*Department of Business and Management*

*Course of Digital Transformation*

# The Digital Transformation of Supply Chains: opportunities and risks in the Italian Industry 4.0 landscape

SUPERVISOR

PROF. Paolo Spagnoletti

CANDIDATE

Angelica Craveli

MATR. 671811

CO-SUPERVISOR

PROF. Stefano Za

ACADEMIC YEAR 2016/2017

*Thanks to all those who have been close to me in these years, with their support, encouragement and love.*
*I would like to express my special thanks to my parents and family, who have made this important achievement possible.*

# Table of contents

## Abstract

This paper addresses the theme of Digital Transformation and how it influences industries' supply chains, and underlines the relevance of the Italian Industry 4.0 framework. It is composed by four chapters related to each other.

The first chapter describes the positive effects of Digital Transformation; enhancements and innovations such as Additive Manufacturing, Internet of Things, Cloud, Big Data, Machine Learning, Wearable, and Robotics that are becoming an integral part of many industries structures.

The digital revolution is bringing with it the need for development of new professional figures, such as CIO or CISO and is involving in a specific way companies' supply chains.

The supply chain is the fulcrum of the second chapter. Digital Transformation is improving and speeding up the different stages of the production process, including planning, procurement, and logistics. The machines used are increasingly innovative and interconnected, based on robotics and the use of sensors that allow different parts of the warehouse to converse with each other.

In chapter three, starting from brief references to the industrial revolutions that evolved over the years, I went through the analysis of the challenges and problems that Industry 4.0 brings with it. From negative effects, such as job losses to environmental issues, from cybersecurity to the need to retrain the current employees, passing through to the comprehension of how companies, schools, universities and Governments should intervene and invest to exploit the opportunities of Revolution 4.0 we arrive at the final chapter.

In the last part of this paper is considered as a controversial theme and growing risk for an interconnected world: Cybersecurity.

The number of hacker attacks, in recent years, has seen a widespread increase, including the WannaCry ransomware attack that struck in May this year. The European Community has already taken steps to increase computer security measures through the 2016/1148/EU directive of 6 July 2016, which urges the Union countries to standardize and increase security levels.

In the top ten of the countries that have suffered more attacks, we can find Italy.

The cyber threat is significant in our country and the creation of a "National Framework for Cybersecurity" was necessary to provide essential guidelines to all companies, that have the duty to apply them, in order to protect themselves and the entire Italian economic landscape.
It is mandatory for our country to take advantage of this deep revolution paying attention to the relative risks.

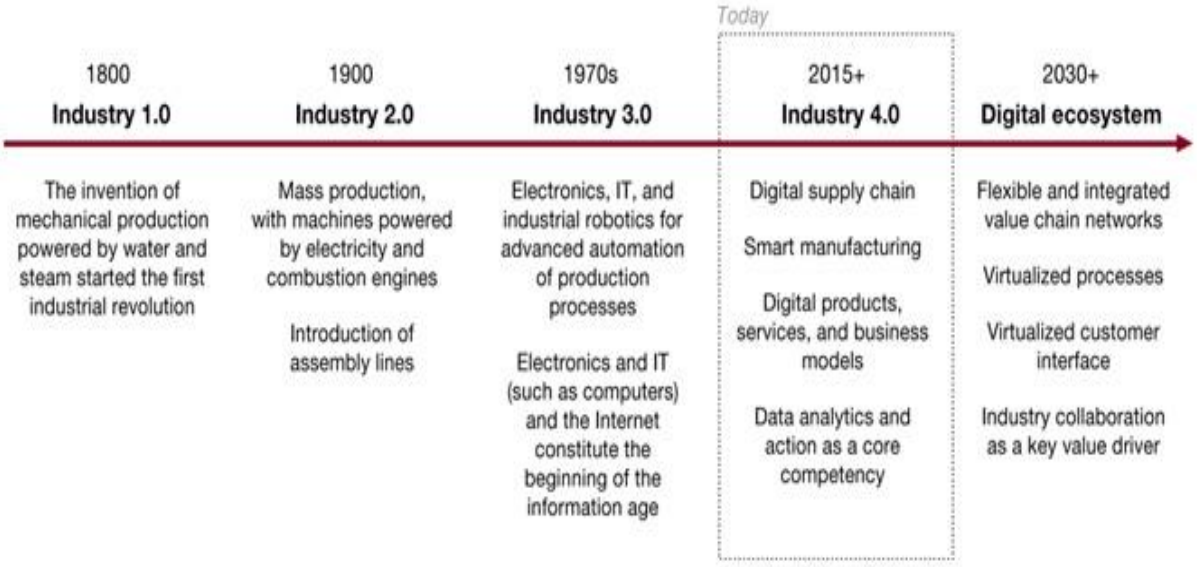
## 1: Industry 4.0 revolution

The ability of human invention has never been as stimulated and free as in this moment of fourth industrial revolution, where ideas find their materiality as a way of expression in near real time.

New digital technologies, that are finally available, often at low cost, allow us to design and manufacture almost everything we imagine, that we would have had and become functional to improve every area where we apply technology.

We entered the third digital revolution in the world of manufacturing.

Following the first two digital revolution in the world of telecommunications and computing, today we are taking part to the meeting between digital manufacturing (fabbing), new approaches to the design, production of goods and open source platforms, which take the form of new ways of creating assets that compose the environment around us.




[1]

[1] Figure 1- Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused, Stefan Schrauf, Philipp Berttram, September 7, 2016

This sparkling, revolutionized digital world, presents numerous unimaginable opportunities and challenges not only for the industrial design, but also for the Communication Design.
The evolutionary process of technological-manufacturing sector is leading the consumer towards a new awareness: the ability to be part of the change himself. This is steering industries towards a new production and distribution model, based on the modulation of goods and services, which meets the real needs of each customer through a flexible production structure, interconnected and highly localized.

The modern approach to manufacturing is undergoing a "democratic development" as now, through the media and the digital network, the intuition of a single individual can become something concrete, produced at very low cost.

In fact, the concept of Digital Manufacture (or Digital Fabrication, or fabbing), refers precisely to the process by which you can create solid and three-dimensional objects from digital designs that are usually available to any user.

