D1.1. Critical Infrastructure base security characteristics and market analysis

WP1. Adaptation of security components to Critical Infrastructure environments

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 31-10-2016

Actual submission date: 31-10-2016

HORIZON 2020. WORK PROGRAMME 2014 – 2015			Project No	700378
Call			Instrument	Innovation action
Digital Security: Cybersecurity, Privacy and Trust			Start date	May 1st, 2016
Secure societies. Protecting freedom and security of Europe and its citizens			Duration	36 months
DS-03-2015: The role of ICT in Critical Infrastructure Protection			Website	www.cipsec.eu
Public	Confidential	Classified	Lead contractor Atos SPAIN S.A.	

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

Document contributors

Editor	COMSEC		
Contributors			**Reviewers**
		AEGIS	
	Fernando Carmona	ATOS	
		BD	
	Jonathan Gutman Guy Levi Miki Partush Raphy Bitton	COMSEC	Baruch Menahem Gil Cohen Amir Atzmon
	Barbara Lunel	CSI	Barbara Lunel
	Christian Schlehuber	DB	Till Voß Christian Schlehuber
		EMP	
		FORTH	
		HCPB	
		TUD	
		UPC	
		UOP	
		WOS	

Document history

Version	Date	Author	Notes
0.0	20-07-2016	Amir Atzmon	ToC.
0.0	03-08-2016	Fernando Carmona	Analysis for Financial Services
0.1	03-08-2016	Amir Atzmon	1st draft
0.1	19-08-2016	Fernando Carmona	Financial Services domain
0.1	02-09-2016	Fernando Carmona	Atos contribution is now finished
0.1	17-09-2016	Barbara Lunel	CSI contribution
0.1	03-10-2016	Barbara Lunel	New version after HCB contribution
1.0	07-10-2016	Amir Atzmon	Ready for review
1.0	11-10-2016	Fernando Carmona	CSI comments fixed.
1.0	12-10-2016	Till Voß	DB review
1.0	19-10-2016	Christian Schlehuber	New version with the missing parts added.
1.0	20-10-2016	Baruch Menahem	New integrated version and fixed all the remarks

Index

1 Executive summary

Critical infrastructure (CI) are defined as systems and assets whether physical or virtual, extremely vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, loss of life or adversely affect the national morale or any combination of these matters.

After identifying what may be considered as CI, a protection strategy has been stablished to identify which elements of the infrastructure are critical to its function or ones which pose the most significant danger to life and property, based upon two major aspects:

- External/Internal Threats: important Central facilities, such as power-plants, central control units etc. are exposed to various threats which may cause considerable damage or even worse catastrophic damage to central infrastructure, causing damage to cities or even to country in which they are located.
- Securing Critical Infrastructure: major industries which are supported by critical infrastructure such as transportation, environment, energy, health and more, depend largely on control systems which dictate the requirements.

CI security features may differ significantly from one CI category to another. Each category may contain different critical assets, implement different technologies and tools, and use different protection methods based on the specifically identified threats toward the CI category. With that said, there are shared aspects of security characteristics that have been analysed in this document: High-Availability, Physical Protection, and Cyber Security.

Then, the document presents a detailed review of specific security issues for each of our three pilot scenarios: Transportation, Health, and Environmental monitoring. Financial services domain has been included as well to reach an enhanced perspective.

- Transportation. During the last years a change is moving through the sector: digitalization. More and more systems are moving to highly interconnected systems built on COTS components. In transportation, the main target of security is to ensure safety of the system, which also leads to the term “Security for Safety”. The three layers of this approach are detailed in this document: Operation Layer, Interlocking Layer, and Field Element Layer.
- Health. There are many subsystems that can be considered critical directly involved in the proper daily functioning of any hospital. In our case, some of these OT and IT subsystems are integrated and managed from the corporative network whilst others (mainly the ones considered more critical) are kept physically isolated from this network security.
- Environmental monitoring. Considering a typical environmental monitoring system, it is necessary to protect the monitoring stations, the data collection servers, and the post elaboration, data management and assessment applications. These tree components of the monitoring network are exposed to different kind of risks and have different security needs, so they have been discussed one by one.
- Financial services. As the institutions that store and distribute funds, that provide loans and handle transaction processing, banks are potentially very vulnerable. Principles and processes for effective cyber-security in the Financial Service arena could be addressed in seven key dimensions that are introduced and explained in this document.

Market Solutions for CI domains have been reviewed in D1.1 under a technical perspective, whereas D5.1 contains complementary competitors and market analysis sections, business and exploitation-oriented, trying to demarcate CIPSEC potential advantages in its go-to-market strategy. Here, for those market solutions, a cross-domain analysis has been tackled, recognizing elements such as Data, Application, Host, Internal Network, Perimeter, Physical security, Policies, Procedures and Awareness, and Governance, Risk management and Compliance. Industry solutions for Environmental Monitoring, Transportation, and Financial Services have been included as well.

2 Introduction

2.1 Security and privacy in Critical Infrastructures

Critical infrastructure are defined as systems and assets whether physical or virtual, extremely vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, loss of life or adversely affect the national morale or any combination of these matters.

Due to the increasing pressure from external and internal threats, organizations responsible for critical infrastructure have to have a consistent and iterative approach to identifying, assessing and managing cybersecurity risks.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology and industrial control systems. This reliance on technology, communication, and the interconnectivity of information technology and industrial control systems has changed and expanded the potential of vulnerabilities and increased the potential risk to operations.

In order to manage cybersecurity risks, a clear understanding is required of the organization's business drivers and security considerations specific to its use of information technology and industrial control systems. Because each organization's risk/s are unique, along with its use of information technology and industrial control systems, the tools and methods used to achieve the outcomes described by the framework will vary.

Recognizing the role that the protection of privacy and civil liberties play in creating greater public trust, the Framework must include a methodology to protect individual privacy and civil liberties when critical-infrastructure organizations conduct cybersecurity activities.

2.1.1 What must be protected

After identifying what may be considered as critical-infrastructure, a protection strategy must identify which elements of the infrastructure are critical to its function or ones which pose the most significant danger to life and property. Not all assets may be critical, some may be more so than others. However, the size and complexity of these infrastructures may present the task of identifying which assets of an infrastructure are critical as a daunting task.

To obtain protection on a critical infrastructure there is a need to first perform a full risk assessment of each system to better understand the different logical processes. After a basic understanding of the contributing sub systems to the entire logical system and given that a complete understanding of the entire logical operation of a system and the interconnections of its subsystems there is a need to derive a complete set of classifications in order to determine the criticality of the system.

It is of utter importance to protect the Availability, Reliability and Flexibility of systems on which critical infrastructures exist which enable both the ability of the people to maintain personal safety and the security of the country.

There are many areas associated with critical infrastructures such as emergency services, water, agriculture, food, government, defense industry, information and communication, health care, banking, energy, transportation, chemical industry, automation and control materials, postal services, shipping, national symbols airports and more.

2.1.2 External/ Internal threats

Vulnerabilities and potential threats to Critical Infrastructures (CI) are well recognized for quite a long time now. Critical Infrastructure refers to all infrastructure segments that support nation-wide basic needs, such as the ones described in this document (Transportation, Health, Environment and Finance). Another important characteristic of CI is the dependency of each CI component on other CI components. For example – A cut in gas or fuel supply to a country, may lead to electric power downs, which in turn will disable additional CI components such as hospitals or computer-based traffic control systems, causing possible loss of life and a continued chain reaction effect that can go on and on.

Critical Infrastructure threats can be divided into three main categories:

- Environmental threats – such as weather and geological hazards like volcanic eruptions, storms, earthquakes and more, which can all cause serious damage to physical facilities (e.g. power plants, roads, or critical factories).
- Human-caused threats – to CI such as terrorism, cyber-attacks, riots, explosions and other sabotage methods performed by individuals, groups or by countries.
- Accidental threats – referring to accidents and failures of CI components and devices, hazardous material accidents and other infrastructure malfunctions.

Each CI component should be designed to withstand potential threats originating from all three threat categories. Full protection against all three categories, may pose a major challenge when taking into consideration the fact that, unlike the well protected and closed IT facilities and end-points in organizations, many of the CI facilities are much more exposed to the public.

Some examples may include power-lines, traffic light systems, various sensors (such as cameras, weather sensors, etc.) located in relatively exposed locations in cities, etc.

Important Central facilities, such as power-plants, central control units etc. are exposed to various threats which may cause considerable damage or even worse catastrophic damage to central infrastructure, causing damage to cities or even to country in which they are located.

Most Critical Infrastructure components are usually required to maintain the highest possible availability, given that even a minute down-time of just a single system may disrupt the normal life order of a major city or even a country.

The previously mentioned conditions, in which a CI component needs to operate, dictate the need for proper physical protection against threats.

After assessing the threats and the pertaining vulnerability's, Critical infrastructures can be protected according to an anti-vulnerability threat plan. The plan will help minimize or prevent the threats. In order to protect critical infrastructure, there is a need to:

- Asses CI vulnerabilities for physical and cyber-attacks.
- Create a CI layout to counteract serious vulnerabilities.
- Find the various prevention and detection systems of significant large-scale attacks.
- Develop early warning programs against attacks in real time.
- For investigation purposes the ability to restore the minimum and essential skills and capabilities of an attack.

2.1.3 Securing Critical Infrastructure overview

Defense in depth means to defend an asset or system against any particular attack combining different methods.

This type of defense uses a layered tactic which was primarily conceived by the national security agency as a very comprehensive approach to information security.

Like a military strategy Defense in depth seeks to gain time by creating a delay rather than preventing an attacker from deploying an attack. This type of protection mechanism, policies and procedures increase the dependability on IT systems, where different layers of defense hold back directed attacks towards critical systems and assets. Defense in depth can buy time resulting in better detection and better attack response time which will minimize and mitigate the outcome of a breach.

Major industries which are supported by critical infrastructure such as transportation, environment, energy, health and more, depend largely on control systems which dictate the requirements. Currently there is a strong dependence of CI advanced control systems on old control systems such as SCADA controllers. As a result of this dependence the data/communication exchange protocols used between the new and old controllers present a new threat hence new cyber risks. The more advanced modern controllers adhere to company-based proprietary standards having a negative and positive effect. On one hand, newly introduced protocols and products by a wide variety of manufacturers introduce new solutions, while on the other hand the introduction of new protocols and new advanced controllers pose new risks. The entry into Cyber era introduced many new non existing risks largely due to the use of both new and old controller based technologies simultaneously. The increase in controller based technology development, the use of old architectures lacking a layered defense architecture has increased the quantity of attacks carried out by hackers and their ability to abuse these older architectures. Incidents of unauthorized access to critical infrastructures have become much more frequent.

Prior to deploying/manufacturing advanced CI systems, there is a need to conduct an extensive review of the CI architecture. Lack of such a review may lead to many problems such as an increase in dependence between automation systems and the controller's control, secure connectivity to external networks, use of technologies with known vulnerabilities. Technology control systems have very little security aspects incorporated into the control system. They are designed to perform their required function without if any security considerations. Hence, many controller communication protocols are lacking sufficient security application.

When considering critical systems that must disconnect external environment from internal environment, the considerations become greatly more significant.

In addition when considering advanced control systems the security challenges have also increased significantly due to the newly introduced vulnerabilities that have evolved because of the way we are interconnected in the modern way of living. The mere fact that everything is connected to everything has complicated even minute and simple systems, however, lacking a proper layered defense architecture ie: defense in depth protection in place for such systems will continue to expose them to existing and new vulnerabilities.

Currently, controlling critical infrastructures networks have evolved such that they connected with enterprise IT environments, therefore, contributing and creating many more security vulnerabilities.

Defense in depth in Critical infrastructure in short

- Data – Protecting databases, Identities, documents, and so on.
- Application – Preventing the manipulation of the data.
- Host – Protecting the computers that are running the applications.
- Internal Network – Securing the CI network.
- Perimeter – Securing the network that connects the CI to another network, such as to external users, partners, or the Internet.
- Physical – Prevent theft or damage to servers, hard disks, network devices, etc.
- Policies, Procedures and Awareness - Overall governing principles of the security strategy.
- Governance, Risk management and Compliance – monitoring and recovering from incidents and disasters.

An extended information of each topic can be found on section *5.1 Cross-domain solutions*.

2.2 Definitions and terminology

CIPSEC platform design is affected by two main aspects, technical needs and business needs. Power, communication and capacity of growth are comprehended as technical needs, while resources and risk management are business ones. These significant needs impose particular challenges to CI operations and the approach of protection.

Well identified, there are several dependencies and interdependencies.

For example, system controllers and legacy systems are both infrastructures mutually serving advanced technologies, thus a dependency is present that impairs reliability and leaves little room for error. Interdependencies are known to take the place between CI sectors, for example, transportation depends on fuel as oil depends on transportation to transport the oil to be refined into fuel.

CIPSEC practices as well, cannot always be implemented, for example, “air-gapping” is a CIPSEC essential, but centralized control points improve efficiency and reduce costs. Such contradictions frequently happen due to management interests and business goals.

However, it is imperative to recognize that CIPSEC is not about securing the infrastructures itself but the services that are produced and provided.

3 CI Base security characteristics

3.1 General security characteristics

Critical Infrastructure security characteristics may differ significantly from one CI category to another. Each category may contain different critical assets, implement different technologies and tools, and use different protection methods based on the specifically identified threats toward the CI category.

With that said, there are shared aspects of security characteristics that do appear in most CI categories and can be analyzed in a more general sense in this section:

3.1.1 High-Availability

Most CI facilities and services are required to provide vital services and perform vital tasks in a continuous matter. An outage of a single system, for even the smallest amount of time, can disrupt additional CI elements, possibly causing a chain reaction between various CI components, and disrupting the normal life order of an entire city or even a country. This creates a demand for services to be available 7 days a week, 24 hours a day.

No system is prone to malfunctions and most systems and infrastructures will require periodic maintenance, which may require shutting down parts of the systems for various periods of time.

As a result – most CI component are planned and built with fault tolerance solutions, such as system duplication, additional Disaster Recovery facilities and various Backup Strategies. A correct planning of fault tolerance solutions, results in a more stable system that is able to provide vital services regardless of outages of different parts of the CI.

3.1.2 Physical protection

CI facilities and components may differ in size and complexity and may vary from big and complex facilities such as power plants or railroad stations, to anything as small as a traffic control camera.

As mentioned in previous sections, these facilities and components may be subject to malicious sabotage attempts by individuals, or even pose a target for hostile countries. These kinds of threats, require various physical protection techniques. These techniques may include armed guards, closed-circuit TV systems (CCTV) with manned monitoring centers, fences, and various additional physical protection solutions.

