

This research constitutes the second step in our approach to create a security policy for the IT infrastructure of the establishment.

Based on the knowledge that we have acquired from the examination of the mission, the objectives of the establishment as well as what it has or what it must acquire in IT equipment to fulfill its mission and the importance of the change of the external conditions to which it can be subjected, we can seek and identify the threats which it will have to face, the vulnerabilities of its system and seek the

protective measures that it will be necessary to take in order to alleviate these threats.

These protective measures will vary not according to any degree of risk, but depending on the importance of any individual element of the IT infrastructure so that the establishment can achieve its objectives, so that its core business is never disrupted by any failure or attack.

The objective of this research is to prevent possible failures (due to the staff or to external elements) and to prevent potential attacks which could be carried out by a person with an intention to harm, or who pursues a goal of quick gains or who acts in the context of a espionage enterprise.

This research also aims to ensure maximum protection of the digital assets (data) of the establishment.

This research will focus on each element individually taken and which linked to each other, constitute the IT infrastructure of the establishment. I am thinking here of:

- Any element which is used for:
    - Processing data / information (desktop computers, laptops, etc.),
    - Safeguarding data / information (data servers, backup, etc.),
    - Safeguarding applications, operating systems…,

- Any element involved in:
    - Transfer of data, information, via cable or Wi-Fi, internally (Wi-Fi, cables, router, switch, emailing and central telephone, servers, etc.),
    - Transfer of data, information, cable or Wi-Fi, to or from the establishment (Wi-Fi, cables, router, switch, emailing and central telephone, servers, etc.),

- Any element in which the physical infrastructure of the establishment is located (secure places and those open to the public, supply to a source of energy, internet, telephone, air conditioning, etc.) and to which can be added the geophysical environment of the establishment and finally,

- Staff members directly concerned by:
    - Processing of data,
    - Network maintenance,

- Equipment maintenance in general,
- Maintenance of the premises

It is therefore possible to draw up a table in which, just as we did it for industrial network, we will divide, in 3 groups or classes, the elements of IT infrastructure taking into account the importance that they take in the accomplishment of the mission / object or core business of the establishment.

But, as what is of primordial importance for one sector of activity is not necessarily for another, we will thus distribute these 3 classes according to the type of activity of the establishment.

I'm going to create 3 main activity groups here.

- GROUP A: In the first group we will have the establishments for which payment security is primordial (Banks, Finances, large distribution, payment organizations…),

- GROUP B: In the second group, we will include the establishments for which professional secrecy is essential (Medical, Legal, advice, etc.),

- GROUP C: In the third group will appear the establishments / institutions whose object itself and / or the pursuit of it require absolute secrecy (Military, Armament, Government, research centers ...).

The elements that make up the infrastructure can be distributed according to their usefulness as we have just seen: Process, safeguarding and Backup - transfer - environment - staff.

In the information system, the goal pursued by the cyber-attacker is not as important that the impact of its attack on the mission of the establishment. But it is always good to know that the danger of a cyber-attack, depending on the goal pursued by the cyber-criminal, can also be either (1) destruction of the installation, encryption of the data that it has collected or theft of sensitive data if the cyber attacker is pursuing easy gain or simply intends to cause harm, (2) deprogramming of the installation if the cyber attacker is pursuing the same goal, and (3) theft of the collected data if the cyber attacker is in the business of industrial espionage.

The impact on the mission of the establishment can then be considered as being:

- **MAJOR** if the establishment is in group A and if the cyber-attacker pursues an easy gain by attacking the transfers, the process and the backup of the data specific to financial transactions,
- **MAJOR** if the establishment is in group B, regardless of the intention of the cyber attacker who is attacking the safeguarding of data and their transfer,

- **MAJOR** if the establishment is in group C, without taking into account the intention of the cyber attacker who is attacking the safeguarding of data and their transfer and if the origin of the threat is in the environment or the staff,

- **MEDIUM** if the establishment is in group A and if the origin of the threat is to be sought in the staff,

- **MEDIUM** if the establishment is in group B and if the origin of the threat is to be sought in the staff,

- **MINOR** if the establishment belongs to groups A and B and if the origin of the threats is in the environment.

It is therefore obvious that the greater the impact on the mission, object or core business of the establishment, the more serious should be the protection of the elements of its installations that directly intervene in its accomplishment.

The next quadrant represents the need for protection of an installation with respect to the threat it may face where the **RED** color indicates that the installation requires the maximum security, the **ORANGE** color indicates the need of a medium level of security and the **GREEN** color indicates that the installation requires a standard security.

Establishment / Threat	Process and Safeguard	Transfer	Staff	Environment
GROUP A	RED	RED	ORANGE	GREEN
GROUP B	RED	RED	ORANGE	GREEN
GROUP C	RED	RED	RED	RED

Figure 9: Quadrant of the impact level of an attack

This quadrant is very useful to determining the type of protection that elements of the installation need to counter a cyber-attack (from the outside), just an attack (from the inside) or a failure in its availability.

However, looking at the predominant red color, one can imagine that high protection is required for all the components of an information system, whether at the level of data processing, their storage, their backup or their transfer regardless to the very purpose of the establishment.

Imagining that we would not be entirely wrong because indeed, given its role and its importance in the activity of the establishment, the information system requires very high protection.