The entire system is then expanded via sharing dynamics that allow the diffusion of ideas and continuous innovations. The word Openness is becoming the key to new and exciting sustainable developments. Digital manufacturing brings inside a huge and fascinating revolution, which is the ability to enable potentially anyone to the creation and innovation.

The machines used for digital manufacturing are easy to use and not expensive; these elements, together with the extreme usability of software for the design and modeling, are allowing the spread of fabbing also towards unprofessional consumers.

This phenomenon, called "Personal Fabrication", is also fueled by the emergence of community in which digital drawings, experiences and creation of digital artefacts are being shared and made available for free by users.

Another distinctive feature of the fabbing world is that of "rapid prototyping", which, thanks to the technological evolution of some ways of production, leads to the "additive manufacturing", used for example by the 3D printing (which we will return later).

In addition, "digital manufacture" means also the process that uses CAD data (Computer-Aided Design) or other types of data to drive an additive manufacturing machine that realizes assembled parts.

In addition to the CAD data, which represent the clear majority of the data used in these processes, for the control of these machines may also be employed other types of data, such as scan data and data DICOM (Digital Imaging and Communications in Medicine for the physical representation of medical images in 3D).

With "additive manufacturing", we refer to the name used to identify the processes that lead to the construction of an object through the superposition of layers (layer manufacturing). Opposite processing, respect to milling or laser machining based instead of "subtractive" processes. The finished products of a company are carried out not more shaping or removing material, but adding the material, layer by layer.

The elimination of transactions, usually required in conventional methods, as pre and postproduction lowers costs, time or labour now become superfluous in the manufacturing process. The additive manufacturing processes, however, work in different ways depending on the technological needs that arise for the realization of a project.

Whatever the chosen technology, digital manufacturing provides huge advantages over conventional methods. The most important relate to the acceleration of time-to-market design cycle, the investment elimination, productions with reduced volumes, the quickest and less expensive redesign and above all customised parts.

A further advantage is represented by the "green" character of many of additive manufacturing technologies, which produce less waste of working with respect to milling processes, does not involve the use of harmful chemicals, do not emit noxious fumes into the environment and the choice of used materials is very wide (plastic, metal, ceramic or sand).

There are no waste parts to store, because there is no reason to build more units than those that are required at a given time so there is a reduction of inventory costs and inventory.

The economic impact of this impressive "fourth industrial revolution" is not yet quantifiable, but the economic models that are emerging around digital fabrication are called "regenerative economic model". These models plan to reduce dependence on economic resources by creating, as a result, new markets, generating a "circular economy" system that increases the value of the entire industry ecosystem. Currently[2], the Italian Industry 4.0 is worth 1.2 billion

[2] Data from: Osservatorio Smart Manufacturing PoliMi: "L'Industry 4.0 italiana vale 1,2 miliardi di euro", 21 giugno 2016.

euro, but 38% of companies still say they do not know the theme of Smart Manufacturing and projects are often on a pilot basis with strong differences by sector.

SMEs are almost absent and 62% of digital skills assessment identifies gaps to be filled. In these years, Italy is developing a national program to guide industries towards the Fourth Industrial Revolution, which will certainly not ignore, a focus on operator training.

The framework of the Industry 4.0 in our country is basically positive: almost a third of companies have already started three or more projects based on innovative digital technologies such as the Industrial Internet of Things, the Cloud Manufacturing, Advanced Automation, the Industrial Analytics or Advanced Human Machine Interface.

The market value of smart Manufacturing in 2015 in Italy is around 1.2 billion euros, a significant value that represents just a bit less than 10% of the total industrial investments (10-12 billion euros).

Over 600 applications were surveyed, the +30% in a year, especially Industrial IoT technologies and related Industrial Analytics. For 2016 is forecasted a growth rate of 20%, unfortunately insufficient to recover years behind international technological development plans.

The 66% of the market is represented by projects of Industrial Internet of Things, it is worth 790 million, followed by Industrial Analytics (23%, 270 million) and Cloud Manufacturing (10%, 120 million euros).

If we look at the international scene, in addition to a broad growth across all technologies, in IT's area the most significant growth concerns applications of Industrial Internet of Things, +46%, which tows also projects of Industrial Analytics and Cloud. In the area of operational technologies, there has been a boom of the Advanced Automation with a + 169% thanks to strong interest in the "collaborative robots".

Very vital is the Additive Manufacturing, especially in certain niche markets like aeronautics, defense and in the medical field, while it is still being tested in other sectors.

A limit to the spread of Smart Manufacturing in Italy is the poor "digital maturity" in different industries: although 70% of has already adopted the standard solutions (such as CAD and production control systems), less than 30% are using more advanced management systems as Product Lifecycle Management, Computerized Maintenance Management System and Manufacturing Execution System.

The identified barriers are many: the environment, cost, lack of infrastructure and innovative facilities, cultural and organizational boundaries. Businesses are demanding to Government incentives for the modernisation of networks or for new IT systems (in 50% of cases), followed by incentives for new machinery for SMEs (46%) and for training to large companies (38%).

In fact, rarely companies shall carry out an analysis of digital skills (29% of large enterprises and small to medium 13%), and when performed important gaps emerge, requiring in this way some corrections in 62% of cases, whereas in 32% only a few figures have the skills and 6% businesses recognize themselves ready.

With regard to the number of start-ups funded worldwide, Smart Manufacturing grew by 15%, for the third year in a row (full data to 2014) and the total funding has risen to more than 1.5 billion dollars, of which 39% picked up by new enterprises in the area of Industrial Analytics. On a list of 173 identified start-ups, the 60% is headquartered in North America and only 30% in Europe[3].

The United States is the home of innovation, with an average value of funding five times higher than that observed in Europe (respectively 10 and 2.7 million dollars). Despite this, there are many interesting cases even in Italy where they were surveyed 20 start-ups (funded or not) ranging from Industrial IoT ("the Internet of Things" Plug and Play "Alleantia) in Advanced HMI solutions (Experenti Srl) until the Additive Manufacturing (Kentstrapper). In Italy, the most fundamental start-ups able to attract financing are in the area of Cloud Manufacturing.