3.1.3 Cyber security

As in physical protection, CI facilities may also be subject to Cyber-attacks, requiring additional Cyber-security measures. The majority of these measures will be discussed further in the next sections of the document.

Most of them are meant to protect the CI against Information leakage/loss, prevent unauthorized access, and secure all communication in and out of the facilities.

- **Access rights management –** proper access rights management is important for both, the physical and the cybernetic domains. Access rights are usually implemented in all CI facilities, and allow granular management of all authorized personnel, with ability to restrict access to only some parts of the CI facility or its information.
- **Monitoring sensors –** Most CI facilities, are properly monitored both physically (for example via specific sensors that ensure the health state of critical equipment) and electronically (via Cyber security sensors and control systems), allowing efficient detection of malfunctions and possible security breaches as they happen (or even before that), thus preventing potential damage to the systems.
- **Command and Control Centers** – Most CI facilities use centralized control over all equipment (physical and virtual alike), to create a full picture regarding the health state of each facility or the entire CI altogether. The vast amount of information flowing to one centralized location, makes it easier to discover interconnections between different incidents, and manage them more efficiently.

- **Incident response teams** – Since all Critical Infrastructure may be subject to all sorts of incidents (such as cyber security breaches, physical sabotage and technical malfunctions), many CI facilities maintain dedicated incident response teams to deal with each scenario. This enables a well-controlled response, by a crew, specifically trained to treat such incidents.
- **Regulation and standards –** Like all big and important facilities, the CI facilities use standards and regulations, that dictate homogenous requirements regarding the facilities, the required security and protection measures, and standardized management for all similar facilities across all CI.

3.2 Transportation

Due to the needed admissions for most transportation systems these were monolithic and proprietary systems for long times. During the last years a change is moving through the sector: digitalization. More and more systems are moving to highly interconnected systems built on COTS components. While attacks were hard to perform on the former systems due to secret proprietary systems, protocols and closed the emerging standardization, usage of standard components and networking enables more attack vectors on transportation systems.

In transportation the main target of security is to ensure safety of the system, which also lead to the term “Security for Safety”. The system itself can be divided into three layers:

- **Operation Layer**

  In this layer the operators are working at specialized workstations and tell the interlocking system, which route has to be built and in which direction the trains have to go. On this layer are the workstations, which consist of a safe display of the controlled area. This workstation also is connected to several communication systems like GSM-R or the telephone network. On this layer not only the operators are located, but also the infrastructure dispatchers, which come into action, if trains are running out of schedule or defects on the infrastructure occur.

  The buildings, in which the operation systems are located have to fulfil special requirements, regarding to fire safety or access control. Also the personnel is trained to perform a safe railway operation.

- **Interlocking Layer**

  On this layer most of the safety systems are located. The interlocking layer is located between the operation layer and the field element layer and checks the commands from the operation layer for validity and if they respect the safe operation. Besides this it monitors the components on the filed element layer for correction operation and in case of anomalies falls into an error state. On this layer, systems like the interlocking itself, the MDM and ETCS are located. These systems are connected to the operation layer and the field element layer via a wide area network owned by the railway operator.

  The networks are separated by firewall systems and only valid traffic is allowed to pass to the other layers. The components on this layer are developed according to several safety standards and only the required functionality is available. Additionally these components have to be assessed by a safety authority and changes or updates to these components also have to be assessed by the safety authority.

  The components on this layer are built redundant, which means that in case of a defect one of the standby systems comes in place and the maintenance personnel is notified, to replace the failing component. Also the data networks and the power supplies are redundant and according to the size of the facility the building is equipped with a battery or also a generator, which is started if the energy provider is not able to provide power.

  Buildings on this level are designed to current object security rules, which mean, that there are several systems for alerts in place, like intrusion alerts, and doors and windows are designed to prevent from an intrusion.

- **Field Element Layer**

  On this layer the field elements are located. These are elements like points, signals, axle counters or other equipment of this type. Each element is controlled by an object controller, which is connected to the interlocking layer via a network connection. The communication between these elements is secured by a security gateway that encrypts the communication. For key distribution a PKI is in place.

Each of the object controllers is located in a box near the element, which it controls. The boxes are secured by an alert system and the operation is stopped if the box is opened. Every object controller is equipped with redundant network interfaces and power supplies. For the communication the RaSTA protocol is used, which ensures, that the communication is safe according to EN 50159.

3.3 Health

There are many subsystems that can be considered critical directly involved in the proper daily functioning of any hospital. In our case, some of these OT and IT subsystems are integrated and managed from the corporative network whilst others (mainly the ones considered more critical) are kept physically isolated from this network security.

- **OT area**
  - Water: The hospital provides water by 3 independent connections, physically equidistant. Each one has its own pumping system responsible to produce the necessary pressure to the distribution ring located in every floor. These equipment's, not connected to a SCADA, are located inside closed technical premises w/o any specific protection so their vulnerability is scarce. Besides this triple replicated feed, there is a dual contingency plan based on the deployment of several hydrants, easily accessible from the street, located at strategic sites predefined to facilitate the disposition of several trucks with tanks that could partially reinforce (or totally replace) these usual water sources to the hospital in case of need.
  - Electricity: From the point of view of power supply, by regulation, all the Hospital must have hired a double redundant electrical wired connection (although, in fact, both depend on the same supplier company). In the case of HCB, those lines feed four totally independent transformer stations sized to meet the electrical needs of the entire hospital, so that if one falls the rest bear the burden of the entire center. This flexibility base on different connections and transformers is additionally enhanced by the existence of four generators that become operational, also covering 100% charge of the hospital except for some secondary loads such as air conditioning non-clinical areas, in case of total catastrophic failure of the external network.

    The generators are installed in pairs inside two technical rooms with restricted access and are permanently monitored by a workstation located in the maintenance department through a communication network isolated from the main corporate network.

    Analogously as what has been done with the pumping water systems, several distribution panels on which you can connect other external mobiles generators have been strategically emplaced inside the main building to ensure the continuity of the electrical supply to the most critical areas of the hospital in case of failure of generators.

    A third level of electrical safety is covered with a big amount of UPS distributed among all the critical areas. These devices can support any potential micro cut and the unavoidable gap (about 20-30 seconds) that could appear between the instant of failure of the main power supply and until the generators are synchronized, enter in work regime and totally stabilize the electrical grid.

    The existent UPSs are not monitored remotely by any application. Instead of that, all of them usually have some repetition monitor located in the control site of the different critical areas that, in case of failure, shows some sort of signal that alert the users to report the incident and call Maintenance. They are placed in closed technical areas with restricted access.

    It should be noted that one of the main priorities of the Directorate of Infrastructures is gradually replacing all locks of such technical premises by a biometric reader and the installation of a complementary video surveillance camera focusing on the gateway, configured to automatically record the event each time somebody tries to access to the technical rooms. This is an HCB phased deployment project started three years ago that has virtually ended.
  - Fire control: Another critical installation is the one referred to the fire detection and extinguishing systems. This is composed by a huge amount of smoke detectors from different brands and suppliers linked to several proprietary bus nets (one per each floor and pavilion according, defining independent physical fire sectors as requested by the national policy and regulations) isolated from the rest of the corporate intranet.

Within this system there are also included sirens, actuators and drives of alarms; the elements with which users interact.

The fire centrals are found mostly within technical rooms but there are some few units located in public corridors without any particular safety measure. The centralized gas facilities (oxygen, medical grade air, vacuum), located into dedicated technical premises, are nor managed neither monitored remotely so all the systems and equipment's that compose those installations operate independently the IT network. In the same way as defined with the water pumps and the power generators several auxiliary distribution panels on which you can connect other portable gas cylinders have been spread throughout the building to ensure the continuity of the gas supply to the most critical areas of the hospital in case of any major failure.

- HVAC: Air conditioning and heating facilities are effectively managed through SCADA. The machines, the probes control panels and all the actuators are located between the 10 main lateral pavilions of the building. All of them are connected to the hospital's IT network allowing the maintenance technicians to monitor and control remotely the cooling plants, the climate and the boilers from everywhere with tablets and portable laptops. This critical infrastructure works over a virtualised server resident in our redundant Centre of Data Processing (CPD), a specific VLAN for equipment's and Ethernet clients and counts on a VPN per supervision managed by our IT department.
- Security: Within the Hospital there are deployed +400 surveillance cameras AXIS brand, most over IP, which are connected to the corporate network. There are also a few analog units' brand BOSCH with accessory IP converters to finally converge to the same LAN ACCES platform that manages the whole Security Service. In addition, in recent years there have been implemented +200 DORLET biometric access readers in the entrances to all the critical areas communicated with a virtual server through which all updates applied in the database of the Department of Human Resources are received in real-time to give access rights to the institution staff as well as the outsourced collaborators.

- **IT area**

There is a complex ecosystem in which thousands of equipment's and electro medical devices of all types, producers, models, configurations and year of purchase coexist so its integration into any IT network is habitually difficult and in many cases directly cannot be performed due to the technical obsolescence of the equipment's and/or the lack of protocols and standards (as HL7) defined to facilitate the interconnection with the common Hospital Information Systems.

In the area of Hospital's IT we find about 6,000 computers (PCs, VDI, network printers, etc.) as well as numerous electro medical subsystems that integrate the IT network such as:

- Vital signs monitoring systems: Those equipment's are responsible to monitor, record and analyze most of the patient vital signs. Currently those devices are connected to the corporate network and are viewed from a central monitoring display, normally installed in the nursing central station of each clinical care unit. Usually, the required software resides locally on one dedicated PC of every central station although currently is being under development a cross-departmental project with the aim to install a single software for all the hospital in a virtualized server, capable to communicate with our HIS and centralize the complex hospital's data flow to the Patient's Clinical History.
- Other basic devices integrated into the corporate network via WI-FI are the electrocardiographs (ECG), capable to send a PDF or a XML file to the HIS for recording clinical parameters.
- Of course, there are always integrated into the network all the medical equipment's dedicated to obtain medical images (Ultrasounds, MRI, X-rays, CT scans, PET, etc.). All of them point to a virtual server that receives the image files associated with each individual patient in a DICOM international standard and stores them in our CPD.
- Refrigerators, freezers, ultra-freezers, cold rooms, cryogenic tanks, CO2 incubators and all those equipment's in which the accurate control of the temperature and/or the concentration of certain gases vs. time is critical, are monitored by a proprietary system consisting of probes, RF transmitters and receivers that constantly send these parameters via Ethernet to a server that manages and records alarms and discreetly send messages to those responsible for the various areas (usually biomedical Laboratories).
- Passive UHF RFID readers: +100 readers and +500 UHF Antennas are deployed in several areas inside the hospital. Among them: the Surgical Area (including all the Operating Theaters), two Critical

Care Units and the complete Emergency Building. That system is being used to locate and track +1,000 fixed assets, the patients undergoing certain surgeries, the doctors and nurses that work in some infectious areas… and to actuate as triggers for certain automatic mechanisms (soap and disinfectant dispensing, door opening/closing functions, customization of A/V messages that appear in certain tablets embedded in the walls, time measures that are being used to automatically complete some forms,…

- Partly IP telephony has been deployed in specific areas of the Hospital. It has been implemented a new call center capable to communicate with the HIS so that calls are identified and automatically recall certain data stored in our systems, facilitating the patient's management and the acquisition of their clinical histories without opening another application such as SAP.
- A platform has been deployed with an integrated IT infrastructure, equipped with MCU, Gateway, traversal firewall and a gatekeeper, besides having nearly 40 terminals distributed in different meeting rooms scattered over some independent buildings.

3.4 Environment

Environmental monitoring consists in the processes needed to monitor the quality of the environment and usually is applied to air, water or soil to detect the presence of various kind of pollutants and also to collect data about weather or natural resources to estimate pollutants spreading. Environment monitoring networks essentially consists of:

- Monitoring stations with complex analyzers or more simple data loggers with sensors, used to measure environmental data.
- Data collection servers, used to collect data from the stations and for station management and supervision.
- Data management, elaboration and distribution applications used for environmental assessment.

3.4.1 Security and privacy for Environment CI

While automatic computer based monitoring systems have a lot of advantages, compared to manual sampling and analysis, on the other hand their adoption can raise many security and privacy concerns.

As automatic collected data are used for environmental impact assessment of human and industrial activities and to detect various kind of environmental issues, someone may have the interest to alter the data collected to influence choices made by the subject involved in the monitoring. Other threats may be trying to undermine data availability or worse the entire monitoring network or to gain access to environmental data when not publicly available.

The subjects involved in these malicious activities may be:

- Cyber criminals with the purpose of damaging environmental networks, managed by public administrations, to interrupt the measurement service
- Environmental activist that may alter data incrementing pollutant values to demonstrate that public administration is not able to grant good environment quality
- People with economical interest in industrial plants that wish to reduce pollutant values to avoid fines or to avoid expensive filter systems for pollutants reduction accordingly to limits set by laws.

3.4.2 Environment CI base security characteristics

From a general point of view, considering a typical environmental monitoring system, it is necessary to protect the monitoring stations, the data collection servers and the post elaboration and data management and assessment applications. These tree components of the monitoring network are exposed to different kind of risks and have different security needs, so they should be considered and discussed one by one.

3.4.2.1 The monitoring station

Depending on the kind of the environmental monitoring required, the monitoring station may range from a simple and small data logger with integrated sensors to a complex monitoring station with expensive analyzers and instrumentation, industrial PC and network equipment's hosted in a big container.

In both cases the station is located outside corporate networks and it situated throughout the country in places without supervision. This situation obviously implies two different type of risks: cyber-attacks through the network connection and physical attacks or vandalism on the station itself.

On simple data logger based stations, where at least an embedded OS is present, cyber security is achieved with software firewalls like IPTables, secure protocols for data transmission as SSL, VPN connections and so on. When data loggers with custom firmware are used, the only protection may be the difficulty of reverse engineering a byte based custom protocol and the fact that the firmware cannot be changed through the network connection. Beside this, for GPRS or UMTS connection better security may be achieved using a dedicated APN.

More complex stations with industrial PCs and standard OS like Linux or Windows may be protected with standard security hardware equipment's or standard security software and protocols. Even the analyzers connected to the data acquisition PC may be the subject of a cyber-attack, but usually they are only connected to the acquisition PC using serial cables or a dedicated internal network, separated from the communication network provided by routers or modems.

As for vandalism and physical attacks it is necessary to protect the stations with robust enclosures. Simple data logger based stations are protected with thick metal boxes, usually placed on high poles. More complex stations are constituted by a big container placed in an enclosed area, protected by locked doors and high metal fences.

