2023

Document N°SSI.0 – Contextual Analysis

Date	Rev	Reason for Revision:	Written By:	Approved By:
06/11/2023	0	First Release	Francesco Cinotti	Matteo Viggiani

Purpose

The purpose of this document is to:

1) Introduce the Techpol company and its development in recent years;
2) Explain the reasons that prompted it to carry out an 'information analysis' process and the objectives it intends to achieve;
3) Define the scope of the analysis.
4) state how the system is updated and checked periodically

Brief description of Techpol Srl

In 2018 Tech-Pol completed 40 years of business and has its commercial and production headquarters in MORRO D'ALBA (AN) in the P.I.P. industrial area in Loc. S. Amico.

It is located on a site of 9,566 square metres, of which 6,500 square metres are under cover.

The company successfully manufactures Injection Moulding of Plastic Products; it has achieved a leading position in this field in the AUTOMOTIVE sector.

TECH-POL S.r.l. produces Plastic Products for the following Merchandise Sectors:

1) Automotive
2) Lubrication pump components
3) Automotive electrical connectors
4) Fitness

The Company is structured to produce medium/large volume lots.
The know-how it currently possesses enables it to design, develop, initialise and manufacture products of a high technological, quality and reliability level. Following the consolidation of its production activities, over the last five years the focus has shifted to increasing the skills of its personnel in order to increase their level of awareness and preparation to be able to protect themselves from possible cyber attacks that could slow down or even bring the business to a halt.
The company is changing its production capacity in the automotive sector, adapting to the needs of the ever more imminent 'electric' market.

Objectives of the Information Management System:

Organisational objectives:

1) Increased operator awareness and education on cyber security issues

a. To this end, the CSO sends periodic attack reports and awareness-raising e-mails to all operators, indicating the threats and how they can be prevented

b. Operators have an e-mail address to which they can send all questions and doubts relating to security, such as e-mails that are considered dangerous, or requests made by telephone that are 'dubious'.

Technological Objectives:

1) Business Continuity
2) Information Confidentiality

Business Continuity

Tech-Pol works with major automotive groups and for them it must guarantee a level of service that is not only of the highest quality, but must also ensure business continuity in order to be able to respond to the constant demands of its customers. For this reason, since 2010 management has been especially concerned about data security and the remote possibility that its information systems could be shut down, thus incapacitating the company.

Over the years, investments have been made in order to avoid any 'slowdown or malfunctioning' of the entire system, but at the end of 2017, when the life cycle of the hardware had come to an end, it was decided to implement a Business Continuity system, in response to the VW Group's request to carry out an audit of its information management practices, using the TISAX assessment.

The two Datacentres have been completely upgraded with IBM equipment; the choice of supplier is the result of more than 10 years of experience with this brand in which we have assessed the extremely efficient nature of their support system; the latest versions of the IBM SANs purchased are equipped with a system called CALL HOME which, in the event of an alert or a failure of the hardware and/or the ancillary transmission systems, directly contacts a telephone number; the number that has been included in the configuration is that of the CSO, who evaluates the extent of the damage and the level of disruption to the system and has the private mobile phone numbers of the technical personnel who maintain the computer system.

A brief description of the distributed system between the two data centres follows:

A) The two datacentres are virtualised using VMWare at the LUN and operating system level; at the data level, the two NAS, located in the first and second datacentres respectively, are constantly connected and synchronised, using the dual-system clustering system named HyperSwap Manager; thanks to this architecture, if one of the two datacentres were to fail, the second one would completely cover Techpol's needs, both in terms of disk space and computing requirements;

B) Each data centre features a firewall clustered with the other so as to be completely fault-tolerant in the event of one of them going down;

C) Internal connectivity is provided by a meshed network between 9 switches located in the factory and offices;

D) 11 Vlans

E) segment the network into dedicated networks to host internal services; the server management Vlan is unreachable by the other Vlans, in order to keep the data contained in them as secure as possible;

F) The backup system follows a schedule based on the 3-2-1 concept by making three copies in total, two of which are saved in the other data centre and one saved on a NAS located in a dedicated rack outside the datacenters;

G) External connectivity is provided by a supplier that has deployed two WI-FI backbones, running off two separate repeaters; the routers are configured in fault tolerance mode, so as to avoid line drops. FTTH fibre was connected a few months ago, which allowed a fourth data backup of the ERP software in the datacenter.

Information Confidentiality

The company is extremely careful to enhance the level of confidentiality of information within its organisation, in order to prevent any leaks of information relevant both in terms of business and industrial secrecy, both its own and its customers'. To this end, it does not consider the confidentiality agreements, signed by all employees and contractors, to be sufficient, and demands a continuous technological update aimed at tightening authorisation systems and eliminating the use of USB storage devices, which are particularly risky in this context; to this end, the situation to date is as follows:

1) There is no local data on operators' PCs;
2) All data is stored on the file server; access to directories and files is related to the business function performed by the user; in the event of a change of role, access rights are changed only after authorisation by the head of department;
3) A special encrypted file server has been created for special customer, to which only the authorised personnel have access; a certificate has been installed on each of these persons' devices, enabling them to access the files without having to decrypt them each time;
4) Access to the company ERP is linked to user profiles; users are organised into homogeneous groups by function; system passwords are systematically changed (every 6 months) and have the necessary complexity requirements in place.

PAY ATTENTION – VERY IMPORTANT:

The information security policy provides that any new initiative affecting information security, even in a minor way, must be shared with the CSO; any change in terms of equipment, processes, operating methods must be shared with him.

Scope of Application:

The analysis was conducted exclusively in relation to information relating to the so-called PROTOTYPES and the relevant databases, following the flow of data through a series of checks and interviews with key personnel within the company. Following identification, the measures to be adopted are set out for the reduction or elimination, where possible, of the risk and the foundations are laid for a monitoring activity that aims to progressively improve the level of security, also through the preventive identification of possible new risks.

ISGI system is updated and checked periodically:

The system is periodically internally reviewed, at least once a year or in any case of need due to major changes. An external control assignment has been entrusted to a professional with proven experience and seniority, who is responsible for checking the state of compliance of the procedures and their actual implementation, through a scheduled annual visit and any other interventions to be planned