These data refer to the results of the Observatory's Smart Manufacturing Research of the School of Management of Politecnico di Milano.

Development and innovation periods need to be shortened, essential factor for success is becoming the ability and flexibility to innovate and understand the future technology trends to keep for long time the competitive advantage.

To cope with these continuously evolving conditions, firms need to decentralize and to reach faster decision-making procedures. That is the reason why; organizational hierarchies need to

[3] Data from: Osservatorio Smart Manufacturing PoliMi: “L'Industry 4.0 italiana vale 1,2 miliardi di euro”, 21 giugno 2016.

flatten and supply chains of production (of which more later) should adopt digital solution to increase their flexibility and ability to satisfy consumers' needs.

## 1.1: New professional figures

To create a flexible and responsive digital supply chain firms cannot just gather technologies and build infrastructures. They must also manage the shift to a completely new culture, finding people with the right skills, able and willing to carry out the effort. In other words, they must rework their entire organization starting from the human resources.

### - 1.1.1: Chief Innovation Officer

The increasingly important development of Industry 4.0 sees the emergence in the last 10 years of new professions, one of those is the CIO (Chief innovation officer). This figure created in enterprises of the Anglo-Saxon countries is characterized by an innovative profile, which embodies a strategist, an IT manager and a market and management of information systems expert.

Among its many tasks, we can identify the importance of understand and, where possible, improve and rationalize business processes, knowing the business, enhancing human resources, defining and managing the budget dedicated to information systems and organize the management with continuous updating.

The word "Innovation" is not just related to coming up with the best and most original ideas. Indeed, the success or failure of an innovative idea is often a question of time. That means that is crucial for a CIO to have a good experience in the market, in order to be able to predict and see where a specific market might be going, identify possible future product and consumer needs and finally decide and plan how those needs will be satisfied.

After that, he must be able to communicate in the most efficient way those predictions, in a way that make sense to the different workers within the organization. They should explain how they analyzed the gathered data and reached their conclusions mapping out how the organization might adapt and react too those new changing realities.

All this must be achieved by keeping a "do more with less" profile usually with limited budgets, for which reason the CIO needs high communication skills and being a resource optimizer. Therefore, it is not enough to have just a vision.

A CIO needs to have the power to drive ideas and actions around his vision to make it a reality. He does not just need to be able to ideate, prototype, and launch a product, he has to do so in a team environment and in a way, which keeps into consideration each team member's individual strengths and skills.

In Italy, this new figure is still not well known, because of the medium-small size of our industrial structure and the notion that innovation concerns just the scope of research and development.

Even larger companies seem to be still undecided towards introducing a figure devoted almost exclusively to the development of innovation. Abroad, as opposed to our country, the manager of innovation is "catching on", especially among the big brands such as Coca Cola, Johnson and Johnson and Procter and Gamble.

This is because, in a context of rapid revolution, managing a complex business, staying anchored to past business models, is no longer enough. Innovation becomes a top priority for companies that want to remain competitive, or if you prefer, survive.

Often, however, risk aversion, the inability to have a long-term strategic vision and the presence of a poorly integrated business structure, make it difficult for business development and innovation management.

For this reason, it is necessary that companies take awareness of the importance of the Chief Innovation Officer, a manager with cross-organizational development capacity and powers, which go to nourish the creation of an integrated environment, innovation friendly and strictly governing the processes of innovation.

This revolution is not just influencing firms, their human resource organization and processes, is completely changing the way in which manufacturers and common people think the production of goods.

That is the reason why we should move our attention, from the influence of innovation on the closed environment of a company to the opportunities that it offers to the society expanding the possible technology users.

### - 1.1.2: The CISO

With the acronym CISOs we can identity the Chief Innovation Security Officer, a figure that attends the fundamental roles of handling security technologies (technologist) and defend enterprise assets (guardian).

At the same time, they are progressively expected to concentrate more on creating security strategy (strategist) and advising business leaders on security's relevance (advisor).

- **Technologist.** The CISO as technologist leads the strategy, development, and disposition of protected technical architectures, implanting safety standards and executing innovative countermeasures. Technicians cautiously choice and implement platforms that are able to support threat detection, monitoring practices, and integrate facilities delivered by external sources into a unified framework.

  To respect future security needs and standards, they have to guarantee that architecture plans are flexible and extendable. They develop and preserve the security guidelines and standards that an organization should adhere to, collaborating with the CIO to ensure that platforms meet these requirements.

- **Guardian.** As guardian, the CISO's responsibility is to control the efficacy of the security program and procedures. He/she addresses opinions and reflections regarding whether information is correctly shared, if data are protected and controls are working properly monitoring processes that defends the privacy, truthfulness, and accessibility of data driving the entire security program.

  He/she is also responsible to formulate reports about the dangers affecting the information security to keep stakeholders informed and meet compliance and specific requirements.

- **Strategist.** As strategist, the CISO can be considered as the "chief value architect" for all the investments regarding the cyber risks capturing the cost of security expenses to protect enterprise assets. He/she has a deep knowledge of the entire enterprise structure and in this way; he/she is able to provide information and advices regarding how the risk management can support the entire business.

  The strategist is able to understand which are the most important and core business processes and assets developing a strategic governance that can prioritize information security investments and ensures that safety, business resources and budgets are completely aligned to execute the urgencies of the company and deliver the expected results.

- **Advisor.** The CISO as advisor can understand the consequences of new or future emerging threats, and helps in the identification of cyber risks that could arise as the business implements new strategies. The advisor guides the organization towards the

continuous improvement of its security plans and risk mitigation competences understanding where the firm should concentrate on some specific cyberthreats, and in this way, can create a strategic roadmap to align cybersecurity efforts with business risk necessities. Advisors possess significant political capital and are able to recruit, teach, involve, and align executive stakeholders' interests to increase security consciousness.

The Chief Information Security Officer or CISO figure is identified from top management, ensuring that the role is assigned to a person with appropriate skills and experience in the field. In medium / large companies, this role should be assigned a figure devoted to this purpose.