3.4.2.2 The data collection server

The data collection server is a critical element of the system that must be protected. Typically it is located inside corporate networks so it benefits of the protection provided by corporate firewalls and networks. As it has to communicate with the monitoring stations, particular attention is needed to secure this kind of connection to avoid attacks performed through the monitoring stations or data loggers, where it may be difficult to have a very high level of security.

In particular, it is necessary to protect the software that controls the acquisition of information from monitoring stations, the databases and the networking facilities used to grant the connection with the monitoring stations.

3.4.2.3 Post elaboration and data management and assessment applications

Post elaboration, data management and applications used for environmental assessment are usually hosted on corporate servers and do not need to communicate with monitoring stations. For this reason they are not part of the core of the monitoring network and standard corporate security may be applied to grant the necessary protection level.

3.5 Financial services

3.5.1 Security and privacy for Financial Services CI

The banking (and insurance) markets operate in marketplaces that increasingly depend on flexible collaboration and rapid, Omni-channel transactions. There is exponential growth in financial transactions from mobile devices, in particular, and that leads to growing concern about data security as more and more

information is exchanged across mobile and collaborative networks. The most tempting of targets by criminals are the banks[1]. Cybercrime is the second most common type of economic crime reported by Financial Services, after asset misappropriation and in front of money laundering, accounting fraud, bribery and corruption.[2]

As the institutions that store and distribute funds, that provide loans and handle transaction processing, banks are potentially very vulnerable. The same trends can be seen in phishing: the method most commonly used to steal customer identities for online fraud. Many financial institutions are routinely subjected to Denial of Service attacks, both by conventional criminals and politically motivated hacktivists. Some recent attacks have installed hardware in bank branch systems to enable transactions to be manipulated via mobile networks.

The results can be devastating, with customer records being lost and reputational damage caused in ways that leave a lasting impact.

Financial services infrastructure is becoming more and more complex as new devices are arising, mainly coming from the IoT development because many IoT devices do not support the implementation of strong security controls:

- IoT / M2M enable wireless functionalities for ATMs and branch devices achieving improved services and more reliable data handling. ATMs now incorporate elements of the IoT to monitor and decide upon consumers' actions, overlapping the experience of the bank branch with the convenience of a traditional ATM, even offering optional videoconference with an actual human being. Sensors and networked cameras-enabled ATMs deliver faster notifications about cash availability, performance and required maintenance and are able to detect presence, shoot and analyze video.
- Wireless backup system allows remote branches to have failsafe connectivity for contingencies and recovery purposes.
- Centralized dashboards are based upon IoT middleware ability to use APIs to translate data collected from sensors and to aggregate the information from a range of systems. Reliable communications with these disparate systems are improving security and surveillance systems.
- Banks are using cellular GPS units that report location and usage of financed cars in addition to locking the ignitions to prevent further movement in the case of default.
- Banks might supply personal finances status to their customers in real time through the ability to access data captured by smart devices, using the connection of financial services to some of the ordinary household equipment.
- As in the household area, banks are interested in gathering IoT data from factories to support their lending decisions. By monitoring equipment performance, banks are informed up to seven months earlier than they usually would about cash flow diminishing. That allows bankers to restructure debts accordingly.

3.5.2 Financial Services CI base security characteristics

Principles and processes for effective cyber-security in the Financial Service arena could be addressed in seven key dimensions that are introduced and explained in this section.

Cyber risk management

Objective: Putting in place a **comprehensive policy** that covers effective Business Continuity Management and enterprise-wide Governance.

[1] The financial services industry topped the list of 26 different industries that cyber criminals most targeted. "Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry," Mandiant, September 23, 2013.

[2] 45% of Financial Services organizations have suffered economic crime during the survey period, compared to only 34% across all other industries. Threats to the Financial Services sector. Financial Services sector analysis of PwC's 2014 Global Economic Crime Survey.

Subject:

Based on lessons learned and best practices that financial services can borrow from other sectors, new techniques and controls might be applied under an organizational approach. These practices should include a proper analysis of the nature of the attack to understand the motives, tactics and patterns of the attackers in order to protect themselves with countermeasure and safeguard strategies.

- "Defense-in-depth" cyber risk strategy to be driven at the executive level as an integral part of the company core addressing known and emerging threats.
- Preemptive-driven approach to security by means of a dedicated cyber risk management team.
- The "human factor" in the defense framework can be empowered as part of a cyber risk-aware culture.
- Cybersecurity collaboration through industry relationships and public-private partnership.

  Financial companies are establishing industry associations to work together not only to benchmark and share expertise, but also to join resources to face risks that companies belonging to common industries likely undergo. National and International security agencies should share more information, and more quickly, under a natural flow of information with Financial Services stakeholders. Notably, timely feedback and engagement with regulators for best practices advice are both required.

  - The Financial Services Information and Sharing Center (FS-ISAC) is a mature industry forum created specifically for the financial services industry to share regarding cybersecurity in their sector.[i]
  - Securities Industry and Financial Markets Association (SIFMA) represents hundreds of securities firms, banks and asset manager's.[ii]

Cyber security advisory

Objective: Integrating every element that relates to security processes within **complete security architecture**, with full integration of IT and Operational Technology, ensuring that sensor information is also managed and protected.

Subject:

Financial institutions are viewed as one of the critical infrastructures that support the economic welfare of individual nations and worldwide, as they are operating under increasingly interconnected business relations.

In the current state of the art for IT architectures, any technological implementation can support improved data capacity and bandwidth, real-time operation, advanced tools for fraud assessment, etc. However, Financial Services companies should consider their overall cyber resilience capabilities across an IT integrated governance and global risk model comprehensive of:

- Risk mitigation (market, credit, operational, brand).
- Firm's "crown jewels" protection (customer information, corporate information, intellectual property, and infrastructure).
- Regulatory requirements compliance (consequences of these regulations on business processes, information systems, and infrastructure in the front, middle, and back office layers).
- Secured trading transactions.

Cyber operations

Objective: Keeping the entire IT environment secure, based on a Security Operation Center (SOC) and **incident and event management**.

Subject: Two type of incident and event management are prevailing in the Financial Services sector:

- Network behavior anomaly detection tools (NBAD).

  This is what NBAD is intended for: additional threat detection solutions, provided with powerful artificial intelligence, to permanently monitor network activities and generate alerts that often require further analysis to track down anomalies and reveal suspicious behavior.

- Security information and event management (SIEM).

  SIEM is defined as a complex set of tools and technologies working jointly to analyze log and event data in real time from multiple security applications and devices, providing threat detection, event correlation, incident response, and a holistic view into not only infrastructure but also workflow and regulatory compliance. Data can be collected from a wide variety of host systems and applications, security and network devices, portals, languages, drivers, UIs, and methods of collection and use cases.

Insider threat protection

Objective: Effective methods for ensuring that **data is not lost** as a result of internal attacks, routine migration or any other factor.

Subject:

Financial Services institutions should have an overall policy on data security requirements led by a comprehensive governance framework. In addition to technical solutions to countermeasure data leak, roles and responsibilities, compliance constraints, inventory, data classification and handling, and reporting needs on data assets are required to be set up as well.

Automation, data encryption, tokenization, chip cards and other solutions can be implemented to better protect bank's critical information assets and render stolen data useless to hackers. Data encryption tools are used to protect sensitive data around high-risk and high-value repositories that limits the value of raw data, such as debit card PINs, swapping over communications networks or left in storage.

Secure cooperation

Objective: Bringing the additional level of **physical security** that only integrated encryption technologies can offer, including biometrics, Public Key Infrastructure or use of cards and tokens.

Subject:

Security issues are straining Financial Services institutions in a myriad of different directions; even though banks have been traditionally fully aware of physical security, the banking industry faces nowadays what level of physical security to implement across separate branches: decisions about physical security are usually made company-wide and on the facility level. Another major concern is the increasingly convergence between cyber and physical security, where technology-enabled smart systems warn networks rather than operate over phone lines.

Additionally, although integration of security systems is quite ordinary in bank's infrastructure, there are cautions yet, due to compatibility issues and fear of an overall blackout instead of just a portion of it, if not integrated.

These are the main assets in a financial environment whose protection must be considered.

- Physical security zones, such as data center and branches.
- Environmental hazards (fire, flooding).
- Access control.
  - Traditional "keyed" solutions have been overtaken by "identity management" utilizing cutting-edge technologies such as facial recognition, keypads, card activated units, or biometrics.
  - Employee badges provide customized access instead of keys.
  - ATM kiosks, surrounds and panels. Security systems, including cameras, keycards and devices that protect against ATM theft. Anti-skimming devices.
- Surveillance.
  - Alarms and monitoring are expected to transmit signals through the internet, network or phone lines using dial-up, cellular, wireless or IP technologies, and should include alarm monitoring, panic button technology, several layers of physical security, remote video monitoring, and off-site back-up.

- Video surveillance (network/IP and analog cameras), ATM and building surveillance, collecting, retrieving, reviewing, and storing image capabilities, DVR's, integrated set of cameras, monitors and switching devices.
- Synchronized lighting and Intruder detection devices.

- Vaults, locked cabinets, equipment and paper storage, media storage.
- Power outages and fluctuations. Emergency services. Backup communications.
- Locks or other devices for PC, laptops, PDS, hand-held devices.
- Cabling and wireless equipment.

Digital identity & access control

Objective: From outside and within an organization, the greatest danger often comes from unauthorized access. Appropriate solutions deal with this critical issue through identity and **access management**, role and compliance management and building federated identity for secure single sign-in.

Subject:

The identification of information flows inside and outside Financial Services institutions is one major concern of a sound data governance policy. Furthermore, if the bank provides a wireless access for customers in physical branches, the public network must be isolated from the bank's private network. All staff-connected devices accessing critical data must be connected just to the private network.

Regulatory requirements and OpenData initiatives are also rowing in the same direction to widen how banks gather, manage, and share data. The so-called" democratization of analysis" is enhancing access to more employees and external stakeholders to use and analyze data instead of solely using teams of specialized data analysts.

Cyber intelligence

Objective: **Security analytics** to identify issues and threats from outside or inside in real-time, managing all areas of vulnerability and conducting forensic responses to any incidents.

Subject:

Financial Services organizations should carry out continuous risk assessment whereby reach situational awareness. Continuous monitoring activities, focused on both external and internal threats, can develop a situational awareness of the threat environment, capturing the risk indicators across the information layers so experience-based learning is supplemented and organization's defense is enhanced.

Financial services companies should also consider social media analytics to bring intelligence, cover brand prestige, and support crisis management.

4 CI security issues

4.1 General security issues for CI domains

There is a need to understand, identify, and analyze the interdependencies between the various systems. This is the greatest challenge and the most significant one. Such challenges are growing very critical when it comes to infrastructure at the state level. These infrastructures affect all aspects of daily use including oil and gas, water, electricity, telecommunications, transport, health, environment, services liberty and government, agriculture, finance and banking, aviation and other systems that at the basis of their services are essential to state security, the prosperity of the state, social welfare and more. So the big challenge is the dependence and independence of these different systems and complexity factors interplay in protecting critical infrastructure. These include business, social and political, technical, legal, regulatory, public policy, health and safety may disrupt the infrastructure activities. Environmental systems influence many aspects of functioning systems, emergency operations and rehabilitation and reconstruction operations. The extent to which these properties are affected infrastructure and interactions, may contribute to or exacerbate existing infrastructure from one to another.

These relationships can have a geographical, cyber, physical, or natural connections.

When multiple critical infrastructure systems are connected together as chain of interconnected systems, it is important to examine and protect not only each system separately, but also all systems' interconnections required for the entire infrastructure to function properly.

Many CI Facilities can be close or even physically connected to each other, but can also be located on different sides of the planet. Since many modern CI facilities are now being supported and managed by modern computerized systems (such as electricity networks being controlled by SCADA systems), geographical dependencies become less important and cyber and information security interdependences become more and more relevant when considering all-around protection measures to the centralized CI control systems.

When centralized control systems are required to manage geographically distant facilities, the communication with each facility becomes dependent on network connections, making the entire infrastructure vulnerable to various network problems and vulnerabilities, such as cyber-attacks, network connection outages, etc.

The selected physical location, as well as the deployment methods of many critical infrastructure facilities can influence (directly or indirectly) their vulnerability to various physical and natural threats. Furthermore, numerous distant CI facilities can all be affected by one local physical or natural event.

For example, power lines can be hung underneath roads or bridges. They are physically connected to electricity, communications and transportation infrastructure. There is a mutual dependence in many cases, but usually due to the proximity of infrastructure status, will not interfere with other infrastructure example as many vehicles travel daily on the bridge.

On the other hand when the bridge itself will be damaged, electricity and communication infrastructure as well as transportation, will directly be harmed.

By applying defense in depth, such critical infrastructure will be able to keep existence and functionality.

Attacks

The constant technological advancement and the slow but constant shift to fully computerized systems (including mobile and cloud based control systems) lays a solid foundation for innovation in the products and services area, but also makes the infrastructures vulnerable to new types of attacks, such as cyber-criminal-attacks, digital-frauds, sabotage, digital warfare and more.

	[iii]Cyber Crime Actors	Criminal Motives	
■ Hacktivists: Sabotage systems to make a political or social statement. ■ Cybercriminals: Range from lone actors to large crime organizations. Goal is to steal identities and money. ■ Nation States: Seeks secrets or intellectual property to help their host nation gain strategic advantage. ■ Insiders: Employee, contractor, supplier or business, partner with system access, steals information or sabotages systems.		■ Politically Driven: Attackers carry out a group's goal to destroy an institution's economic stability or damage its reputation by compromising information or systems. ■ Espionage Driven: Attackers intend to steal sensitive information to sell to be used by a third party. ■ Financially Driven: Attackers seek to compromise systems to commit theft or financial fraud	

- **Advanced Persistent Threat**

  APT consists in undercover and permanent computer hacking routines to gain access to an organization's resource. When the fake person reaches access, they often stay unrevealed for a significant lapse of time whereas quietly stealing data, committing fraud, or jeopardizing its reputation.

  Although phishing email remains a significant attack mechanism for cybercriminals to mislead employees into downloading malware, there is an increased appetite toward social media platforms. The bulk of the social media scams were manually shared and are lucrative for cybercriminals because of their quick propagation, due to the fact that people are more likely to click on something posted by a friend.