Pushing our thinking further, we realize that in fact, the degree of protection required by the elements of the system is not only a function of the category to which the activity belongs, but also varies depending on the type of activity actually carried out there.

There is, however, one constant: for any sector of activity, safeguarding data is of primordial importance as are all the components of the infrastructure that are affected by it.

We will also assume that all components in contact with the outside world and those close to them, even if they are not connected, constitute vulnerabilities.

To protect such vulnerabilities, the establishment has at its disposal:

- The firewall either at the level of the establishment or at the level of a section thereof or just assigned to certain devices,
- Antivirus software,
- The possibility to isolate,
- Data protection,
- Protection with VPN.

All of this will need to be taken into account when developing the information system architecture.

Finally, to prepare the architecture of the information system, we will only take into account threats from the outside world. Those that emanate from inside the establishment and from the environment are subject to security policy.

II - ARCHITECTURE OF THE INFORMATION SYSTEM

The degree of protection that the elements of the information system need therefore varies according to the category to which the activity belongs. But it also varies according to the type of activity which is actually carried out there and according to the material or immaterial means which are used to exercise this activity. There can therefore not be a single type of architecture to protect the IT infrastructure of all establishments. We will therefore present an architectural project for each of the categories of activities that we have selected.

1 - ESTABLISHMENTS IN THE FIELD OF FINANCE

For this type of activity, it is essential to preserve the devices used to process data, protect and save it and to transfer data that does not belong to the payment activity.

A) Payment activity

In fact, in the payment activity, what must be totally protected are the sensitive data that a customer sends to the establishment and the authentication of the originator, which require the development of tools that are foreign to the information system of the company.

Authentication is only done using passwords. The data is protected by encryption. For transactions made from a mobile phone, the data of the phone used by the customer is also part of the authentication.

We therefore understand why there is so much fraud in the remote payment system.

It would be different if the financial institution changed its working method. The institution could use SydCloud© and include its payment system in it. Thus, the customer, whether he uses his mobile device or a computer, has no application on his device which is not and cannot be secured. The customer who wants to proceed to a financial transaction will then be directly connected to the SydeCloud of his financial organization to which he will have exclusive access by VPN with the consequence that his sensitive data and their transfer will be protected by the protection of the computer system of the financial institution.

It is a completely new system developed by the Indonesian company PT SYDECO that guarantees total security in remote payment.

Thus, apart from the transfer of money, in the activity of the establishment, it will be necessary to distinguish the material allocated to the activities directly related to the data processing, their conservation and their transfer from that dedicated to activities relating to customer service or of the general administration.

Figure 10: Payment system without any application in the user's device

B) General mission

The equipment used by the establishment to pursue its activities and which is limited to general administration or customer service can be protected globally by a simple firewall and individually by antivirus programs.

In addition, there can be no connection between workstations to prevent further spread of contamination. By connecting each device to the Archangel firewall, all data emanating from one device to another is filtered by the third firewall in the system. (Archangel contains three firewalls, a dynamic router, a honeypot and four intelligent agents connected to an electronic brain).

It will also be necessary to ensure that every member of the staff respects the security police.

This space will also host its own data center which will be protected by an individual firewall of the type Archangel A4 (see below) and its own online file sharing system as we will also see later.

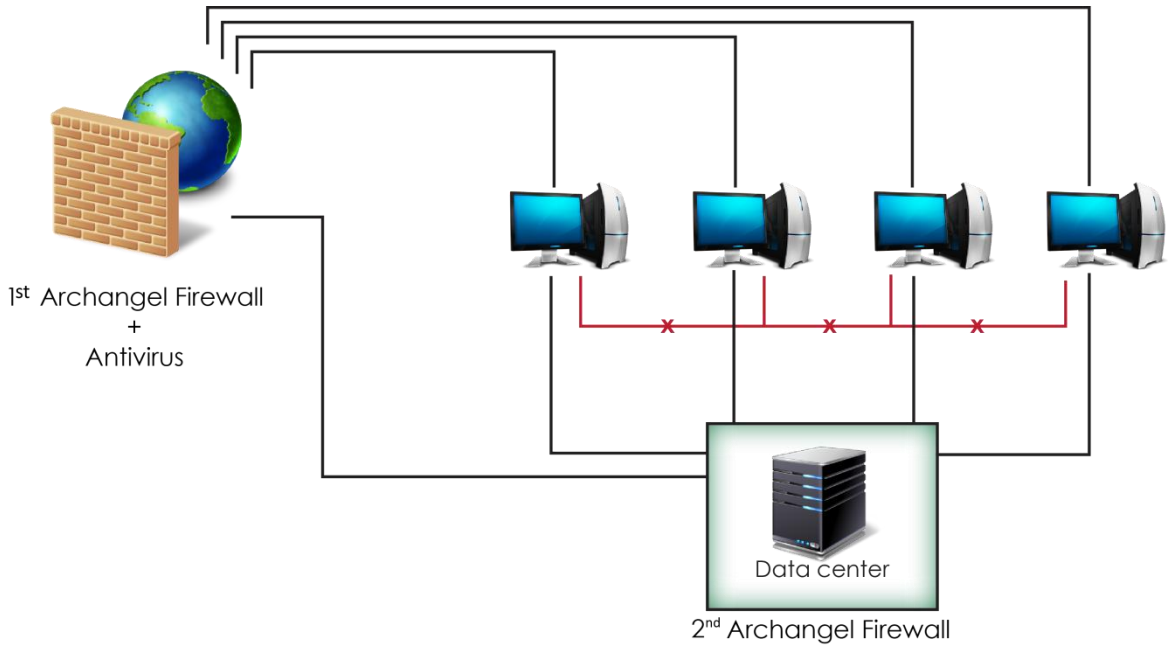

Figure 11: IT Infrastructure for the department of administration, service clientele

C) Data processing department

The equipment used to create and manage the financial data as well as the staff in charge of their processing must be isolated from the rest of the equipment and staff of the establishment, both from the point of view of the workplace and of their connections.