## 1.2: FabLab

Many people are now interested in technology and new digital application, but often they do not have the opportunity to get in touch or know how to use them.

A FabLab (fabrication laboratory) is a small workshop of "Arts and crafts" where a set of computerized tools allow flexible and inexpensive personalized services of digital fabrication.

The main objective of a FabLab, it is to be a space for experimenting with digital technologies and understand how they can influence the development of prototypes, innovative objects and solutions for Smart City, using open source software and big data analytics.

The concept of FabLab was developed at the MIT, Center for Bits and Atoms, also thanks to the course "How to Make (Almost) Anything" taught by Neil Gershenfeld since 1998. He began to understand how relevant was the change that digital fabrication technologies were bringing and that once democratized, would have allowed everyone to access numerous benefits.

From this thought was born the idea of opening a workshop that would allow the usability of these technologies to a wide audience of people; this occurred in the first FabLab from which then took place the development of the whole network of FabLab that now exist. The latter evolved (rather than planned), through the years, without having yet defined business models, processes and tools for improvement.

Before the Center for Bits and Atoms, then the Fab Foundation, in collaboration with the community of FabLab, have long worked to go to delineate the characteristics that define a FabLab. Four are the conditions to be met so that your lab can be called FabLab:

- at least once during the week access to the laboratory should be public.
  Different business models can be applied (e.g. free or paid access), but access must be public.
- The laboratory should sign up and show the Fab Charter, the manifesto of FabLab, within their premises and website;
- The laboratory should share processes and tools with all network of FabLabs, applying the idea according to which a project carried out in a laboratory can be easily reproduced in other laboratories all over the world.
- Finally, the laboratory should be active and participant in the global network of FabLabs, so can neither compete nor isolate themselves.

Inside a digital workshop, you can learn the use and function not only of 3D printers, but also of laser cutting and CNC milling machines. You can scan 3D objects, build electronic circuits and learning how to use the Arduino's system functions.

The latter is a programmable hardware platform, with which you can create circuits "almost" of all kinds for many applications, especially in the field of automation and robotics. It consists of a physical card with micro-controller and a software part, or Development Environment (IDE). Connecting the card to your computer via a USB port allows, through the application of a particular programming language, to go to run any kind of instruction.

Arduino was founded in 2005 in Ivrea, from the brainchild of an electrical engineer and College Professor, Massimo Banzi, who decided to create a platform available to their students, to facilitate them in the study of Interaction Design. This insight was a complete success, to push the engineer to make this Open Source platform.

This means that you can find on the official website www.arduino.cc, components, circuits and the instructions to carry it out yourself.

The most significant effect of this innovation is the circuit diagram: being accessible and viewable to everyone (Open), means that it can be continuously updated and improved by the community and it is thanks to them that were developed several software libraries that facilitate the interface with devices of any kind.

It also has a standard form that allows the manufacturers of electronic components to provide expansions and modifications of any kind in order to increase the possibilities for managing inputs and outputs. The Arduino platform has become very popular for those who are beginning to learn the basics of electronics for its low cost and ease of use.

In fact, every time you write a new code, it can be loaded onto the physical adapter using just a USB cable. You do not need to have special training to access a FabLab, using Arduino and develop a project; what is essential is to be curious and willing to build its own parallel path often to that educational and professional.

Even if they cannot compete with mass production and the associated economies of scale in the production of consumer goods, FabLabs have shown great potential in providing their users with the necessary tools to the manufacture of technological devices. Such devices can be tailored to personal needs thus customization of goods in ways that are still not accessible to large-scale productions.

As already mentioned above, there is still much work to be done on business models that should be adapted to FabLabs, in fact, they can be defined as small businesses, which face a number of costs such as those related to the salaries of employees and vendors. All this must be balanced with funding from public or private organisations that allow reaching the break-even point.

The FabLab therefore must be financially viable to last over the long term. For this reason, at the moment, most of the FabLabs are hosted by universities or research centres or developed in simple places obtained from disused premises or rented at low cost. Now, Italy is the third country for number of FabLabs in the world, but we still have to figure out how to find and how to manage resources better, especially in small communities.

To ensure that new technologies strongly impact on our economic development and become new organisational models, will require a strong cultural action capable of adding value to the "Do It Yourself", hobbies and creating unique consumer experiences in key technology.

## 1.3: Digital Transformation

The term Digital transformation identifies a set of mainly technological changes, but also social, organizational, cultural, creative and managerial skills, which allow the company to go to redesign the offering of their business to make it more competitive and closer to consumer expectations thanks to digital technologies.

Becomes necessary, for a company, to find out whether the technology that is going to apply within its production process, will be efficient in the long run, that is, his analysis should go to try to understand the way that innovation will evolve over time.

Gartner Inc., a leader in the world in research and advice on Information Technology for businesses, has developed a useful model for understanding temporal development of a particular technology: the Hype Cycle, ("cycle of exaggeration"). Every Hype Cycle is divided into five main stages about the life cycle of the technology concerned.

When we should graph the Hype cycle, we have on the horizontal axis the variable of time, while the vertical axis measures the visibility of technology in terms of popularity, if it generates interest in business and in society.

- The first stage is called **"Innovation Trigger"** where a new technology is discovered, often, yet not resulted in tangible products and which we still do not know the possible applications.

  At this stage, the central role is played by the media, who are able to quickly spread news regarding the innovation on which different entrepreneurs will soon begin to speculate.
- The second phase is the **"Peak of Inflated Expectations"**, or "exaggerated expectations peak", during which numerous experiments and improvements are carried out, accompanied by many failures and retries.
- In the third phase, **"Trough of Disillusionment"**, there is a substantial decrease of interest from the market in respect of new technology because the testing does not lead to satisfactory results, investors are in short supply and many companies offering the new technology tend to fail.
- The fourth phase, **"Slope of Enlightenment"** or "Ascent of consciousness ", represents a turning point. Businesses are beginning to become aware of the importance and benefits that this innovation may bring them, the number of investors increases and technology spreads. However, some companies still remain on the side-lines, watching as the events develop.
- The fifth and final stage is named **"Plateau of Productivity"**. The technology is beginning to be adopted on a large scale becoming widely applicable.