- **Corporate Account Take Over (CATO)**

  In a CATO attack, cyber criminals impersonate the business identity and send fraudulent transactions to accounts controlled by them. Institutions under-equipped with limited security controls and safeguards are especially vulnerable to a CATO attack. Impacts stem from this form of cyber-crime could be substantial, and likelihood of recognition for these thefts is still low.

- **CryptoLocker**

  CryptoLocker is a type of malware that damages by encrypting data, avoiding access to the data on the infected computers. Once the computer is bugged, cyber criminals request the victims for a payment so their data can be decrypted and recovered. Usually the payment is demanded within three days since the attack through a third-party payment method (i.e. MoneyPak, Bitcoin). Obviously, there is no guarantee that payment brings the promised decryption key.

  This malware is typically spread through malicious attachments included in phishing emails and is capable to encrypt files within shared network servers and file shares, USB devices, removable hard disks, and even some cloud storage drives. Furthermore, if one computer on a network becomes infected, mapped network drives might also turn infected.

- **Distributed Denial of Service**

  Not only DDoS attacks fill up networks with a massive amount of connection requests, turning them off to deal with legitimate user requests, but DDoS attacks are often used as a smokescreen or camouflage for other types of network intrusions as well, because whereas response team focus on DDoS mitigation, attackers have a greater chance of secretly overtake firewalls to tackle data and financial theft.

- **Insider and Internal Threats**

  Any stakeholder can compromise company's security if access has been granted to systems and/or sensitive information. Employee, contractor, supplier, or partner has the chance to harm company assets

and prestige, both intentionally or unintentionally, even more with the pervasive trends of BYOD, cloud-based systems and use of personal USB storage devices.

- **Physical factors**

  In a recent attack on Santander Bank in the UK, came into a branch and installed a KVM (keyboard, video, and mouse) switch, a device that enables one computer to remotely control many others by manipulating their keyboards, mice, and video screens.

  BYOD truly has consequences. These devices are now part of the firm's ecosystem with no control over them. This is the rationale behind the corporation's consideration about real cost-savings of BYOD trend in opposition of an undermined corporate security. The required extension of corporate security means to protect personally owned devices belongs to a sensitive territory, so mandatory controls as a consequence of employment can be foreseen.

- **Supply Chain Infiltration**

  Cybercriminals are continually devising new ways to infiltrate organizations, pretending to be supplier employees to install infected equipment or hardware able to tamper transactions via mobile networks.

  Trusted providers of software and hardware have been targeted in recent years by cyber criminals seeking to gain physical and technical access to institutions.

- **Trojan-based attacks**

  Trojans addressing institutions have become one of the most widespread threats on the internet today. According Symantec report, nearly 95 percent of the raided organizations belong to the financial sector.[iv]

4.2 Security issues for the Medical and Healthcare domain

Vulnerabilities that must be considered in the field of health may be due to various aspects and all of them should be collected by the CIPSEC project. Besides physical vulnerability, the uncontrolled access to technical rooms where the racks of communication or connection rosettes are enabled in public spaces, we consider that, at least, the following points must be respected to ensure confidentiality, integrity and permanent availability of the clinical patient data:

- All access to applications installed on the servers should be secured via username and password and contrasted with the Microsoft LDAP. It must exist a policy of permissions that could be defined by the hospital's Information Systems department (SI).
- Any equipment/computer connected to the network must be known by SI, inventoried and its firmware updates should be monitored so that each supplier could be aware of the vulnerabilities found and be responsible for their immediate correction.
- It must be possible to control somehow the usual practice of the hospital staff and the various providers to use their personal USB on the devices connected to the network to obtain information from them or rescuing protected health information.
- It should be possible to implement and update some security policies so that unauthorized users cannot get administrator permissions over any machine to avoid the voluntary or involuntary installation of any malicious software from the web. It must be possible to limit the VNC TeamViewer type remote connections or giving access to teams from outside.
- Staff should be made aware of the impact of a cyber-attack, do not leave passwords written on paper or pass them to peers and make dissemination of informational messages regarding the threats that may arrive via email. Under no circumstances should open suspicious emails or send passwords in applications that handle clinical data.
- Connections from outside via VPN must be monitored, detecting the direction of the information flow and the amount of transmitted data, all in real time. The registers should record the right and failed accesses to virtual private networks (VPN) as well as the connection times and the amount of data sent and received by each particular user.
- It must be maintained updated the security policies in the 2 existing firewalls and accurate contingency plans for possible cyberattacks over them ought to be drafted.

- It should be possible to detect processes of massive search for IPs of computers on the network, alerting with immediacy and identifying the unique equipment that is conducting this process and the particular application that is running on it.
- You need to scan and monitor all the equipment's connected in every moment via WIFI and detect those that could be considered abnormal, not officially temporary registered or included in any permanent inventory.
- Attacks can not only come from within the Hospital since the HCB is composed of different buildings, all interconnected by fiber belonging to the contracted operator (Vodafone), so the attack can be indirect through their infrastructure.
- In addition to the efforts focused to identify and prevent vulnerabilities, the hospital should minimize any potential threat by detecting and stopping any malware before it can achieve its goals. Among the tools available always should be included: antivirus software, services of detection and removal of spyware, intrusion prevention systems (IPS) and firewalls.
- It is essential to design with the help of experts a contingency plan that includes all those mechanisms that guarantee the absolute functional continuity of the Hospital after any incident. It is necessary to ensure the recovery and immediate use of the infrastructure and the equipment's as well as the custody and privacy of all vital patient data.

4.3 Security issues for the Environmental Monitoring domain

Considering the topology of environmental monitoring networks, consisting of measurement stations, located throughout the country in places without surveillance, and of data collection and elaboration server, located inside corporate networks, it should be better to examine security issues specifically for the stations and for the servers.

In general both the stations and the servers may be the subjects of attacks like account takeovers, advanced persistent threat (APT), distributed denial of server (DDoS), internal and external threats and, for servers only, cloud base attacks.

4.3.1 Security issues for measurement stations

The way a measurement station may be attacked depends on the technology used for the connection to the data collection server. The stations connected via the Internet, using wired or wireless technologies, are subjected to the typical cyber-attacks coming from the Internet. For stations directly connected to data collection servers, using ISDN technology, attacks could come mainly through connection attempts on the ISDN line.

For all the types of stations the attacks could get even physically entering the station, then trying to log into the station PC or using a cable connection added to the internal network of the station.

The monitoring stations, particularly the ones with ISDN connection, if compromised remotely or directly, could be used as an entry point to attack the data collection servers.

Simpler monitoring stations based on data logger with custom firmware as a result of an attack may stop working correctly or the data flow towards the data collection server may be altered.

The stations with a data acquisition system based on a PC and connected via a standard router, offer better way of data protection but are more interesting for cyber-attacks and, if compromised, may be used as bridge to attack data collection servers or other users of the Internet. If a station PC is compromised by viruses or Trojans, causing very high system load, near real time data acquisition may be affected as well.

Using a compromised PC, it is possible trying to alter the configuration of the environmental analyzers connected to the PC via serial ports or LAN.

4.3.2 Security issues for environmental monitoring servers

The data collection servers and the data elaboration and evaluation appliances, hosted in corporate buildings or in cloud computing, are subject to common security issues. Data protection can be achieved with standard security techniques.

For environmental monitoring network with a topology, where connections originate from the data collection server towards the stations, there are not additional security issues: it is usual for server appliances to connect to external resources to obtain data for elaboration.

If the network topology requires the stations to connect directly to the data acquisition server, then more security issues have to be faced. In this case possible attacks could come through the monitoring stations.

In all cases attacks may come:

- Indirectly from the Internet, where the corporate network is compromised, for example, through other servers that expose services on the Internet;
- From the internal corporate network by employees, contractors or suppliers with system access.

4.3.3 Impacts

When an environmental monitoring network is compromised by a cyber-attack, its capability of providing environmental data and reliable pollutant measures may be partially or totally broken. If only a small percentage of the monitoring stations is not operational, the network may still be able to fulfil the purpose for which it was deployed. Any bigger functional disruption may lead to:

- Loss of the reputation for the subject operating the network
- Costs to recover to a fully functional status
- Loss of environmental information, needed to public administration to take decisions
- Impossibility to fulfil legal obligations about environmental monitoring

4.4 Security issues for the Transportation domain

4.4.1 Potential internal threats

Internal threats in the context of railway systems could be employees of the operator or external service personnel, which has the order to repair or maintain parts of an interlocking system and have valid access to the systems.

These can be divided in the Internal Perpetrators, which have a certain target and act on premise. They may be driven by the wish to damage certain parts of the system out of personal motives. Besides this they may be offered money from other potential attackers.

Also, the other group of potential threats is the normal employee, which may perform unwanted attacks on the system due to his actions. E.g. an employee could infect a system with a virus while trying to charge his smartphone via USB.

4.4.2 Potential external threats

The group of external threats in case of railway systems is widespread and consists of high and low potential attackers.

- **Terrorist organizations**

  As terrorism is getting more and more popular within the last years, also railway systems have to deal with this attacker group. Such an attacker could try to produce a massive outage of interlocking system or to find a way to enforce collisions of trains to produce fear.

- **Governmental Organizations**

  GOs in normal cases are working in the area of industrial espionage, which is not relevant for railway operators. In case of conflicts these organizations also could try to completely disable the railway operation by taking out the interlocking systems.

- **Criminal Organizations**

  Criminal Organizations try to find a way to gain financial profit from their actions. Most likely this could be done by finding a way to disturb the railway operation and then blackmail the operator of the affected infrastructure.

- **Competing Companies**

  Competing companies can exist in two types. The first type are other railway companies, which want to be better than their competitors. The second type are the competing system providers, which could try to take out systems of their competitors to gain a better market position.

- **Activists**

  Activists are trying to stop transports, which are against their way of living. E.g. transport of nuclear material.

- **Hackers**

  Hackers are individuals, which most likely come across railway systems only for testing issues, like trying to find a way into the interlocking system but will not try to produce damage.

- **Cyber Criminals**

  These are the more professional version of hackers and could try to gain profit by blackmailing the operator.

4.4.3 Identify any potential attack locations

- **Inside the track field**

  As track fields span over wide areas, where no personnel is located, an attacker can easily enter these areas and try to find a way to enter the network infrastructure, because the cables are located besides the tracks. This is becoming more important, as the new interlocking communication protocols are based on standard IP communication.

- **Inside interlocking building**

  Inside of the interlocking building also network infrastructure is present, but an attacker has more challenges when trying to enter these buildings. All interlocking buildings in Germany are equipped with intrusion alert systems and also have special doors and windows to prevent intrusions.

- **From operation center**

  For operation centers the same measures apply as for the interlocking buildings. Besides this several operators are working in such an operation center, which poses an additional challenge.

- **Workstation of vendor**

  As vendors from time to time have to maintain some of the provided components, their service workstations could be used by an attacker.

- **Over the internet**

  Besides the former mentioned points also the internet could be used for an attack, but for doing so the attacker has to pass several firewall systems as the internet access is only available via the corporate network and this is separated from the interlocking network by at least one firewall system.

4.4.4 Impacts

If a railway transportation system is attacked the results of the attack can have a wide range. In every case the transport operation is influenced and one or more of the following impacts can occur:

- **Service Interrupt**

  Due to the attack the transport service is interrupted. This impact can have several severities, e.g. low service interrupt could be the outage of some signals of points, which results in additional time for traveling from one station to another. A heavy service interrupt could be the outage of one or more interlocking systems, which would result in nearly no railway transport on the affected routes.

- **Weakened Safety**

  Safety is the highest premise in the railway domain. Due to an attack the safety could be weakened, which then could result in damages due to human errors because of the missing safety functionalities (the error rate of a SIL4 interlocking system is 10^-9 to 10^-12 while the error rate of a human is estimated with 10^-3).

- **Material Damage**

  Material damage is one of the impacts that could occur due to an attack. This impact could also be translated to costs. This impact consists of damaged infrastructure and vehicles like trains. Besides this also external damages are included, like damaged cars on crossings or other material damages that could happen.

- **Loss of Repudiation**

  As railway transportation is used by a large amount of persons either for going to work or for travelling to holiday trips the passengers have to trust in the safety of the transportation system. Otherwise they would switch to bus or car. Therefore repudiation is important for railway operators.

- **Human Damage**

  One of the worst impacts in the railway domain is the loss of human lives. This can occur if trains collide or crash into train station.

4.5 Security issues for Financial Services domain

Needless to say that an overpopulated background of cloud, mobile, and emerging technologies are both supplying a consistent foundation for innovation in products and services and providing cyber criminals with an extended ability to launch damaging attacks.

4.5.1 Technological, operational and organizational issues

Attacks

- **Account takeovers**

  Cyber criminals have eagerly realized not only how to trespass financial and market systems that interface with the Internet, but also how to tamper system users rather than the systems themselves in order to get access to existing financial systems, and carry out account takeovers and unauthorized transactions. Automated clearing house (ACH) systems, card payments, and market trades are major targets for cyber intrusion.

- **ATM Cash Out**

  In ATM Cash Out cybercriminal earns access to and modify the configuration on ATM web-based control system used by small- to medium-sized financial institutions.

  Massive losses can stem from ATM Cash Outs. Since an increase activity in these types of cyber-attacks has been reported, financial institutions must face this threat by reviewing the appropriateness of their controls over card issuer authorization systems, ATM setting systems, and fraud detection and response processes.

- **Cloud-based attacks**

  Most Financial Services institutions are already using cloud computing business functions to thrive in flexibility and time-to-market agility. However, security requirements in terms of customer information protection and standards and regulatory compliance are preventing them from taking full advantage of cloud-based technology.

  Claims management, insurance brokerage, and even e-mail outsourcing are useful cloud-based applications for Financial Services companies, but security and privacy concerns arise because whereas just a handful of authorized people have access to the administrative servers within the organization, there are hundreds of people with such access at the third-party cloud provider side.

  Attacks triggered via the cloud are a huge worry for CIOs in the Financial Services industry: cloud-based botnets to disturb processing power, undesirable exploitation of NFCs, Distributed Denial of Service (DDoS), and hacks on authentication platforms are well-known.

- **Cyberterrorism and State-sponsored attacks**

  Since banks are at the very core of the financial system, particularly those departments involved with enabling payments, clearing, and linked with National Central Banks, sponsored terrorists might attack countries to knock down or to provoke a disruption of the financial systems.

- **Payment Card Skimming**

  A skimmer located to the surroundings of an ATM enables criminals to have a glance at keys and personal IDs to sell them or to make phony cards to withdraw money from the affected accounts. While companies continue to deploy new electronic and wireless payment systems, hackers are conceiving Bluetooth-enabled wireless skimmers to instantly download data.