This space must be protected by its own firewall and each device must be protected by an antivirus.

In addition, with the exception of what will be said for its data center and for the online file sharing, this space will not be accessible from the outside, including the space reserved for the general administration, in the sense that only communications leaving this space will be possible. For this, we recommend using the Archangel OW firewall.

This space will also host its own data center which will be protected by an individual firewall of the type Archangel A4 (see below) and its own online file sharing system as we will also see later.

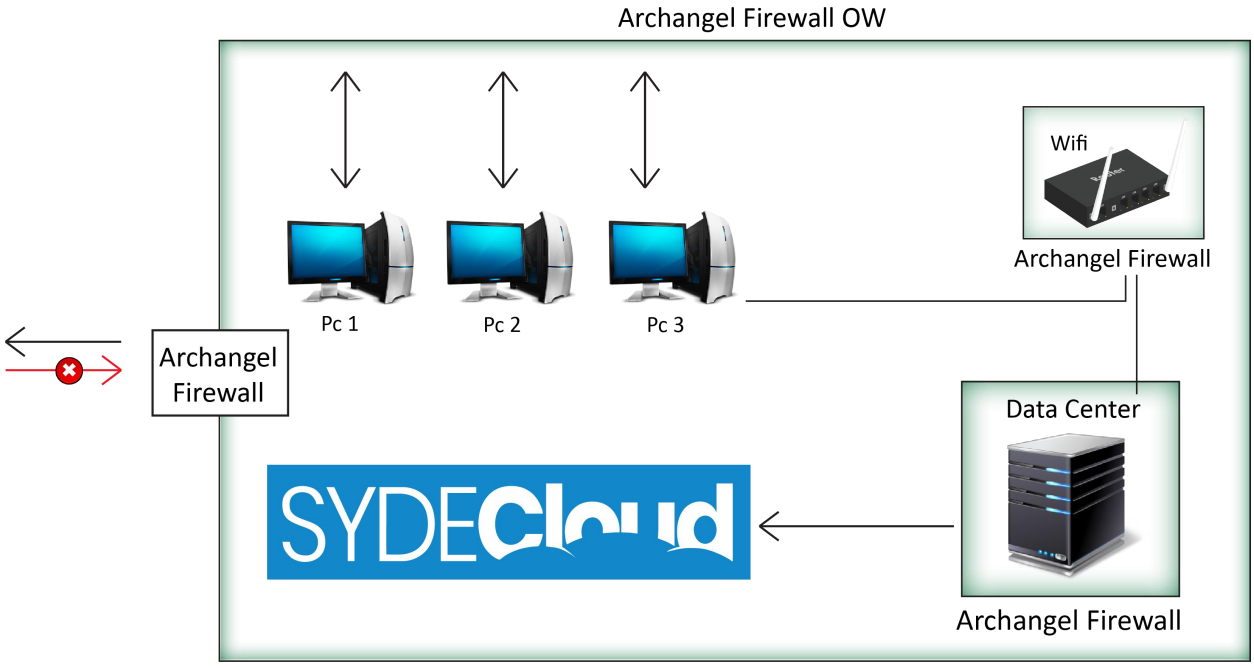

Figure 12: IT Infrastructure of the data processing department

D) Data backup department

For the establishment, all data is important. They must all be protected so that their Confidentiality, Integrity and Availability is preserved at all times.

They should be protected in a place specially assigned to receive adequate equipment and authorized persons.

It will be necessary to provide material specially assigned to the safeguard of financial data and material specially assigned to the safeguard of those coming from the general administration, without any connection link between them.

The material used for the backup cannot in any case be in contact with the outside world and can only be accessible from inside the space which is dedicated to it.

This equipment will be individually protected by a firewall of the type Archangel A4 which can only receive, automatically, the data that will systematically reach it via the back-up system of the data center, one from the general administration, the other from the space creation and processing of financial data.

This material will be individually protected by a firewall of the type Archangel OW A4.

The equipment specially assigned to the saving of financial data will automatically receive, by backup system, the data sent to it by the data center of the financial data processing center. The equipment specially assigned to the backup of data coming from the general administration will automatically receive, by backup system, the data that the data center of this department will send to it.

Why the Archangel A4 firewall? Because it is the only system equipped with a functionality specially dedicated to preventing the takeover of its operating system and in the event of an attempt to do so, capable of automatically returning to the original system by deleting any further access to the hacker. This firewall has also to let enter ONLY data coming from automatic backup, so the one way system is recommended.