[4]

The most important and complex Hype Cycle, is linked to emerging technologies. In fact, researchers are concentrating on the prospects of the impact of innovations on various industries by aggregating, both new technologies for their high level of interest, to those that Gartner Inc. believed to have the highest potential for competitive advantage in the market.

In "2016, Hype Cycle for emerging technologies Special Report", the Gartner Inc., after an analysis of more than 2000 technologies, reveals three distinct technology trends that will fall into the priorities of the companies over the next 10 years.

The first trend concerns the "Transparently immersive experiences": that is, the technology will continue to be more and more human-centric, introducing a full transparency between the companies, people and things.

The second is defined as "The perceptual smart machine age": in the next 10 years the most important technologies are those related to the "smart machine", computational and data processing capability. They will enable companies to improve in problem solving and to adapt quickly to market changes.

[4] Figure 2: Hype Cycle for Emerging Technologies, Gartner, August 16, 2016

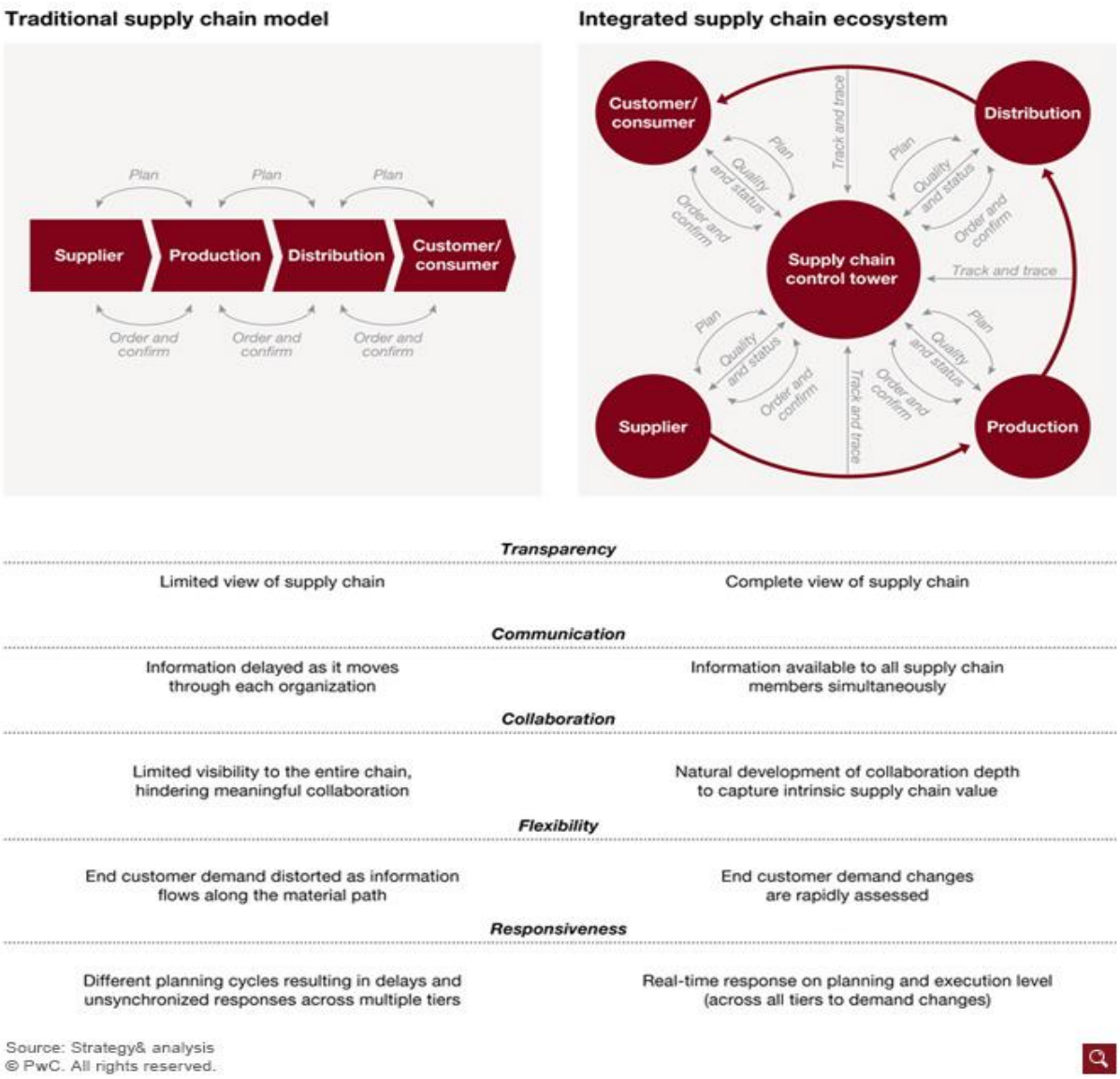
Already existing examples relate to the use, within companies of robots and autonomous vehicles that have completely revolutionized the world of logistics and supply chain management. The impact of smart machine will be increasingly important and it has to be well managed by the CIO within companies, but must also be understood by the entire society. In fact, they will perform more effectively and efficiently the tasks previously entrusted to workers.

The latest trend is "The platform revolution": the emerging technologies are revolutionising the concepts related to the use and definition of the platforms. It has come to creating dynamic ecosystems linking the man to technology; companies must learn to use in order to generate value and going to redefine the strategies with which to plan their platform-based business models.

It should be noted that emerging technologies are primarily focused on the digital world and, in particular, relate to innovations in the fields of mobile, cloud, social and information. These trends show us how it is becoming necessary for businesses to be dynamic and competitive, making technology an integral part of corporate culture, both in production and human resources, both in business relations with partners with customers; they must learn to interact with customers and suppliers by combining conventional and digital channels.

## 2 – Digital Supply Chain

To realize the vision of Industry 4.0, most enterprises need to change and develop a new way of organizing and thinking each of their processes. A critical element is represented by the evolution of traditional supply chains toward a smart, responsive, connected, and highly efficient supply chain ecosystem.[5]




[5] Figure 3- Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused, Stefan Schrauf, Philipp Berttram, September 7, 2016

This ecosystem will be centered on full implementation of a wide range of digital technologies like the Internet of Things, 3D printing, the cloud, augmented reality, big data many and others.