- **Web applications**

  Financial web applications, such as online banking, credit card payment or online brokerage, are fully compromised because they lead to data attackers can monetize, either attacking application vulnerability or faking user credentials.

Cross-border security

Financial Services institutions traditionally lack an organizational wide integrated approach to adequately protect data on risk-based decisions.

Concerns over privacy of sensitive information in the context of cross-border data exchanges have resulted in countries adopting specific national and regional regulation with an increasing number of countries introducing mandatory disclosure of data breaches, as a consequence of shared services and decentralized processing facilities.

Increased information security threats from outside the country are boosting Financial Services institutions to discuss about the need for standards as a means of keeping management aware of threats that originate in other nations. This issue is particularly heightened in Europe, where standards are competing and contradictory across borders and where standards-setting procedures often take years to reach agreement, whereas cyber criminals can easily outpace them.

Financial Services industry worries about foreign nation-states organized crime, and worldwide cyber terrorism. African government initiatives to deploy broadband in that region are coming along with an uprising in cybercrime from Africa. Cyber security experts also notice that cyber criminals are relocating to South Africa from Europe, due to empowered cooperation between law enforcement agencies in the EU.

Offshoring

Pervasive business models such as outsourcing, offshoring, and third-party contracting driven by the current economic crisis scenario may have further blurred Financial Services institutional control over IT systems and access points.

Regulatory compliance

Financial services organizations should develop an all-encompassing compliance policy by identifying all the geographically and industry applicable requirements followed by cleaning overlapping obligations. Although information security should be risk based and compliance-driven it is equally important to get the organization ready to respond to previously unknown threats in a timely manner without converting compliance in the sole concern.

Response time

According a Deloitte Center for Financial Services analysis of an annual report on data security by Verizon found that 88 percent of the attacks initiated against Financial Services companies are successful in less than a day. Only 21 percent of these are discovered within a day, and even worse, in the post-discovery period, only 40 percent of them are restored within that one-day time frame.

Besides traditional reluctance of banks for sharing their findings about infiltration and entailed impact, there is a major lack in today's detection and response methodologies: whereas organizations roll out a complex set of security solutions, cyber-attacks remain unrecovered for months. Additionally, detection systems often produce an overwhelming amount of alerts that take hours to be adequately handled.

Banks must be quicker in raising the alarm when they find suspicion or trail of cyber criminals.

Robotics and artificial intelligence

Nowadays robotics and artificial intelligence applications are being applied to end-to-end processes, replacing people in roles ranging from routine back-office operations, anti-fraud programs, customer relationships, outstanding payment monitoring, to loan officers or other general compliance functions.

Third party security

Use of third-party vendors and outsourcing relationships create an outsized increase in risks.

Economic crisis scenario has been encouraging Financial Services institutions for years to ramp up with use of third-party information and technology providers in the quest of lessening their operational costs.

Some firms consider that supply chain is the major vulnerability so focus on contractors, as the weakest link, must be applied. In other cases the transfer of services or data to the cloud is the big deal because of the lack of control upon their data. An enhanced understanding of what information third parties, or even fourth and fifth parties and further downstream, have access to is another issue for Financial Services security responsible.

There is a challenge to properly manage breaches originate on vendor networks, so Financial Services ranked assessment of third-party suppliers as the utmost concern to their information security efforts. For doing that, the use of risk based security guidelines and agreements can support both sides of the chain for a seamless exchange information and for communicate expectations and concerns about services that are being provided.

Wholesale payments[v]

Financial Services institutions are vulnerable to a variety of economic, reputation, legal, and operational risks in provisioning wholesale payment services and performing related processing to counter parties. Fake transactions involving inter-and-intra bank payment and messaging, wholesale payment, clearance and settlement functions both in-house and with third parties, may entail financial loss and compliance risk.

4.5.2 Impacts

It is extremely significant than Financial Services institutions recognize that they cannot quantify losses from attacks. Furthermore, often the impact of a security breach needs months or even years to be properly addressed and quantified, due to faulty corrective measures, delays in discovering intrusions, brand erosion or long-term litigation.

A plethora of potential impacts comes from the digital disruption in the Financial Services firms, and massive cost of failure could show up, such as regulatory penalties, lawsuits, lost revenue, brand damage and spoiled shareholder confidence.

Brand reputation

The mere reporting of a security incident may damage brand reputation for Financial Services companies, which is a common reason businesses hesitate in reporting breaches. Even more, subsequent spear phishing attacks on their customers have been detected by firms that previously informed about security issues.

Far beyond the immediate financial impact, the consequences of a security breach can spread from brand and reputation damage to lessen turnover, affected consumer faith, lower share prices and greater regulatory scrutiny.

Business disruption

The pervasive impact of cyber-crime has increased with Omni channel banking and the Internet of Things financial applications. In addition, there is a growing trade of cyber-crime tools, and uprising threats from organized crime. Financial Services firms expecting that they will not be attacked are plainly naive, looking at a context in which 37% of respondents reported a double figure increase in cyber security incidents.[vi]

Verizon's dataset revealed that most data breaches affected organizations in the financial, accommodation, information, and public sectors. Web apps accounted for the greatest number of confirmed data breaches, particularly in the finance, information, entertainment, and educational sectors.[vii]

Financial Services institutions are not risk-free with regards to cyber-attacks affecting the global supply chain, especially around commercial Internet usage. Loss and disclosure of sensitive data affect Financial Services on the ability to run business and severely impact reputation and associated costs of mitigation, litigation and notification of compliance, leading to fines and solvency issues.

Financial organizations and assessment institutions, such as Financial Conduct Authority (FCA) are deeply concerned by potential business disruption stem from IT incidents as having the potential to unfold an adverse effect on the soundness of the financial system.

Cost

A cyber-attack can drag a business through experiencing massive financial losses and extensive litigation. A security incident affecting compliance for a Financial Services institution can also provoke regulatory fines.

Traditionally, Financial Services organizations have used the well-known cost-per-record amount to rate the costs of a data breach, covering detection, escalation, notification and after-incident response.

Although this approach is easy to calculate it fails to distinguish between minor and large-scale breaches. Larger organizations experience higher losses per breach because they have more records and thus higher overall costs. As insurers become increasingly reluctant to estimate potential losses by means of the cost-per-record technique, Financial Services institutions are progressively adopting new breach-cost models that reckon for uncertainty as the Big Data trend widen the compromised record volume.

Destruction of critical infrastructure

Point-Of-Sale attacks were the second top breach pattern observed by Verizon in 2015, which have targeted some Financial Services companies like payment processors and card issuers.[viii]

Regulation

Some important regulatory guidelines are summarized below:

- The European Banking Authority's Final Guidelines on the Security of Internet Payments, December 2014.
- European Central Bank, Recommendations for the security of internet payments, January 2013
- E-Privacy Directive (2002/58/EC).
- International Standard Organization Guidance (ISO/IEC 27001:2013)
- Publically Available Standards (PAS) 555.
- Information Security Forum's 2014 Standard of Good Practice for Information Security
- Government's Cyber Essentials Scheme, June 2014. Gov.UK

Cyber security has been embedded in regulations for years but as governments enact more privacy laws, the risk of discrepancy between countries increases, creating more hurdles for counteract to cyber-crime. Some of these regulations can cause severe penalties, such as the European General Data Protection regulation in which firms may be penalized 4% of global turnover for non-compliance.

Rating

Rating points to measure the effectiveness of companies and countries for abiding and managing risk. Rating agencies consider cyber risk as a major threat to solvency not only because of the significant impact of an event but also because the ability to react to that event. Rating agencies qualifications can have an economic effect on countries and corporations.

The rating of insurers can entail also consequences for their customers; if rating for a Financial Services institution falls below a certain level, it will be unable to access to mitigation capacity and will become more exposed to risk. Besides, insurance rating downgrades can prevent access to A-rated capital, involving the likelihood of defaulting on claims.

Systemic failure

Far beyond the Financial Services industry, there is unanimous recognition that financial institution blackout can have cascade effects across borders, entire segments of the Financial Services industry, and, eventually disastrous consequences upon business, global economy and society.

5 Market solutions for CI domains

5.1 Cross-domain solutions

5.1.1 Data

5.1.1.1 Encryption file systems

Description

Disk Encryption technology refers to the conversion of clear-text code and information files stored on a hard-drive, into a bit-by-bit encrypted information, inaccessible to a third party without knowing the passcode or without holding the encryption key.

Disk encryption technology implements various encryption solutions, such as encryption software or dedicated encryption hardware, to encrypt every bit of data that goes on the disk.

“FDE” or “Full Disk Encryption” term, may often suggest that the entire disk is encrypted, including the bootable operating system partitions. This full encryption, often doesn’t include the MBR (master boot record) to allow initial access to the hard-disk, to start the decryption process upon authorized access. Even so, there are some hardware-based FDE systems that can actually encrypt an entire boot HD, including the MBR.

Usage

Full Disk Encryption is used in all sorts of environments, organizational and private alike.

The main idea behind this solution is to protect data-in-rest (statically stored on the HD) from unauthorized access, by physically accessing the computer or HD, in cases such as a stolen laptop or a PC, containing sensitive information, stolen from a corporation.

It is important to note that these solutions don’t protect against unauthorized network-based access, or other common attacks such as malware or viruses.

Available solutions on the market

Most operating systems have some sort of built-in encryption abilities, such as the EFS and Bit-Locker for Microsoft Windows systems, FileVault for MAC users, and various encryption solutions for Linux, depending on the distribution and version of OS. Third-party solutions can be divided into open-source and free solutions and commercial solutions.

- Open Source:
  - VeraCrypt (Successor to TrueCrypt)
  - AxCrypt
  - GNU Privacy Guard (GnuPG
- Commercial solutions:
  - Symantec Drive Encryption
  - Trend Micro Endpoint Encryption
  - McAfee Complete Data Protection

5.1.1.2 Online storage and backups

Description

Online or Cloud storage, is a data storage model in which all digital data is stored in a logical storage pools, while the physical infrastructure supporting it, can span across multiple servers in multiple server farms and even in different countries. The physical storage environment is typically owned and managed by a separate hosting company, responsible for the entire infrastructure, and for keeping the data available and accessible. The host company can also offer various backup plans and implement various security measures to protect the data (measures such as secure access, data encryption, multiple backups, etc.)

Cloud storage services can be accessed in various ways, depending on the service, and may include dedicated end-point applications, web-interface, and some additional interfaces, such as dedicated APIs.

Usage

Online and Cloud based storage and backups are becoming more and more popular, with almost every company putting at least part of its non-sensitive information in those storage solutions.

Some companies rely entirely on Cloud based storage, thus putting all their information and files online and maintain various safety measures to secure their information.

Private Cloud solutions are also very popular, allowing an end-user full access to his/her files from virtually anywhere, via a dedicated application or via web access.

Available solutions on the market

Most popular enterprise-level solutions includes the following:

- Amazon S3 (Simple Storage Service)
- Microsoft Azure
- Google Cloud Storage
- Rackspace
- Dropbox for business

5.1.1.3 Data Loss Prevention (DLP)

Description

Data Loss Prevention (DLP) is a way of ensuring that corporate users will not, accidentally or intentionally, transfer or copy sensitive information outside the corporate network.

The term is also used to describe security software products, used by network administrators and corporate security teams that allow control over what data is considered sensitive and what the corporate users can or cannot do with it.

The DLP products implement business rules and business security policies to classify and protect confidential and sensitive data. In essence, the software prevents accidental or malicious disclosure of information via most known electronic methods, such as: Corporate email, web sharing, cloud storage, external USB devices, physical printing of documents, and even screen capturing (print screen).

Usage

DLP solutions are very common in big and mid-sized companies, containing sensitive information, in virtually any industry.

Whether its customers' private data (like credit cards, SSN's, etc.) or corporate information such as financial information or intellectual property of the company, this kind of information, if leaked, can cause damage to the company and even expose the company to various law suits.

The DLP solutions are intended to prevent such information disclosure across the entire corporate network, using local end-point agents, network monitoring, implementing web proxies, etc.

Available solutions on the market

There are many DLP solutions on the market. Some of the big names include:

- Forcepoint (formely known as Websense) Triton-APX DLP
- Intel Security (McAfee) – Total Protection for Data Loss Prevention
- CA – Data Protection (formerly known as CA DataMinder)
- Symantec DLP
- Trustwave DLP

5.1.1.4 Information right assignment

Description

Information rights assignment refers to the process of managing sensitive information access and protecting it from unauthorized access.

Most organizations have some sort of hierarchy and different departments, responsible for various aspects of the organization (for example: Management, Sales department, Finance department, HR department, etc.).

In most cases, the different company departments only deal with specific data, related to their department, which means that they don't necessarily need access to data related to other departments.

These conditions allow a granular information right assignment, in which the users from one department can't access (read or make changes) files of other departments.

Usage

Information right assignment can be performed in various ways, with NTFS permissions being one of the most popular, allowing granular control over access rights to files and folders, based on LDAP users and groups.

NTFS rights management is implemented in almost every company, running some sort of centralized storage.

Some other implementations are available for Linux based and OSX systems that also divide access rights to data, according to users and groups in the system environment.

5.1.1.5 Password vault

Description

Access to almost every service today, requires some sort of authentication that involves (at least) a username and password.

This is especially true to privileged access to various corporate services and infrastructures, such as servers, network devices, and security appliances.

The large number of personal and corporate passwords, in use by each user, combined with the struggle to remember them all, may lead to a use of weak and/or repetitive passwords for many different services, personal and organizational alike.

This kind of behavior is very common among all users and may lead to major security issues that may eventually allow an unauthorized access to organizational assets and sensitive information and cause serious damage to an organization.

The Password Vaults, also known as Password Managers, were created to address these exact issues.

Password Managers, store all users' passwords, locally or online, in a secure and encrypted manner, and protect all of them, using one very strong master password, selected by the user.

Many pass managers also include various ways of generating strong and pseudo-random passwords automatically, thus reducing the need to think of new passwords manually.

Some solutions also offer various ways of automatically filling in the passwords, on various authentication platforms, thus eliminating the need to know the current passwords for each service the user uses.

Usage

Password Vaults are commonly used for private use. But can also be implemented in organizations for various use cases.

Some password vault solutions are enterprise oriented (such as the Cyber Ark's Enterprise Password Vault) and allow integration with LDAP services and other custom authentication methods specific to corporate use.

Implementation of such password managers and vaults in a corporate environment, can significantly contribute to the overall security of the authentication process.

Available solutions on the market

Password Vault (or Password Managers) can be divided into two main groups: Private use oriented, and Enterprise oriented.