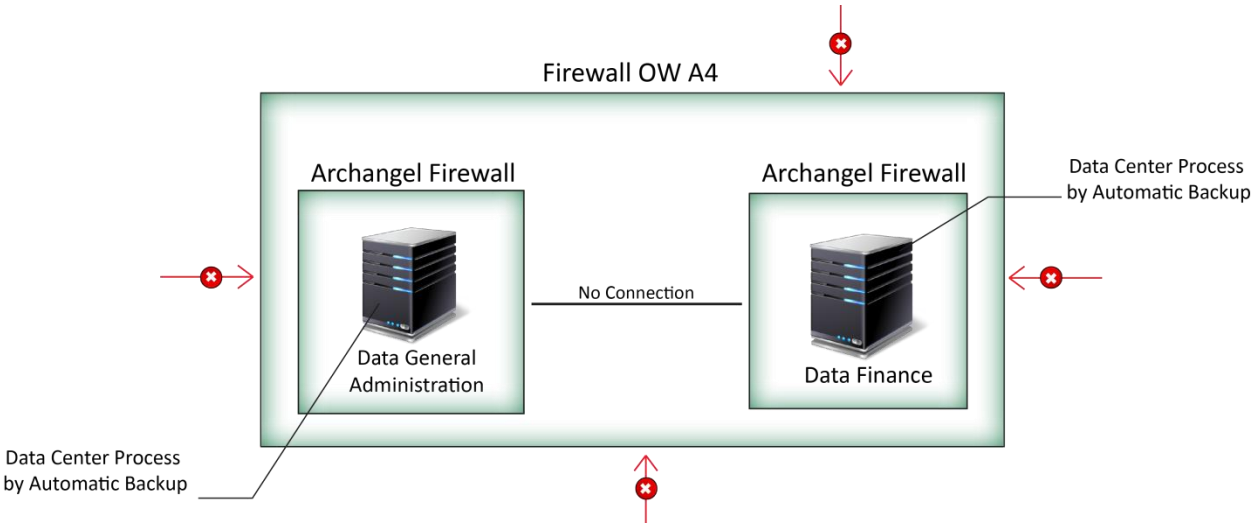

Figure 13: IT Infrastructure of the data backup department

E) Data sharing

However, since the establishment is in operation and since the both financial and other data must be able to be consulted by duly authorized members of the staff, we recommend creating a fully secure data sharing system in each of the spaces that reserved to the general administration and that reserved to the creation and processing of financial data.

In this way, the data of each department can be shared among the staff authorized to do so.

We recommend a fully secure online data sharing system such as Sydecloud©.

Why Sydecloud? Because Sydecloud helps the company to create its own online file sharing system, without any third party intervention and because the data that is conveyed is within a VPN created by Sydecloud and protected by the SST system, that they are translated into alien language and written in the form of waves, not using the system based on the theory of numbers as used by traditional cryptography and not using any key. In addition, the SST and Sydecloud servers are located in the establishment.

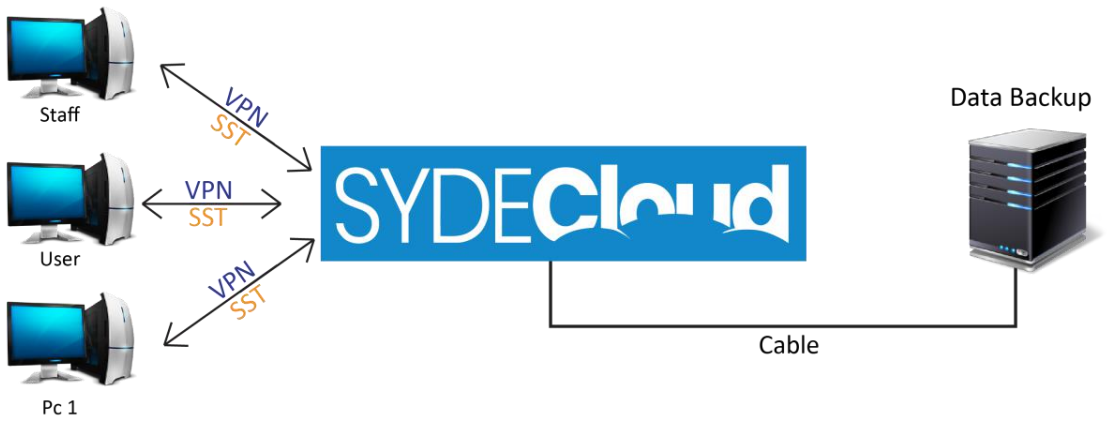

Figure 14: IT Infrastructure of the online data sharing

F) Transport of data

The transport of communications originating from the service processing the finances should be protected by a VPN in the direction establishment to the outside.

The transport of shared data online, regardless of the department, will also need to be protected by a VPN.

It would be desirable that the data circulating within the establishment also be.

But we must pay attention to the choice of VPN that will be used. Indeed, the VPN is a private network that relies on the protection of data and their access by encryption. However, whoever creates the encryption has the keys.

We must also pay attention to the system that will be used for sharing data online. Indeed, if this system is not specific to the establishment, for example Google drive... the third party may be aware of everything that is shared.

G) WI-FI NETWORKS

Binary Defense recently discovered the current possibility of the EMOTET botnet to spread via WI-FI networks and describes its operating mode as follows: It uses the victim's wireless adapter to analyze the local Wi-Fi signal space, then lists all identified wireless networks (SSIDs). This Wi-Fi analysis can take place without the victim's device being connected to any of the networks found. (Pascal Le Digol, Country Manager France at WatchGuard, April 2020).