Together, they are allowing the digitization of the production of goods and services, enabling new business models and the integration of every step of a company's value chain.

A supply chain is defined as the global network of organizations and activities involved in designing a set of goods and services and their related processes, transforming inputs in outputs, consuming and finally disposing the goods and services produced. Therefore, the supply chain involves almost all the different areas of an industry, from the procurement through suppliers (upstream supply chain) to the logistic, from marketing to human resources and from the production to the final customer (downstream supply chain).

Usually most companies use a very standardized process to deliver their final products to customers. Marketing department has the role of analyzing customer demand trying consequently to predict sales for the next period. With that information, manufacturing will order the necessary inputs; distribution will account for upcoming changes in the amount of product coming down the pipeline, and to customers will be told when to expect shipment.

If everything goes well, the gap between supply and demand at any level of the system is relatively small, but this rarely occurs unfortunately.

In fact, forecasting always remains an inexact science, and the data it depends on can be incomplete or inconsistent. Too often, indeed, the different departments and figures operate independently one from the others and the lack of transparency among them means that none of them, working in the supply chain, really understands what any other is doing.

Digitization brings down the walls among the different areas, and the chain becomes a completely integrated machinery, completely transparent to all the players involved from the suppliers of raw materials, parts and components, to the transporters of inputs and output, and finally to the customers that buy the final products.

Better yet, transparency will enable companies not just to react to troubles and difficulties but also to anticipate them. Supply and demand signals that can originate in any moment will

travel immediately throughout the network in real time. Thanks to the creation of "what-if" scenarios, the firm can forecast possible future market developments and consequently model its network and adjust the supply chain immediately according to the changing conditions.

When planners are notified in near real time of changes in customer demand, they can quickly assess the impact on supplies of raw materials and consequently on inventory, capacity, and other possible customer orders.

The different possible scenario outcomes can be analyzed to evaluate their impact on financial performance, delivery times and fill rate to identify the final and more efficient solution. This solution is then immediately shared with suppliers, logistics providers, customers, and other partners for further refinement or a final acceptance.

That will allow all involved players and most important, the customer to plan accordingly and the rapid exchange of information boosts the agility of the entire chain.

The digital supply chain consists of eight key elements: Procurement 4.0, smart warehousing, integrated planning and execution, prescriptive supply chain analytics, logistics visibility, efficient spare parts management, autonomous and B2C logistics, and digital supply chain enablers.

The business goal of the digital supply chain is to deliver the right product to the right customer as quick as possible. Companies that can put together these fundamental elements into a coherent and completely transparent ensemble will gain massive advantages in flexibility customer service, efficiency, and cost reduction reducing in this way all the possible delays.

An efficient solution is certainly the integration of data across the supply chain that, often without human intervention, reduces significantly lead times and optimize freight and inventory management.

Driving the transformation to the smart supply chain are two different linked trends. On one hand, we have new technologies, as the cloud, the Internet of Things and big data analytics that are pushing into the market. On the other, there is the ensemble of expectations on the

part of business partners, consumers, and employees, which are pulling companies to develop more efficient, responsive and reliable supply chains.

Supply chain management can be described as [6]"the design and execution of relationships and flows that connect the parties and processes across a supply chain". It is the administration of all processes needed to design, produce, supply and deliver services and high quality goods to customers.

## 2.1: Planning 4.0

Systematic collection and examination of relevant data and information precedes all strategic planning.

Activities related to planning and in particular, sales and operation planning (S&OP) are among the central topics regarding supply chain management. Innovation and the incredibly fast growth of technology it is becoming always more important to build an agile and reactive supply chain planning process with which organizations can significantly enhance supply chain harmonization and performances.

Suppliers have to face increased pressure on performance and their supply chain is significantly affected by increasing customer demand together with the aggressive global competition, compounded by the necessity of reducing transportation or logistics costs and constraints related to infrastructures and production processes.

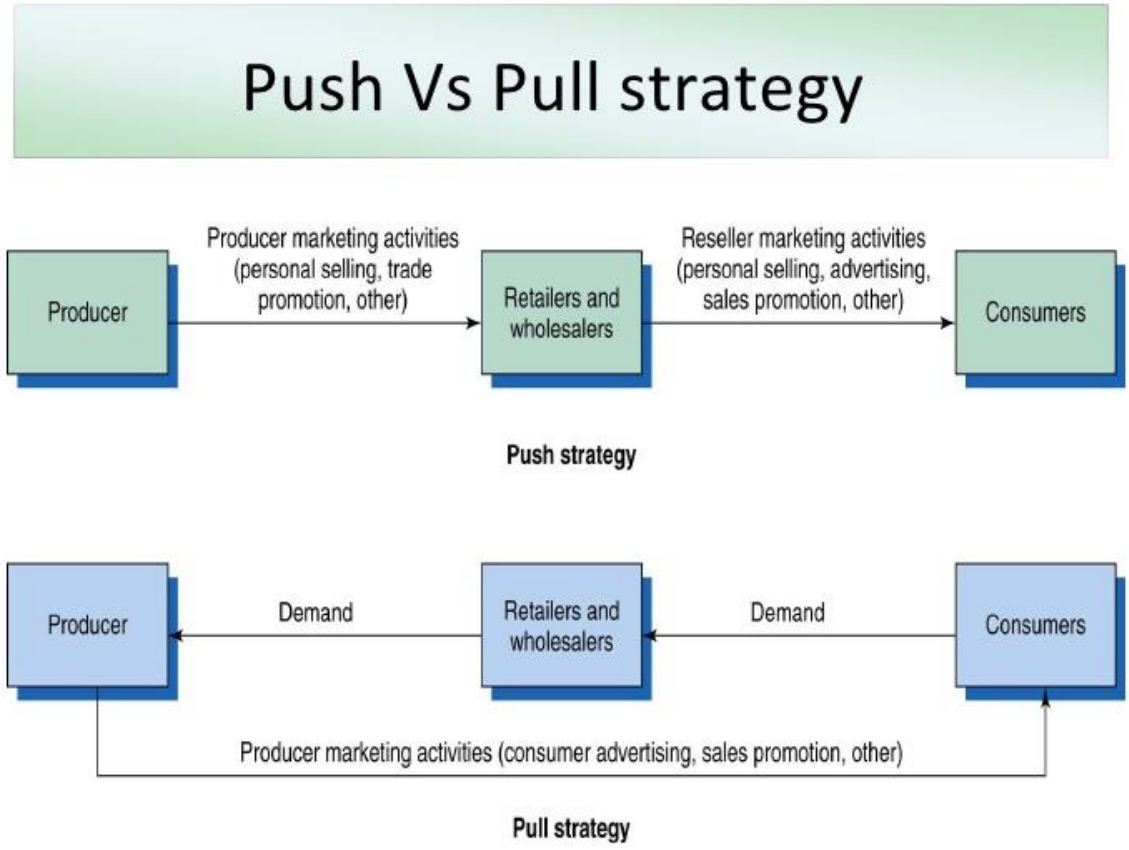
To face these global market complexities, retailers and manufacturers are changing their planning process from a "push" business model to a "pull" business model.