Though both can be implemented in an enterprise environment, the enterprise oriented solutions, usually offer additional management options, such as multi user management, and full (or partial) integration with LDAP services, such as Active Directory users.

Some of the enterprise level solutions available are:

- Cyber Ark – Enterprise Password Vault
- Micro Focus – NetIQ - Privileged Account Manager
- DELL - Privileged Password Manager
- IBM - Security Privileged Identity Manager
- Manage Engine – Password Manager Pro

5.1.1.6 Digital vault

Description

Digital Vaults represent a modern technology solution, to the more traditional physical vaults, in use by many companies to store sensitive and critical information or objects.

Though many companies today, still store physical copies of sensitive documents inside physical vaults, the growing need to access this information or documents on a day-to-day basis, by numerous people across the entire organization, requires a technological solution that comes in a shape of "Digital Vault".

Most Digital Vault solutions contains a list of key security features, essential for securing sensitive information across the organization.

The vaults solution should include a granular control over access rights of users across the organization, only allowing access to authorized personnel to access the vault infrastructure, and then manage specific access rights to different safes or "digital deposit boxes" inside the vault itself. This way, a more granular control over different sensitive information access can be achieved.

The access control should also incorporate abilities to control the allowed time intervals, in which each user is allowed to access the sensitive info and also the allowed geographical and network locations, from which the access would be allowed.

Additional abilities should include: Full auditing of access to the information, including user information, access timing and what type of action was performed on the documents (read, change, delete, copy, move, etc.) and the ability to control access to the vault/safe using multiple authorization levels (such as a security officer, or a manager, that should explicitly allow access by clicking some sort of authorization option, when a user wants to access some sensitive info.

Digital Vaults are usually designed to protect its data using various methods, such as encryption, and also implement network security measures, independent of the security measurements implemented in the rest of the organizational network, thus making it easier to protect the sensitive information and documents, without the need to reconstruct the entire network around the vault.

Usage

The use of digital vaults is very common among corporations dealing with sensitive information, especially if it needs to be transferred securely to third parties. Digital vault solutions often allow a secured client-based access to the vault by external users, thus allowing co-operating companies to securely share sensitive information, without actually allowing access to the company's servers or network, except the digital vault and safe needed to be shared.

Available solutions on the market

Cyber-Ark's digital vault solution is considered one of the major players in the digital vault market today.

Covertix is yet another major player in the data protection business, offering similar vault based solution called SmartCipher Enterprise.

5.1.1.7 Access/change auditing

Description

Almost every organization has some sort of sensitive information that needs to be protected, and accessed only by authorized personnel on "need to know" basis.

Access and change auditing, refers to various monitoring and auditing mechanisms, allowing a full record of all actions performed on this kind of information.

The auditing process usually includes full mapping of the sensitive information in the organization, and a definition of when this information can be accessed and by whom.

The second step includes an implementation of an auditing system, configured to log all actions performed upon the mapped sensitive data (for example: digital documents or various data-bases). These actions may include actions such as: Read, edit, delete, move, copy or changing permissions on various files or databases.

These systems will usually also record additional information, such as the time of action, the user that initiated it, and the details of the computer the user used to perform those actions (such as its IP address, username, operating system, etc.).

Most systems also allow integration with centralized monitoring software, such as SIEM solutions. This integration also allows configuration of warnings in live mode, meaning unauthorized access can be monitored and detected as it happens. Allowing quick response by the IT and security crews.

Usage

Various auditing are used in the majority of organizations, allowing varying levels of auditing and control over the sensitive information of the company.

Available solutions on the market

Various companies offer different monitoring solutions, allowing different aspects of access monitoring. Some of the known brands include:

- Imperva
- Fortinet
- Guardium
- Netwrix

5.1.1.8 Data Redundant Array of Inexpensive/Independent Disks (RAID)

Description

"RAID" stands for "Redundant Array of Inexpensive/Independent Disks". As the name suggests, RAID is a data storage virtualization technology that implements multiple physical hard disks into one logical unit, in order to achieve data redundancy (thus higher fault tolerance), higher performance, or both.

RAID technology is divided into multiple RAID Levels, representing different data distribution strategies among the array of available hard disks on the RAID machine, as well as the minimum amount of physical hard disk required to implement each level. These levels are represented by numbers, and the most common RAID setups include the RAID 0, RAID 1 and RAID 5. RAID 0 represents a setup made for performance, higher overall disk space and no redundancy or fault tolerance. RAID 1 offers high tolerance at the expense of lower overall performance and lower overall disk space. RAID 5 offers both, a higher performance and fault tolerance, but requires at least one more hard disk to work (3 hard disks, instead of only 2 required on RAID 0 and 1).

Some other, less common RAID Levels, include RAID 2,3,4,6,10,50 and 0+1, mainly representing different variations of the basic three (RAID 0,1,5).

Usage

RAID solutions are very common these days, and are used by most enterprise level storage systems. The use of RAID in storage devices and servers, adds the ability to swap faulty hard disks, without the need for down time, and in most cases (except RAID 0) overcome disaster and data loss in case of a faulty disk.

RAID solutions are also common in home environment use, especially when small storage devices are used to store important data on multiple hard disks (such as important document or photos, etc.).

Available solutions on the market

RAID technology is available in almost every server and storage machine available in the enterprise market today and can be implemented by configuring the desired RAID level on each machine.

5.1.2 Application

5.1.2.1 Authentication, Authorization, Accounting (AAA)

Description

Authentication, Authorization and Accounting (AAA), refers to a commonly used framework, which allows control over access to digital resources and allows policies enforcement and Usage auditing. These three components are considered an important combination to effectively and securely manage network assets.

- Authentication – is the first process inline, allowing user identification, usually by having the user enter valid credentials (such as username and password) before being granted access to the network. The

authentication process is usually based on an identifier, unique to each user. If the user credentials match the ones stored in the system, the user is granted access. Otherwise the user access will be denied.

- Authorization – refers to the authenticated user rights to perform certain tasks or issue commands inside the interface. In essence, authorization is the process of enforcing policies and determining what types of access rights the user has in the system/network.
- Accounting – is the final part of the AAA framework, referring to the auditing and logging options available to monitor user activity inside the system. These auditing and logging options, may include usage statistics, overall load on the system, access to sensitive information, login hours, etc.

These three main services are often provided by a dedicated AAA server, via a program that performs these functions.

Usage

The AAA framework is implemented by the all known RADIUS (Remote Authentication Dial-In User Service) network protocol, and also by its newer counterpart the Diameter protocol.

Similar technique is implemented in almost every application and service today that requires identity-based access to all sorts of information or services.

5.1.2.2 Code review

Description

Code review refers to the process of a systematic examination of computer programing source code. The main purpose of code review is to find overlooked mistakes in code that occurred during the initial development phase.

A well performed code review, can have a significant value in making the software more robust, more secure and better performing in general.

Code review can often help find and remove common vulnerabilities such as memory leaks, buffer overflow and more, thus improving software security.

Code review practices can be roughly divided into two categories: formal code review and lightweight code review.

Usage

Code review is an integral part of a SDLC (Secure Development Life Cycle) incorporated in almost every development team today.

It is crucial in developing secure software products that will protect users and service providers alike, and will prevent potential damage or information leakage to malicious users that can exploit potential vulnerabilities in the code.

Available solutions on the market

Many security companies offer various services – such as secure code review, allowing the development team to outsource the intensive work of code review to security experts, while concentrating on code development for the software.

There are also various automatic tools offered by companies like “Checkmarx” – allowing automated process of code review and quick detection of common code security issues. These tools still require a human being inspecting the results due to possible false positives and false negatives generated by the tool.

5.1.2.3 Application vulnerability scanning

Description

As in code review bullet, mentioned earlier, Application vulnerability scanning refers to automatic scanning tools that help find code weakness, and security vulnerabilities, in applications – mainly referring to web-applications.

These tools usually address the well-known security issues, such as cross-site scripting, SQL injection, command execution, directory traversal and insecure server configuration.

Although effective, these tools are still used in conjunction with more traditional human code review practices, mainly to fill the gaps of less obvious vulnerabilities and reduce false positives from the tools.

Usage

Application vulnerability scanners are widely used by many development companies. They can greatly reduce the code reviewing process time, and reduce the time needed for human review – thus reducing cost and effort. These tools are used by companies from all sizes, and even by security companies offering code review services, as a helping tool to find additional issues in code.

Available solutions on the market

There are many solutions on the market, offering vulnerability scanning tools. Part of these tools are open source and free to download by anyone, and some are commercial tools, usually offered to organizations, that include support for their tool, and sometimes higher abilities for code review and app vulnerability scanning. Some of the available tools include:

- Acunetix WVS
- IBM AppScan
- HP – Fortify
- Trustwave App Scanner

5.1.2.4 Patch management

Description

Patch management systems are controlling all the patching process of updates for popular third-party software.

In addition to tighten security, these patches provides new features and improves software performance.

The system acquire, test, and install updates from relevant vendors to specific software suites. It acquires available updates as they're released, test their compatibility, automatically install and check that it was properly done.

Note that some updates requires OS restart, commonly scheduled in advanced.

Usage

Patch management systems are constantly running in background, but can be set to install updates only at predefined times.

It is intended to use in large scale organizations.

The system could overcome the demanding task of individually update numerous software types on every endpoint.

Available solutions on the market

Some systems are vendor-centric, others are cross-vendor solutions, and they can run in agent-based or agent-less mode. Among solutions:

- SolarWinds - Software Patch Management
- GFI – LanGuard
- IBM Tivoli Provisioning Manager

5.1.2.5 Input validation

Description

Input validation refers to secure coding methods, implemented in application development. The various methods verify that the input from the end-user (or the service communicating with the application) is not malformed and can't damage the program or make it operate in an unexpected way (for example make it crash, or expose sensitive information to unauthorized user).

User input in a program can never be trusted by the developer and all input should always be checked for correctness, meaningfulness and implement security checks to prevent possible attacks on the program/application.

Some examples of validation techniques include: Data type validation (integers, strings etc.), range and constraint validation, code and cross-reference validation and structured validation. Each technique can be implemented depending on the security requirements of the system.

Usage

Input validation is used in all kinds of applications and programs, regardless of their usage profile. It is also considered best practice and an inherent part of every secure development cycle.

Available solutions on the market

Input validation checking is done on the programing language level and can include:

- Data type validation.
- Range and constraint validation.
- Code and Cross-reference validation.
- Structured validation.

5.1.3 Host

5.1.3.1 Endpoint security

Description

Endpoint Protection is known as the last line of defense for workstations, laptops and smartphones who are connected to organization networks. Various systems and software suites provides a wide range of solutions to address most common challenges. They can be separated to deal with a specific threat or unified as a platform against several ones.

The structure of the solution can be set as client-server model or software as a service (SaaS) model to enforce policies and run security modules. Anti-Malware, Host Intrusion Prevention System (HIPS), Data Loss Prevention (DLP), HDD encryption, Mobile Device Management (MDM), etc. are all examples for Endpoint Security solutions.

Usage

Endpoint security has to be integrated by default in all devices regardless their usage or the user position. This is widely recommended as best practice.

This array of solutions almost decline unintentional security breaches and decrease lateral movement possibilities.

Available solutions on the market

- McAfee Endpoint Protection
- Trend Micro Endpoint Protection
- Symantec endpoint solutions.

5.1.3.2 Operation Systems (OS) patch management

Description

OS patch management systems are controlling all the patching process of security and system updates.

In addition to tighten security, these patches provides new OS features and improves performance.

The system acquire, test, and install updates on correspondent servers or endpoints operating system. It acquires available updates as they're released, test their compatibility on preset replicas, automatically install and check that it was properly done.

Note that some updates requires OS restart, commonly scheduled in advanced.

Usage

OS patch management systems are constantly running in background, but can be set to install updates only at predefined times.

It is intended to use in large scale server farms, datacenters and organization with numerous endpoints.

The system could overcome the demanding task of individually update every operation system.

Available solutions on the market

Some systems are platform-centric other are cross-platform solutions, most of them can run in agent-based or agent-less mode. Among solutions:

- GFI – LanGuard
- IBM Tivoli Provisioning Manager
- WSUS server (Microsoft environments only)
- Microsoft SCCM solutions (Microsoft environments only).

5.1.3.3 OS vulnerability scanning

Description

OS vulnerability scanning systems are assessing security weaknesses.

Unlike Antiviruses, OS vulnerability scanning are matching publicly published vulnerabilities to the operating system patches and current security-level. Commonly part of OS Patch Management or OS Vulnerability Management solutions.

The system checks specific attack vector preconditions and run tests on potential vulnerability for exploitation.

Usage

OS vulnerability scanning systems are typically used before and after OS patching cycle as verification and validation of the process, by user demand or at pre-defined times.

It is intended to use in large scale server farms, datacenters and organization with numerous endpoints, saving precious time in Vulnerability and Risk management objectives.

Available solutions on the market

Some systems are network-based scanners, available as appliance and others are host-based client or software. Among solutions:

- Tenable - Nessus Professional
- GFI – LanGuard
- Rapid 7 Nexpose

5.1.3.4 Clustering

Description

Computer clustering refers to various methods of duplicating existing infrastructure – such as critical servers (holding various services and applications), and configuring the duplicate servers (in a cluster) to take over the roles of the original servers in case of down-time or excessive load on the original server (the latter may also be considered as load-balancing). Clustering can also be used to increase performance, by using numerous separate computers to perform the same task simultaneously.

The cluster usually consists of two (or more) “nodes” – representing the physical (or virtual) machines running duplicate instances of the same operating system and applications required by the cluster.

In most cases, the nodes will use the exact same hardware and operating system on each node, and will be connected to each other through fast LAN connection, which allows full and constant replication between them.

Most clusters will use a single shared storage used by all nodes. This configuration allows each node to interpret the shared storage as its local drive, even though it is shared between all separate nodes.

Usage

Clustering technology has a wide range of applicability and deployment, varying from small business clusters to anything like super-computers.

Clustering is widely used to reduce down-time to minimum, and also allow continuous system maintenance while still providing service to the end-users.

Available solutions on the market

Clustering is an integral part of the Microsoft Windows server operating system and is available in other operating systems as well.

5.1.4 Internal network

5.1.4.1 Segmentation

Description

Network segmentation is to divide a physical network to multiple logical sub networks called VLANs. VLANs configuration can be achieved with layer 2 (in the OSI model) devices like switches. Basically, VLANs are

separated from one each other and communication are not allowed between them unless a routing device is allowing route between VLANs.