It is therefore very important to protect the establishment's WI-FI networks.

We suggest the following:

1. Create separate WI-FI networks, which can only be used by the space in which they are located, for example, a network for the general administration department, another for the process and management of the data department.

2. Protect each network with a firewall to prevent the botnet from spreading from an infected workstation. By using ARCHANGEL©, this protection is automatic since the WI-FI network is directly connected to ARCHANGEL© and its third firewall prevents such propagation, finally,

3. Never install a WI-FI network in the sector reserved for data backup.

   We can then propose the following architecture

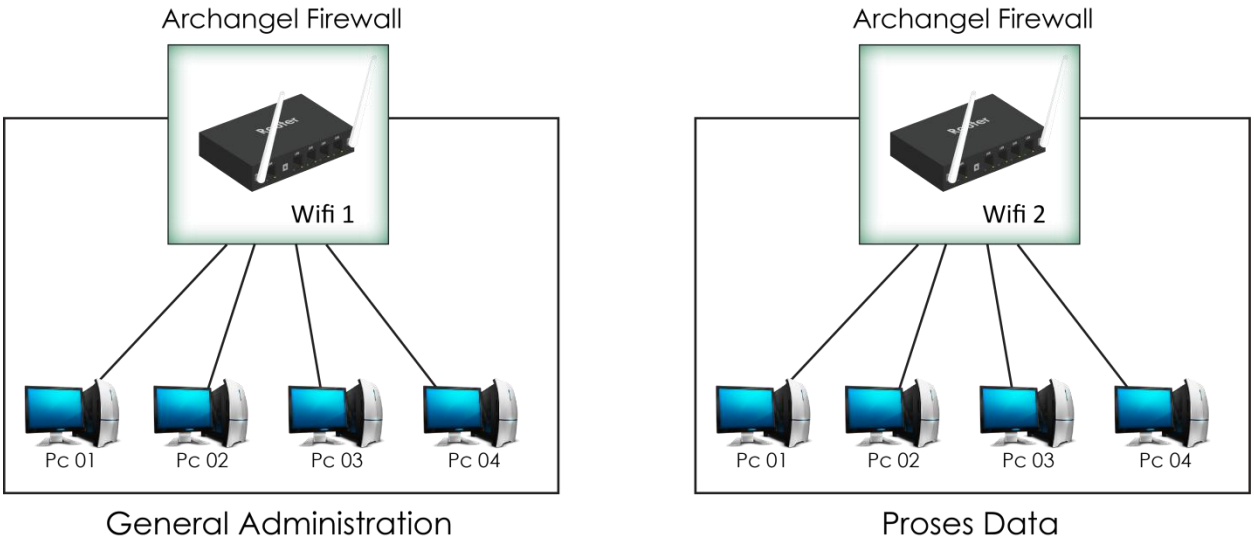

Figure 15: IT Infrastructure of separate WI-FI networks

2 – ESTABLISHMENTS FOR WHICH PROFESSIONAL SECRET IS PRIMORDIAL

For establishments in this category, it seems difficult, if not impossible, to physically gather all the workstations involved in the creation and processing of data in one place. Indeed, each doctor or each lawyer receives in his office.

Therefore, what must be isolated is not the physical space but the internet network to which these workstations are attached. In addition, each workstation had to be protected by an individual firewall and obviously with an antivirus.

For the rest, everything that has been proposed for establishments in the financial sector applies to establishments for which professional secrecy is of primordial importance.