The first one is a strategy where the term push is connected to the idea that marketers are trying to push their products to consumers. This process can include common sales tactics where organizations sell their merchandise directly to customers through company showrooms often negotiating with retailers to sell their products for them, or arrange point-of-sale displays.

[6] Managing Operations across the supply chain, Mc Graw Hill (second edition)

Pull marketing, on the other hand, has the opposite approach. The central goal of pull strategy is to get the customers to come to the firm. Therefore, the term pull means that marketers are attempting to pull customers to their organization.

Commonly used tactics in a pull strategy include a high spending for advertisement, sales and mass media promotions, and word-of-mouth referrals. From a commercial perspective, pull marketing attempts to create brand loyalty and a close relationship with customers to keep them coming back, whereas push strategy is more concerned with short-term sales.[7]




Companies are required to adopt agile solutions to create highly responsive supply chains. Examples are; the supply and demand synchronization through actual demand and the analysis of order trends to be warned in advance of possible constraints, identifying crucial forecasting events and observe events that can provide useful insight regarding changes in demand.

[7] Figure 4- Push and pull strategies

These early warnings allow the organization to forecast and answer to demand movements planning orders of raw materials, production schedule and subsequent supply.

For example, sophisticated analytics software permits demand to be forecasted, much more precisely, through specific tools such as predictive maintenance of machines, trucks and vehicles. That consequently allows organizations to optimize storage and delivery, more information can be gathered and integrated, such as social trends, traffic and weather data, on which demand and distribution can depend.

### - 2.1.1: Big data

In terms of information, a critical element of Industry 4.0 is big data analytics.

Data becomes big data when their variety, speed and volume exceeds the abilities of your IT systems to store, process and analyse them. Many organizations are equipped and expert enough to handle large quantities of structured data but with the always-increasing volume, flows and variety of data, they lack the ability to select the necessary ones for their goals and need new types of data processing and analytic solutions.

Data can be structured or unstructured, collected from instore warehouse, reports, networks video cameras and sensors. However, big data does not always fit into Excel spreadsheet with columns and rows. Indeed, the first idea is to “reduce” the data to a level that allows the organization to put them in a structured form. Then they can be compared to the rest of data and subsequently scrutinized with traditional business intelligence (BI) tools.

For more advanced data analysis, such as data mining, statistical analysis, text mining and predictive analytics, organization have usually moved the data to particular servers for more complex analysis.

Different companies already have the right tools to describe much of the current state of their supply chains where the inputs, raw materials and final products are, where the demand for specific items is currently coming from, and when requested goods should be delivered.

Companies are also learning how to predict critical events, thanks to the analysis of gathered data, that will affect their supply chain and in this way, they can better anticipate market movements and shifts in demand.

Therefore, the next fundamental element in big data analytics will be the ability to prescribe how the supply chain should work and operate. The goal is not simply to improve the delivery time, the management of inventory and spare parts, supply chain's distribution facilities and mobile assets or demand planning. Instead, the real fulcrum is the ability to highlight all the relevant factors that can be improved across the entire chain, and then be able to actively modify them accordingly.

Prescriptive analytics systems support supply chain managers to reach important decisions and can even act autonomously on simple choices. To improve the quality and effectiveness of such decisions, firms will be able to mix external information such as economic indicators with self-learning algorithms to help in increasing the automation level of the decision-making process.

Indeed, with the right amount of data, the analytics engine would produce, for example, a minimum-cost scenario showing not just how much money could the firm potentially saved but also how it should achieve this goal. This scenario could always be adjusted accordingly to other influent factors.

A typical example could be the Toyota case of 2011. If the car manufacturer had known, in advance the risks related to its optimized just-in-time system for delivering components to factories, it might have been able to avoid the costly production shutdowns when supplies were cut off by the earthquake and subsequent tsunami in Japan.

Finally, prescriptive analytics is able to offer very detailed scenarios, describing how product quality can be affect by a shift to a new supplier, or even if the safety on the warehouse floor can be improved by the introduction of new sensors or different robots and autonomous vehicle.

The result is full consciousness and collaboration along different operational, strategic and tactical levels. There is a complete integration thanks to specialized platforms with relevant

planning capabilities, which can support everyday operations, including "what-if" scenario planning. An integrated approach among different functions like logistics, planning and finance can give the firm higher performances but also elements to rapidly solve supply chain issues.

Once the strategy is determined, organization have to exploit their key competences and capabilities to carry it out, in addition to the use of supply chain applications discussed before.

These key capabilities include:

1- **Processes.** Establish end-to-end procedures necessary to connect suppliers and customers thanks to digitization processes, such as how to interact on cloud-based platforms.

2- **Performance management.** Develop a set of specified business rules regarding the management of the entire supply chain, and the key performance indicators needed to measure performances.