VLANs routing can be achieved with layer 3 (in the OSI model) devices such as routers or firewalls. The major advantage of the routing capabilities, beyond the ability to connect between different VLANs, is to apply set of rules (policy or access list) that will allow communication between two or more VLANs. Rules can allow specific IP accessing a specific resource on a specific port.

Usage

Segmentation is recommended to be used in almost every network. It is best practice to divide between assets and clients across the network. Configuring assets in dedicated VLANs and configuring all clients' computers in another VLANs. Communicating between these VLANs will be allowed through a Firewall device with a strict policy or a Router device with strict Access List. Access List or Policy will detail which device can access another and in which port or protocol it is allowed. The Firewall or Router will drop and ignore every other packet crossing the network that do not answer to policy or access list permissions.

Available solutions on the market

All major vendors providing VLAN capabilities in switching products such as Cisco, HP, Dell, Fortinet, Juniper and more.

5.1.4.2 Intrusion Prevention System (IPS)

Description

Attackers can activate manipulations on end-point operating systems, services, protocols and network communication. IPS can detect these manipulations and compare it to an attack-signatures database (which is updating continuously to new attacks signatures) and block the attack.

Another way IPS detects threats over the network is by examination of communications and search for anomalies such as port scanning (which is usually the first step performed before an attack can occur) or when a pre-defied policy or limit is approached, for example, the maximum number of sessions from one source IP, before consider that source as non-human (or malicious) behavior.

In case IPS detects an attack it will drop all the suspicious packets and prevent it from happening.

Usage

Most Firewall devices offer IPS capabilities inside it. IPS detects and prevents attack patterns to be transferred over the network. IPS can also be a dedicated appliance or as host-based application.

Available solutions on the market

- Dedicated Appliances:
  - Cisco FirePower
  - McAfee IPS
  - IBM Security Network IPS.
- Feature in firewall:
  - Fortinet
  - Checkpoint

5.1.4.3 Network Access Control (NAC)

Description

NAC describes a solution meant to identify endpoint devices and computers before they access the network.

Connecting to a network in the traditional way (using network cable) or using wireless, eventually leads to the company core network switch, so just the connection itself potentially grants some level of access to network or data. VLAN segmentation can limit the level of access available from a specific port but VLAN cannot decide to whom it serves data to.

Usage

To answer this security issue, NAC is in use. Every network card has a unique address called MAC. While connected a device to a port in the switch it can learn its MAC address and remember it. MAC solutions can basically remember MAC address and allow or block access to them base of pre-set policy. Some solutions can set the VLAN of specific port based of the MAC address connected to it. Another ways of identification can be in form of checking the endpoint operating system version, a specific registry value present, certificate, anti-virus software installed (and updated) or other pre-defined baseline value.

Unknown endpoints can be leaded to dedicate VLAN that has no valuable resource in it until administrator will manually set the correct VLAN to it.

Available solutions on the market

- ForeScout
- Portnox
- Cisco.

5.1.4.4 Load balancers

Description

Load balancers specialized in distributing workloads over multiple servers based on pre-defined policy. These allow to deliver high availability services and scalability capabilities.

There are multiple forms of load balancing: DNS-based, availability-based, network-based, etc. load balancers can be physical appliance, virtual machines or cloud-based services.

Some load balancer can provide multiple features such as SSL offloading – decrypt encryption before reaching destination servers.

Usage

Load balancers comes in various sizes and shapes. It can be implemented over a wide several of products and solutions. Main usage of load balancers is in front of web or application servers. Multiple web/application servers, delivering the same content, will be presented by a load balancer IP address. Every request for a web page will arrive to the load balancer which will route the traffic to the right server based on the policy pre-defined by the load balancer administrator. If HTTPS (SSL Encryption) protocol is applied, the load balancer can decrypted the information for the web/application servers and reduce their workload.

Available solutions on the market

F5, Incapsula, Citrix, Radware.

5.1.4.5 Network device redundancy

Description

Network devices are delivering services from the suppliers (servers) to their clients (end-computers). Failure in providing services due to technical issues or malicious activity would cause a reduction in productivity.

Network availability is crucial in critical infrastructure since no unavailability can be taken into consideration. This can be achieve by redundant all network devices to allow business continuity in case of a device failure.

There are 2 main redundant configurations: active-active and active-passive. Active-active describe at least 2 network devices that back up each other while they are both active and able to receive and process data. This configuration is not fully supported in all network devices. Active-passive describe at least 2 network devices that back up each other while only one of them is able to receive and process data while the other one is in standby mode. When the active device fails, the standby device becomes active and operational.

Usage

To provide network redundancy, two devices of each certain product are required. Firewall, for example, can be redundant by installing two firewall units, set them as a cluster (to consider them as one logical unit) and connect them correctly to the network. While one of the firewall devices are unavailable for any reason, the other one will come into action.

Other devices, like switches, can be setup in stack configuration. This configuration requires connecting the switches with special stuck cables which redundant both switches for power issues and hardware failure issues. In switch stack configuration both switches considered and one, they are both active-active (active-passive mode not supported) and the second switch is seen as an extension of the first one.

5.1.5 Perimeter

5.1.5.1 Firewalls

Description

Firewalls are the fundamental protection in every network. Logically, all communications flows through it, routed and examined by it.

By design, most firewalls are blocking all traffic unless specific policy set by the firewall administrator allows it. Such policy usually includes the source IP, destination IP and service or the port in use.

Because all communications flows through it, firewall can offer and deliver additional security mechanisms such as anti-virus, anti-malware, anti-bot, anti-spam, IPS, web filtering, application control, load balancing, VPN, etc.

Firewall can be deployed as physical appliance, virtual machine, cloud service or software.

Usage

To provide a defense layer over the network, firewall is deployed. Firewall allows conditioned routing between VLANs or separated physical networks while applying control, security and audit for the passing traffic.

Available solutions on the market

- Fortinet
- Checkpoint
- Juniper
- Sophos

- Cisco
- Palo-Alto

5.1.5.2 Web Application Firewall (WAF)

Description

WAF examines layer 7 communication in HTTP and HTTPS protocols. They can read and understand the protocol and how it is used to communicate with the web server. By doing this they can prevent application attacks from taking place. Application attacks can be SQL injection, cross site scripting, CSRF and so on.

WAF checks for various vectors such as HTTP/S request headers (to determine the nature of the communication and it's propose), application attack signatures, abnormal behavior of the client, source IP reputation, etc.

Usage

WAF protect web server from application attacks. WAF is set in front of the web server and examines all incoming traffic. When malicious traffic is detected WAF drops it.

Available solutions on the market

- Imperva
- F5
- Incapsula (cloud)
- Rebase (Cloud)

5.1.5.3 Content filtering (DLP, Email filtering, URL filtering)

Description

Content filtering is a term that describes various technologies exists to block and prevent access to a certain resource. These blocking abilities can be achieved by a deep inspection of passing traffic. A resource can be a website, email address, etc.

The most commonly use of content filtering is a URL filtering feature. URL filtering blocks access to a certain website which was pre-defined by the URL filtering administrator. Blocking policy can apply automatically over a group of websites answers to a certain category.

Another content filtering mechanism is email filtering which inspects all mail traffic and can apply block or allow policy base on various variables as email headers, email body content, attached file types, source domain and IP reputation, etc.

Another common content filtering mechanism is Data Loss Prevention (DLP) which is able to detect key words or file types that has some kind of valuable data to the organization such as personal identity information or datasheets contains sensitive financials data. On detection, it prevents the spreading of that file\data to be leaked outside the organization. DLP describes also set of solutions that logically prevent connecting personal devices to corporate computing systems such as USB, mobile devices, etc.

Content filtering can be a physical appliance, virtual machine, local software or a feature in a firewall.

Usage

With URL Filtering, an administrator can limit access to known malicious websites using the content filtering feature and preventing user's accidently surfing into malicious websites and download malicious content. Email filtering does the same in email communications. It prevents malicious content from being sent through emails.

DLP installed on network's gateway can detect if personal data (social ID number or credit cards numbers), or business-critical data (Excel datasheets, for example), are sent outside the corporate's network and blocks it from being leaked.

Available solutions on the market

- Zscaler
- Blue Coat
- Websense
- Fortinet
- Checkpoint
- Symantec
- Digital Guardian
- ForcePoint.

5.1.5.4 Data on transit encryption

Description

One of the security basics is keeping data integrity and confidentiality at all times. In many cases sensitive data must be transferred over unsecure networks (internet, 3rd party networks, etc.) and must be secured. This can be achieved by encrypting the data transferred over the network using common encryption protocols such as TLS, IPSEC, and VPN or in some cases by using built-in security mechanisms of protocols when available.

Usage

Encryption can be implemented in many ways. Traffic can be encrypted inside and outside the organization. Encryption of data can be achieved locally at the local operating system or by specific dedicated gateway.

An outside organization encryption example is VPN. It encrypts all traffic from client to server (usually a firewall) ensuring all passing data will be encrypted, even over public network like the internet.

An inside organization encryption is IPsec or TLS. They ensure all traffic is encrypted end-to-end and cannot be read by any unauthorized attacker in the middle.

5.1.5.5 Network Address Translation (NAT)

Description

NAT is a functionality that translates private IPs to public IPs. NAT can also translate IPv6 address to IPv4 address. NAT functionality usually is part of a firewall functionality since all traffic goes through it.

Usage

NAT help to protect networks by hiding private IPs from being exposed to the outside world. Without NAT, every communication will carry the real IP address of the device it was sent from as the source IP. This will allow attackers to know the inside devices IPs and try to communicate them directly. Knowledge of inside IP addresses can also imply of network size and configuration and may help attackers to achieve their goals.

Available solutions on the market

- Feature in firewalls: Fortinet, Checkpoint.
- Feature in Layer 3 Switches: Cisco, HP, Dell, Fortinet, Juniper etc.

5.1.5.6 Denial of Service (DoS) / Distributed Denial of Service (DDoS) prevention

Description

DoS stand for Denial of Service which is a kind of attack that will cause a server to be unavailable by taking advantage of a legitimacy service provided it over and over again until it exhausted or fail. A web server for example is sending web pages stored on it to whomever requests it. DoS attack will request these webpages in a large scale simultaneously until the server reached its limit of concurrent requests and fails to answer new requests.

DDoS, stands for Distributed Denial of Service, and it is the same kind of attack but from multiple sources like botnet network which can contain thousands of devices communicating with the web server.

Usage

DoS\DDoS prevention solutions can protect servers and services from such attacks by examine all traffic to and from the protected resource. Every traffic that considered as part of an attack will be dropped and won't be transferred to the protected resources. DoS\DDoS mitigation solutions can observes large scale attacks depending on its configuration.

There are basically two forms of DoS\DDoS mitigation solutions: on premise and cloud-based. On premise solutions will be physical appliance logically installed in front of the firewall (to protect it). These form of solution has one major disadvantage – it cannot defend against DoS/DDoS volumetric attacks which is a kind of attack that consume bandwidth so no new legitimate traffic can pass and answered. Another form of DoS\DDoS solution is cloud-based. In this solution the traffic is distributed through data centers across multiple geographical locations (CDN network) so an attack will be dropped way before it reaches its destination.

Available solutions on the market

- Imperva Incapsula
- F5
- Arbor
- Akamai
- CloudFlare
- DOS arrest

5.1.5.7 Advanced Threat Protection (ATP)

Description

The vast major of information security products are based on detection of known threats that were already discovered and learned with no different if the threat is a network pattern representing an attack, a virus \ malware \ ransomware file or a malicious website. The security mechanisms create a unique signature of the threat and that signature is used to identify the threat in the future. Attackers can almost easily evade detection just by slightly change the attack pattern (for example, such a change can be a single character added or subtract from the attack program code) and that changes the signature completely so the security mechanisms no longer recognize the new signatures until those are discovered and learned.

Information security product vendors was required to find a set of solutions that are not signature based and can adopt themselves to the current threats and detect new threats never seen before (“zero-day attacks”). In this line of solutions we can.

Usage

ATP Solutions are integrated in many products because of their ability to detect new threats never seen before. ATP is implemented in mail relay solutions to detect threats over email traffic to content filtering products which

examine passing traffic and searching for threats. ATP is also implemented in sandboxing solutions that examine files sent to it and detect threats suck as malicious code or behavior.

Available solutions on the market

- Fortinet FortiSandbox
- Checkpoint SandBlast
- Palo Alto WildFire

5.1.6 Physical

Physical security in all means can be used to limit physical access to critical and important assets, to prevent a theft, damage, unauthorized change, etc. Common ways to apply physical security are:

5.1.6.1 Fences\Walls:

Limiting physical access of unauthorized personal guarantee that only trusted and qualified staff is able to access areas contains critical infrastructures or sensitive data. Restricted areas should be surrounded by a fence. Entering or exiting restricted areas will be possible from controlled passage.

5.1.6.2 Cameras

Cameras can deliver live feed of restricted areas and provide visibility of security status to handlers in the control room. Security cameras should be able to operate in any environment they are deployed in, for example, an outdoor camera should operate at day or night light conditions. Some cameras can be shift, tilt and zoom by remote (PTZ). Cameras are often installed with recording system that saved all video feed for long-terms.

5.1.6.3 Guards

Despite all logical defenses and security automation, security guard will always be part of the defense layer. Human guards can make decisions and conclusions on ongoing events and react accordingly in a fast and accurate way.

5.1.6.4 Building control

Building control systems are software's that control and automats the building systems such as elevators functionality, air conditioning systems, water and electricity management etc.

5.1.6.5 Locks

Locks are preventing access to restricted area by forcing user to identify and preset key, badge or biometric input in order to allow access. Physical key can be a door key, swipe card, RFID badge, biometric keys are iris or fingerprint signature. Presenting authentication parameter is used for promising that access will be granted only to those who have clearance for it.

5.1.7 Policies, Procedures and Awareness

5.1.7.1 Data classification

Description

Data classification refers to the process of organizing and categorizing data according to various properties, such as its sensitivity, the department it relates to, etc.

The main categories should refer to: Data types, data locations, data access levels and data protection levels implemented, with reference to compliance regulations.

A well performed data classification can outline the most important parts of data across the entire organization and allow an effective process of managing this data and controlling all access to it.

The data classification process is an intensive mapping process that requires full cooperation between the data owners (for example: department managers) and the corresponding IT and security teams in the company.

After classifying all sensitive and important data in the organization, the IT and Security departments can implement various security and management measures, allowing to limit the access to sensitive data to allowed personnel only, and apply additional protection layers such as backups and redundancy to information marked as critical to the organization.