We can then propose the following architecture

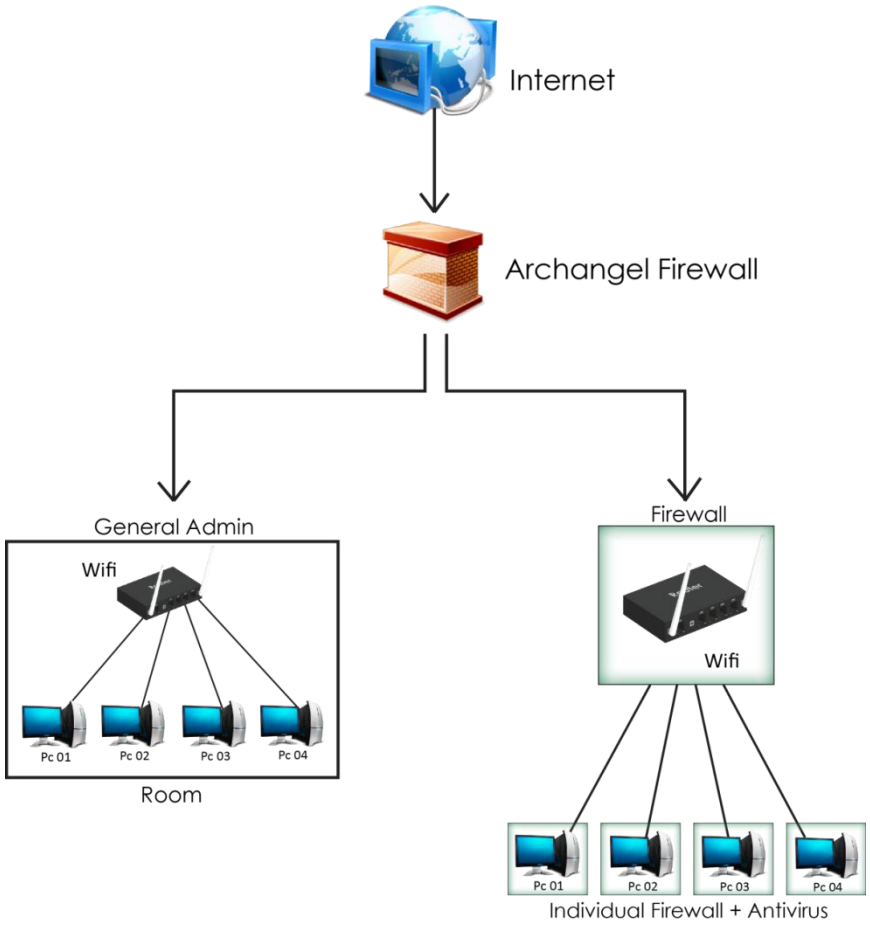

Figure 16: IT Infrastructure when secret his primordial

3 – ESTABLISHMENTS REQUIRING A TOTAL SECRET ON THEIR ACTIVITIES

Governments, at least their department responsible for diplomacy, defense or internal security as well as other armaments companies are part of this category which requires maximum security.

For establishments falling into this category, the system for protecting their IT infrastructure must extend and also cover, in the external entities receiving them, the data reception and backup equipment that the establishment sends to these external entities to which it will be linked by its own VPN. The data in this case is protected by SST if the establishment is using ARCHANGEL.

It would therefore be desirable that the entity receiving the information is also protected by the ARCHANGEL firewall to allow it to stay in reciprocal contact by VPN. Without this, communications from this entity will not be confidential.

Another system would be to dialogue within SydeCloud without authorization to download the sensitive documents.

In any case, establishments in this category may in no case use protective equipment in which a third party is involved.

So,

- the data protection system must be specific to the establishment: It cannot use the cryptography created by another entity,

- the data transfer protection system cannot be created and / or managed by a foreign entity such as GOOGLE Drive…

The systems developed by the Indonesian company PT SYDECO meet these requirements perfectly, the servers that create and manage the protection are located in the establishment which is the only one who can access to them, as well as the online data sharing servers which are in the establishment. Neither system involves external intervention.

For the rest, apart from the fact that each firewall implemented will be of the ARCHANGEL A4 type, establishments falling into this category may adopt, by means of adjustments which will be their own, the architecture of establishments whose activity requires professional secret.

We can then propose the following architecture

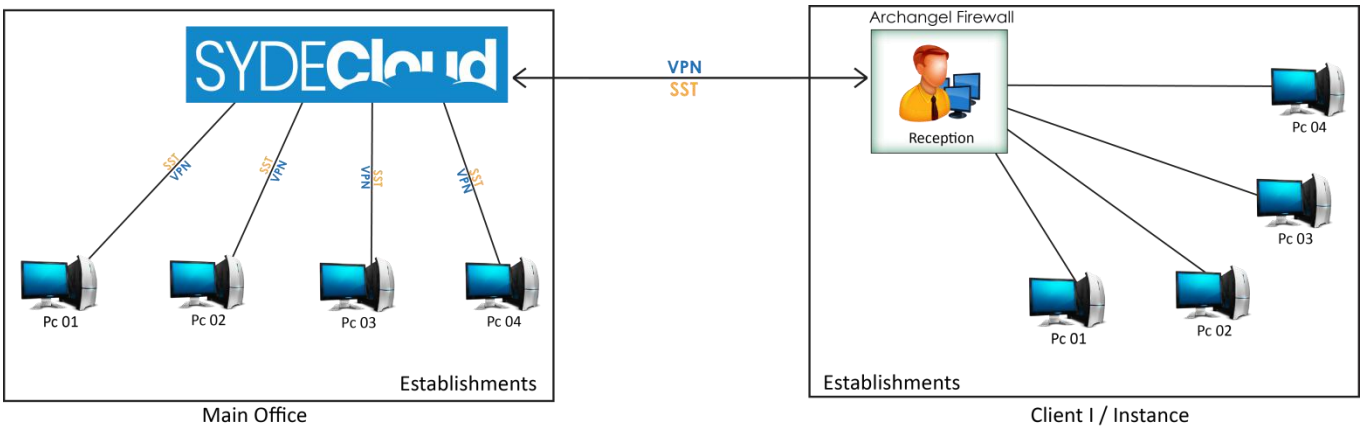

Figure 17: Preserving total secret in the main establishment and in the client's one

PART 3 : IT SECURITY POLICY

Now that we have a complete vision of the establishment's mission, its equipment needs and the security of the parts of this equipment without which the establishment could not continue its activity, and now that we have set up the architecture of the installation with regard to its security, we can start to create a security policy.

The security policy is a code of good conduct in the sense that it contains on the one hand a set of rules relating to what must be done or not by the staff in order to guarantee the security of the information system (IT infrastructure) of the establishment and what to do in the event of a security breach and on the other hand a guide to risk management specific to the information system in the event of a problem originating from the external environment with, in the two cases, a distribution of responsibilities in order to maintain business continuity (availability of information).

The establishment must certainly already have its own security policy and its business continuity planning, but it is important that the IT department of the establishment has its own security policy and its own business continuity planning because only people who deal with problems of the information system will be able to intervene effectively in the event of a problem. In addition, a breach in the security of the computer system requires an immediate reaction that a general maintenance team can never bring.

This security policy must be known by all the actors involved and must regularly, at least once a year, be reviewed and the appropriate case readjusted to deal with new situations.

A) The code of good conduct

1. Educate the staff

   It is not all about creating a security system, it is necessary that those who use the equipment protected by this system know it, comply with its requirements and above all that this security system can be used if necessary.

   Indeed, many causes of insecurity have their source in behavioral errors on the part of staff.

   It is therefore necessary to explain to the staff who is directly in contact with the IT equipment and who uses it, the importance of respecting the security measures specific to the establishment.

   Thus, we have seen that, for example, for an establishment in the financial sector, the space in which the financial data is processed cannot be accessible from the outside, including general administration.

   This means that the personnel of the general administration department cannot seek to enter this department.

   The reason is easy to understand. Insecurity coming from inside the establishment can be caused by carelessness or error by the manipulator, but also caused by a deliberate will to harm.

   By partitioning the sectors of activity, this risk is reduced.

2. Rules of good conduct

It is necessary to develop a list of simple gestures of good conduct that the staff will have to respect with for example:

a) Refraining from using:

- Equipment (laptop, flash disks ...) coming from outside (it can be contaminated),
- His mobile phone except in case of absolute necessity (it can contaminate the workstation of the one who uses it),
- The workstation for personal research (which could lead to sites that contain phishing),
- Another internet network than that of the establishment when it is at work (This network is not protected by the establishment's protection system).

b) Good practices:

- Do not open suspicious emails and if opened, do not click on links or open attachments,
  - If such a link is opened,
    - immediately disconnect his workstation and,
    - call his manager who will refer it to the security manager and,
    - do not reconnect your workstation without the authorization of the security manager.
- If in doubt, refrain from any action and refer it to the person in charge.

B) Problem from outside

Problems can occur at any time, whether it is a power failure, an earthquake, a volcanic eruption, a flood….

Not everything can be predicted, but it is important to develop a prevention strategy specific to the information service of the establishment.

For example:

- Regularly backup database, program (API and application) in a hard drive that has to kept in a safe protecting against fire and water,
- Regularly check the programs including server (API, database), environment, mobile application, and desktop.
- Be ready to covering electronic peripheral and PC when there is eruption or when not in use for long time (on long holiday for example).
- Make sure there is always at least one responsible member of the staff that standby in the area of the establishment when weekend or public holiday to prevent any unpredictable event.

C) Business continuity planning

It is important to organize the teams in charge of security, both the one created to counter any computer attack coming from outside or inside the establishment as well as the one in charge of security against problems coming from the external environment (flood, earthquake, power failure, etc.) or even the internal environment of the establishment (computer failure, power failure, problem linked to the structure of the building, etc.).

This organization includes the creation of these teams and the distribution of roles with different intervention depending on whether it is an emergency, disaster or critical situation.

- **Emergency** is a sudden or unexpected occurrence or combination of occurrences that may cause injury, loss of life, destruction of property or cause the interference, loss or disruption of the normal business operations to such an extent that it poses a threat to the IT department. An emergency is something that may overwhelm the Company's ability to resolve the situation.

- **Disaster** is a sudden, unplanned event with a significant scope of impact involving many employees if not all the employees of the IT department and is based on the scope of the event, number of lives impacted, and the devastation of property; 1) the disruption of critical business activities for some predetermined period of time. 2) The period when the Company management decides to divert from normal schedules and exercises its IT Disaster Recovery plan signified by the beginning of moving from primary to alternate processing.

- **Critical** when processes or services offered could not be interrupted or unavailable for several business days without significantly jeopardizing the Company's ability to serve its clients during an emergency.

There is a need for the establishment to prepare for unexpected events such as natural or human-caused disasters, as well as the need to return the establishment as quickly as possible to its normal operations should such events occur.

This policy has to delineate the responsibilities to respond to emergencies, to ensure that critical functions are maintained or restored in a timely manner.

All IT department's staff should familiarize themselves with their department or business continuity and disaster recovery plan, as well as the Company emergency plan that the establishment has to provide.

That program has to define the goals of:

- The Computer security program and its management structure.

  The basis of organizational goals establish in that policy is the need and the respect at any time of the Confidentiality, Integrity and Availability of all the data the establishment is dealing with.
- Human resource, material and premises security and its management structure.

When implemented, the program should include those procedures and support agreements, which insure on-time availability and delivery of required products and services.

It is therefore necessary:

- For the person responsible for maintaining large mission-critical database to:
  - Stress a reduction in errors, data loss, or data corruption,
  - Emphasize stronger protection against unauthorized disclosure.
- For the person in charge of a Department, to create a Program management structure in order to best address such goals and respond to the particular operating and risk environment of the Company.

All Departments are required to develop and maintain a Business Continuity Plan (BCP) that describes the critical functions of the unit and how each function will be continued or resumed rapidly after an emergency to enable the establishment to resume its activities within minutes or hours, even following a major disaster.