Usage

Almost every organization deals with some sort of data classification. Some organizations are subject to various regulations, requiring them to manage their data in a certain way, other organizations manage their data just to maintain order, thus allowing them to focus their protection upon the most sensitive data.

5.1.7.2 Password strength

Description

Almost every service accessed today, requires authentication using a combination of (at least) a username and password. A successful attempt to guess a password of a certain user, can easily grant access to the system to an unauthorized user.

Password strength refers to the effectiveness of a password in resisting guessing and brute-force/dictionary attacks. The strength is usually measured by the password's length, complexity and unpredictability. By integrating all previously mentioned aspects of the password, it is possible to estimate how many trials an attacker would need, on average, to guess the password correctly.

Brute-force and dictionary attacks can be implemented, to generate a large number of access attempts, using thousands of password variations per second. The longer and stronger the password, the harder it would be to get it using these automatic methods.

But password strength is not only about its length and complexity. Additional security measures must be implemented to properly protect the login stage. These security measures may include various techniques, such as a limit on the number of wrong password attempts in a certain period of time, a time-out between each attempt to login, and even an entire user block after a certain number of times.

Another important aspect of password strength is the password creation process. Passwords are created either automatically (using randomizing algorithms and special programs) or more commonly by a person. Unlike the random algorithms, humans select their passwords based on various patterns which may help them remember the password more easily. These patterns, if known to the attacker, can help greatly at discovering the password (for example: a pet name, a birthday date, the user's name, etc.).

Usage

Many organizational IT and Security departments implement various password policies. These policies are usually configured to bind the password creation and management to various rules. For example: limit the minimum password length, define what characters must be used in each password, define rules about password repetition, limit the password lifetime, etc.

5.1.7.3 User education – security awareness

Description

User education refers to the formal process of educating and raising the awareness level of employees towards computer security.

There is almost no organization today that doesn't use computers and information technologies of some sort. This means, all users in all organizations are subject to various Cyber threats that they need to be aware of.

The vast majority of most companies' employees are not tech-oriented and most of them don't know the potential risks of using the web or corporate network and end-point computers.

This low level of security awareness is usually easily exploited by hackers to infiltrate the company's systems, gain access to sensitive data or even cause damage to the company. The infiltration is executed using various techniques, such as Social Engineering, Phishing Email, Malicious programs and attachments, etc.

Most of the attacks can be spotted or prevented altogether by a security-aware user, who will not open suspicious links, or download attachments from an unfamiliar person. Well educated and security aware users will also report potential risks to the relevant person in the organization, in case they suspect they were attacked.

A well implemented user awareness and education program is usually implemented on all levels of the organization, making it a second nature to all employees. This effort to improve employee security awareness usually originates from the management and from the IT and information security teams, responsible to the company's security.

Usage

Security awareness programs are implemented in various ways in many organizations today, regardless of their main business. Companies dealing with highly sensitive information are more likely to implement broad security awareness programs to their employees, thus reducing risk or potential security risks originating from human error.

Available solutions on the market

Many security consulting companies offer various education and awareness packs and dedicated courses. These packs may include various materials, such as posters, slogans, games, and articles regarding security awareness.

5.1.8 Governance, Risk management and Compliance

5.1.8.1 Logging and auditing

Almost every device is able to produce logs. A log contains various information types - from events detected by the device sensors to configuration changes and hardware status notifications and so on. Some devices logs every single action performed by the system and some of it logs only important events. Either way, logs are not to be ignored from.

Logs are highly important since they can point for events that need administrator's attention. Such events can be hardware failure, security breach, data leak, malicious activity, etc.

In typical organization there could be hundreds or even thousands of machines that produce logs simultaneously. It is not a reasonable task for human operator to read and search throughout log records and seek for meaningful events at real time. In order to do so, automation is required. SIEM Solutions provides such automation.

By setting every device to send all produced logs to a central location (usually by using Syslog or SNMP protocols), SIEM solutions can filter unimportant logs record and provide visibility of meaningful events in readable dashboard console. SIEM solution can provide added value by searching for pre-defined correlation between different events that can point on an on-going attack.

5.1.8.2 Security incident management and response

In an ongoing security event, it is important to manage and orchestrate all involved factors in order to quickly eliminate the threat, minimize impact, gain full recovery and continue all routine operations. To be able to achieve this it is crucial to dedicate personals to be an expert in managing such events.

A dedicated security respond team can be activated in a case of an ongoing event. They will operate to isolate the breach point and prevent further use of the current breach hole. In the physical security world it can be a hole in the fence or biometric lock that no longer functions and allow free passage. In a logical security world a breach hole can be vulnerability exposure, a device that allow uncontrolled access to a network or firewall policy and allows extend permissions. Either way it has to be blocked or removed to reduce the possible damage. After the breach point was contained it is important to investigate what infrastructure devices influenced from that breach. This can be done by view monitoring information displayed in SOC systems or SIEM systems.

5.1.8.3 Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

BCP, or Business continuity plan, referring to all actions need to be taken in order to allow all business operations during and after a disaster. Disaster can be nature hazards such as fire or flood but it can also be data theft, data corruption or data deletion. DRP, or Disaster Recovery Plan, is a detailed technical plan describing all methods and actions that will allow specific business operation to function after disaster occurred. In data theft, corruption or lost example, it is DRP best practice to manage consist data backup operation that will allow data restore in case of need.

One way of doing it is by maintaining a backup site (DR Site) which contains a live replication of all critical systems so in time of disaster, the business process would not be interrupted.

5.2 Focused solutions for Medical and Healthcare domain

As per today, the medical and healthcare domain includes exclusively standard security solutions.

Due to (1) the strong regulatory procedures related to the possession, use and transfer of patient data/images, (2) the fact that most of the technologies are incompatible and/or proprietary in terms of formats and (3) the difficulty to interlink medical and non-medical IT and OT devices, the healthcare systems do not use to be connected through big extensive networks but using smaller dedicated independent VLANs with highly strict access protocols. Only in some particular cases those VLAN are transparent (intercommunicated) to others, particularly among devices capable to process/transmit data over predefined protocols as CDA, ISO CEN 13606 or HL7 (the most widely spread and standardized).

Besides, some OT devices have been designed to work by default in a stand-alone condition without taking into account some basic protection requirements once networked, as per example the safe transmission of the clinical data obtained. Even most of them run actual and updated operative systems, the manufacturer do not include any endpoint protection (antivirus) neither accept the inclusion of it by a third company because they cannot guarantee the proper functionality of the whole system once installed.

Among the standard solutions, hospitals usually count on:

- Perimeter solutions: Hardware firewalls hosted in the Central Data Center dedicated to protect all the independent VLANs and the VPN external connections

- Endpoint protections: Apart from establishing individual user identification procedures, the IT departments always typify some mandatory institutional rules. In the HCB case, install the OS Windows 7 Enterprise plus a commercial antivirus (Symantec Endpoint Protection) in all the workstations and laptops connected to the organization network avoiding the connection of any OS Android due to the difficulty to limit the direct internet access by the applications in such type of devices
- Physical solutions: The communication racks, all locked with keys, are located in closed technical rooms scattered around the different buildings that configure the hospital facilities. These service areas are also protected by cameras and biometric readers deployed at their main entrances.

5.3 Focused solutions for Environmental Monitoring domain

As far as we know, the environmental monitoring domain uses standard solutions to achieve the necessary security level. A typical environment monitoring network consists of:

- Monitoring stations or simple data loggers, placed outside the corporate network.
- One or more data collection servers, eventually placed inside the corporate network.
- Data management, elaboration and distribution applications hosted on servers inside the corporate network.

Generally, all the servers used for the environmental monitoring network, located inside the corporate networks, are protected in the same way as the other corporate servers, for example using the security system according to ISO 27001.

On the other side, the systems outside the corporate network are protected in many different ways, according to the kind of hardware used. Industrial PCs or servers are protected with hardware or software firewalls when they are exposed on the Internet and standard secure protocols are used for data transmissions (SSL, VPN, etc.). In case of ISDN networks, security is usually demanded to ISDN routers with caller id identification and filtering, CHAP protocol; in addition, the same security protocols and firewall used for Internet connection may be used.

For simple data loggers with proprietary byte based protocols, is not unusual having no additional security protocols or hardware, as the data loggers have only the capability to transmit the measured data so it is not possible to change their configuration or normal behavior through the network connection.

5.4 Focused solutions for Transportation domain

A typical control system in the railway domain consists of several subsystems:

- Safety-related components like interlocking, points, switches and axle counters
- Assisting systems like train number systems and automated driveway systems
- Data management systems as the MDM, the documentation system
- Diagnosis systems

Currently these systems are grouped in security zones, which then are secured according to their criticality. The security analysis is based on ISO 62443 and the resulting measures are derived from ISO 62443-3-3 and are enhanced by more advanced measures defined by DB Netz. Communication between these zones is done via standard IP networks. Depending on the levels of the connected zones the communication paths are either secured by security gateways, which establish an encrypted communication path, or a firewall gateway, which filters the communication via whitelisting.

Besides this all components are logging their system states and transmit these logs to the MDM for analysis. The results of this analysis are then transferred to the DB Netz security operations center, where analysts can investigate on possible attacks and initiate countermeasures if needed. Currently plans are developed to include IDS systems in each interlocking network to enhance the detection capabilities.

Furthermore the results of system analyses are later on used as input for the information security management system which is based on ISO 27001. The ISMS also can introduce new controls to the control systems if the threat landscape changes.

5.5 Focused solutions for Financial Services domain

Soltra™[ix], an FS-ISAC and DTCC joint venture created to help secure critical infrastructure entities from cyber threats, has created Soltra Edge™, a software solution designed to facilitate the collection of cyber threat intelligence from various sources, convert it into an industry standard language and provide information on which users can decide to take action to better protect their company.

FS-ISAC and DTCC and their Soltra Edge solution head to help financial institutions to get actionable information faster, streamline workloads and leverage a community defense model to protect against all types attacks, threats and vulnerabilities.

A basic license is available at no cost. Soltra will also offer two premium versions with additional features that support scalability and redundancy. Soltra will offer fee-based maintenance and support for the platform as well as professional services to assist with deployment, configuration and integration.

Main features	SOLTRA
Standards	Soltra Edge leverages open standards, including Structured Threat Information eXpression (STIX™), a uniform format for the threat information, and Trusted Automated eXchange of Indicator Information (TAXII™), an open standards protocol for routing that threat information. Soltra Edge includes capabilities to import structured and unstructured threat information, standardize and organize that threat information using STIX formats, and instantly route that uniform threat intelligence via the TAXII standard to devices and analysts in order to take immediate action to prevent cyber incidents.
Automates Sharing & Trust Circles	■ Peer to peer sharing using existing trust relationships. ■ On premise, full controls for determining what is shared, what is not. Utilizes Traffic Light Protocol (TLP). ■ Supports Community Defense models: Inter-sector sharing (e.g. FS-ISAC) and cross-sector sharing (e.g. with other critical entities) (e.g. ISACs-Information Sharing & Analysis Centers and ISAOs-Information Sharing & Analysis Organizations).

6 Market Products Evaluation

When evaluating products on the market, the following considerations must be taken into account:

6.1 Robustness

- The ability of tolerating perturbations that might affect the system's functional body.
- The ability of a system to resist change without adapting its initial stable configuration.
- The persistence of a system's characteristics after perturbation (includes mutational robustness and environmental robustness).

6.2 Availability

- The probability that a system will work as required when required during the period of a mission.
- The support of the product in high availability capabilities such as clustering.
- The stability of the system – regarding the ability of the system to work for long periods of time without problems or possible "bugs".

6.3 Reliability

- The probability that a device will perform its required function when needed.
- The consistency of the product when used under constant conditions.

6.4 Usability

- The ease of use and learnability of the product by its users.
- The efficiency and satisfaction with which users can achieve tasks in a product.

6.5 Effectiveness

- The capability of the product to produce the desired result.
- The ability of the product to "do the right thing".

6.6 Privacy

- The ability of the product to provide its users with the right to have some control over how their personal information is collected and used.

6.7 Cost

- The price of the hardware, software, implementation and maintaining of the product.
- The Cost Effectiveness of the product.

6.8 Timely Responsiveness

- The ability of the product to complete assigned tasks within a given time.
- The ability of the product to reply to users request in a timely manner.

7 Conclusions

In order to manage cybersecurity risks, a clear understanding is required of the organization's business drivers and security considerations specific to its use of information technology and industrial control systems. Because each organization's risks are unique, along with its use of information technology and industrial control systems, the tools and methods used will vary.

To obtain protection on a critical infrastructure there is a need to first perform a full risk assessment of each system to better understand the different logical processes. After a basic understanding of the contributing sub systems to the entire logical system and given that a complete understanding of the entire logical operation of a system and the interconnections of its subsystems there is a need to derive a complete set of classifications to determine the criticality of the system.

There is a need to understand, identify, and analyze the interdependencies amongst systems. This is the greatest challenge and the most significant one.

These infrastructures affect all aspects of daily use including oil and gas, water, electricity, telecommunications, transport, health, environment, government services, agriculture, finance and banking, aviation and other systems that at the basis of their services are essential to state security, the prosperity of the state, social welfare and more. So the big challenge is the dependence of these different systems and complexity factors interplay in protecting critical infrastructure.

8 References

[i] Financial Services Information Sharing and Analysis Center (FS-ISAC). https://www.fsisac.com/

[ii] Securities Industry and Financial Markets Association (SIFMA). http://www.sifma.org/

[iii] Guide to Cybersecurity for Financial Services Firms. Embracing an Intelligence Driven Defense. An eBook Presented by: Lockheed Martin Corporation.

[iv] Financial threats 2015. Candid Wueest. Version 1.0 – March 22, 2016

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/financial-threats-2015.pdf

[v] FFIEC (Federal Financial Institution Examination Council). IT Examination Handbook Infobase.

http://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems.aspx

[vi] Chartis. World-Class Risk Technology Research and Insight. Cyber Risk Management in Financial Services 2016.

http://www.chartis-research.com/research/reports/cyber-risk-management-in-financial-services-2016

[vii] Tripwire. Takeaways from the 2016 Verizon Data Breach Investigations Report. David Bisson. Apr 28, 2016

http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/takeaways-from-the-2016-verizon-data-breach-investigations-report/

[viii] Verizon. 2015 Verizon Data Breach investigation report.

http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

[ix] DTCC. Dec 03, 2014 • Press Releases. Soltra Edge™, the First Industry-Driven Threat Intelligence Sharing Platform Now Generally Available, Easy-to-Use and Free to License.