It will be necessary to implement the following steps for each department of the IT division of the establishment:

- Conduct a Business Impact Assessment (BIA) that describes the critical functions, identifying both the Maximum Tolerable Downtime (MTD) and the Recovery Time Objective (RTO) of each. In addition to the MTD and RTO, the BIA must also establish the appropriate Recovery Point Objective (RPO) to reduce the impact of data loss. This assessment should be updated whenever a significant change occurs to any of the critical functions within the Departments.
- Include:
  - Strategies for restoring critical functions within the recovery times necessary,
  - Continuity strategies to be implemented in the event of loss of facilities, disruption of IT systems, or lack of full staffing for a period of time,
  - Names, responsibilities, and contact information for the Department disaster recovery team, which should include the unit leader,
  - Procedures and checklists to be followed to achieve timely program resumption after a disaster.

For purposes of this Policy, a “Recovery Time Objective” is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity and a “Recovery Point Objective” is the maximum tolerable period during which Data might be lost from an Information Resource.

This Business Continuity Plan (BCP) has to be:

- Updated annually to ensure that continuity strategies are adjusted if necessary, and that contact information for the unit recovery team is up-to-date.

- Tested annually to ensure effectiveness and to ensure the recovery team members understand their roles and responsibilities.

All Departments that operate the IT systems, must develop and implement adequate Disaster Recovery Plans (DRPs) based upon a BIA. All DRPs must contain the following information:

- A comprehensive inventory of applications, servers, data and support infrastructure necessary to operate the line of business,
- Comprehensive system recovery procedures, which are in line with the MTD and RTO established in the BIA, for each system and or application identified as critical to the establishment. Recovery procedures should be documented with a level of detail that would allow a competent third-party IT professional to recover the system or application.

Each DRP must be tested annually to ensure that it is effective and up-to-date.
Documentation of test details, results and executive acceptance must be retained for a minimum of one year.

Within the teams that will be created within each IT department of the establishment and which can be called Crisis Management Team, it will be necessary to define the roles and responsibilities of each member.

PART 4 : RESPONSIBILITIES

1.
Each State has an obligation to ensure the security of its citizens. This obligation is in fact only the counterpart of the exclusive police right that the State exercises over its citizens.

The result is that every citizen is entitled to expect that the State will guarantee him public security and, therefore, is entitled to sanction the State by recourse to the courts whenever it does not fulfil its mission of security.

We will not going to find out whether the State has taken all the necessary precautions to ensure this security because the obligation of the State is an obligation of result and not of means.

The state is responsible when security is not assured, even if it has taken all measures to enforce it.

2.
The State confers on certain of its organizations, or companies which pursue an interest of public order, even private, the authorization to exercise because the activity of these establishments is vital for the survival and development of the nation.

The State is therefore entitled to expect these organizations or companies to do everything in their power to ensure that their activity is not interrupted or that it does not turn against the interest of the nation.

Paradoxically, but at first glance only, the obligation which weighs on these organizations or companies, is only an obligation of means although they can only exercise with the authorization of the State: to avoid that their responsibility is engaged, these organizations or companies must prove that they have used all existing means to ensure that the activity is not interrupted or that it does not turn against the interest of the nation.

The State could have demanded from these organizations or companies the same level of responsibility it has for its citizens. Not doing so, one can wonder if the State does not commit its responsibility towards its citizens if such an organization or company fails in its mission.

3.
But what becomes of the citizen in all this?

Everyone has the right - and this right is recognized both by national laws and treaties - to have his private life protected. Everyone’s private life includes his image, his personal data, his financial data and his activities insofar as they are exercised within the limits of the law…

The State exercises control over this protection. In fact, it is an obligation of the State.

Citizens are therefore entitled to expect from organizations or companies that they respect their own rights.

Citizens are therefore entitled to expect these organizations and companies to take all necessary measures to ensure that their rights are respected.

But since these organizations and companies act only by virtue of an authorization from the State, without which they could neither exist nor have any activity, the State has an obligation towards its citizens to ensure that these organizations and companies take all necessary measures to ensure respect for their rights.

The State which is subject to an obligation of result cannot escape its responsibility in the event of a failure of a company with regard to its customers or users or members. This failure exists only because the one who is responsible for it has not taken all the necessary security measures and the State has not exercised its obligation of control.

4.
Since the State is responsible for the public security of its citizens, the State is in the same way responsible for the right to the private life of its citizens and in this respect its responsibility can only be a responsibility of result.

5.
That is to say that each organization or company only holds the elements of the human rights of its customers, members or users by virtue of an authorization given to it by the State.

Each organization or company that collects or holds personal data from their members, customers, users, is therefore responsible, both vis-à-vis the State and to those who entrust it with this data and must repair it in the event of failure.

It therefore weighs on those who collect or hold the elements of a citizen's private life, an obligation to preserve them.

There is therefore an obligation imposed on all companies governed by public law, of public or private interest, to take all necessary measures to guarantee the human rights of those with whom they deal.

6.
In this study we have presented the maximum that an establishment can do to preserve its production tool, its activity or the data entrusted to it.

Of course, each establishment will have to choose what suits it best, but without losing sight of its dual responsibility, that vis-à-vis the State and that vis-à-vis the private people with whom it deals.

By taking all the necessary precautions to safeguard its activity and the private life of those who entrust it with confidential information, organizations and companies protect their own interests for two reasons: They do not damage their assets and do not commit their responsibilities to the State or to those who trust them.

Patrick Houyoux
LL.M. ULB, Brussels,
Trinity College, Cambridge, UK.
President – Director
PT SYDECO