3- **Organization and skills.** The entire organization has to switch its mentality from the idea of solving problems when they pop up to prevent problems before they appear managing and optimizing the entire chain. To achieve this level of perception the company also require a shift to an open, transparent and fast-learning digital culture that promotes innovation and communication across different programs, teams, media and users. Furthermore, there is the central need of developing the expertise, skills and talent needed to build the entire technology infrastructure and carry out the new supply chain processes.

4- **Partnering.** Understand the importance of boosting your aptitude to collaborate with other organizations, as a completely integrated supply chain cannot be created without the collaboration with a wide variety of suppliers, wholesalers, and technology providers.

5- **Technology.** Develop a list of old and new technologies necessaries, to reinforce and give strength to the digital supply chain, including data and information database, advanced machineries, analytics capabilities, and the cloud.

## 2.2: Product/Process innovation

Firm's performances can be implemented through the enhancement of product and process innovation. The first one, **product innovation** can be defined as the introduction of goods and services, that have been significantly improved respect to their original characteristics or proposed use.

The improvement can regard materials and components used, software incorporated, technical specifications, design, other functional characteristics or a combination of existing knowledge and technologies integrating different technical subsystems.

Design for example is one of the first characteristics of a product that the consumer can see.

It is an integral part of the implementation and of product innovation; however, the improvements in design element that do not involve significant changes in a product's functional characteristics or uses can't be defined as product innovations, although they can be marketing innovations. In addition, periodical upgrades or regular seasonal variations are not considered product innovations.

This is also due to the fact, that every product has a lifecycle that can be very short or very long, composed by four phases: launch, growth, maturity and decline.

The first step, Launch, represents the presentation of the product to the marketplace, the culmination of a strong effort for the product design and development. When the sales start to grow, customer give information to the firm about how to improve the product characteristics in order to create a standardized good that satisfies consumer requests.

Once the demand is stabilized product refinement become always less frequent, new competitors enter the market and process innovation is often needed to increase efficiency. This stage of maturity can last for many years until the product enters in a decline stage due to technology improvements, changing market conditions, competition and consequent demand decrease.

Firms usually try to avoid reaching the decline stage through incremental product design, development of new features or the replace of the product with a next generation one.

The second one, the **process innovation**, is connected to the implementation of production or delivery methods through important changes in used equipment, planning system, manufacturing methods, or software.

In particular, updated software can be included in different functions of the supply chain such as accounting, purchasing, maintenance and computing. The implementation of an information communication technology (ICT) can be defined as a process innovation if it improves the quality or efficiency of an additional support activity.
In this way, it can allow the firm to increase quality of final goods, reduce processing time and decrease unit costs of production.
Process innovations can be distinguished in production methods or delivery methods:
**Production methods** involve the techniques, software and equipment used to produce goods or services. Examples of new production methods can be related to the implementation of machineries through the use of robots and computer assisted infrastructures, new automated equipment on the production lines or the application of new software for product development.

**Delivery methods** concern principally the logistics of the firm and how it distributes provisions within the organization or how it delivers the final products to the customer. These methods can include new generation software, particular equipment and techniques to obtain inputs.

Example of a new delivery method is the introduction of RFID (radio frequency identification) sensors or bar-coded provided products to track the different good and have always their right location.

There are some significant differences between product and process innovation. Indeed, while the product innovations are usually visible to the customers, process changes are not.

### 2.2.1: IT systems – MES and ERP

In order to answer these expectations, Industry 4.0 concepts should be implemented and applied in the most efficient way possible.
To aspire at the highest operational excellence, manufacturers need increased transparence from the top floor to the shop floor with the possibility to check the status of inventory and its possible changes, the orders management, and the entire process performance.
In particular, it is important to:

- Automatize the production process thanks to the utilization of machines, sensors, terminals and measurement tools all connected together.
- Change the way of transmitting information, not anymore through paper documents but with emails and online networks. Indeed, all the operators should be equipped with PCs, smartphones and tablets that allow them to be always connected to the network and have notifications about any change or new dispositions in real time.
- Finally, to link people, machines and information systems is fundamental to use an IT system in order to reach the complete integration.

This IT system is the Manufacturing Execution System (MES).

A MES is a control system necessary to manage and monitor the entire process of production, the needed data, the quality of used materials and of the final output and the work-in-progress on a factory floor. A MES keeps track of all manufacturing information in real time, receiving and transmitting up-to-the-minute data from machinery, robots and employees.

Therefore, being able to manage integrated data in a single database allows information not to be just passively recorded, but to transform it in a base to create on it further events.

MES has been always considered necessary to fill the gap between the business level planning (ERP and Business Applications) and the executive one (the shop floor).

The **Enterprise resource planning (ERP)** system could be defined as the ability to deliver an integrated series of business applications thanks to the use of tools that allow sharing data model and common processes, covering deep operational end-to-end procedures, such as those of manufacturing, distribution and the supply chain.

ERP applications are necessary to manage, connect and automate a wide range of administrative and operational business processes across all core areas of the organization and among multiple industries. They allow decision makers to improve business operations such as; order management, inventory management, human resources, accounting, customer relationship management (CRM) and product lifecycle with the final aim of reducing cycle time and refining decision-making.

By integrating a MES and an ERP software, factory managers can ensure to deliver quality products in a timely, cost-effective manner allowing an industry to be transformed into a Smart Factory, an active, dynamic and clever company where the events start automatically, autonomously and in real time.

"The customer and customer alone determines whether we win, or we lose. This is increasingly a customer-to-business global economy; the business-to-business-to-customer economy is going away. … Big Data and analytics, the Internet of Things, [and] social media all enable businesses in every sector to reach and thereby better know and fulfil their customers' needs and wants. The digital supply chain holds the promise of real-time data to sense demand, drive innovation, reduce cost, and deliver the customer the right product at the right time and price."[8]

Therefore, important is to analyse the influence of the Digital Transformation on the different functions of the supply chain.

## 2.3: Procurement 4.0

Procurement is defined as the function of a firm related to the activities and processes to acquire goods and services. Its meaning is different from the one of "purchasing" because it involves a different number of activities beyond the ones required to order and receive goods, such as market research and analysis, supplier evaluation, the establishment of fundamental requirements and negotiation of contracts.

Digitizing this function will deeply change the abilities and tools required, in many organizations this process is already on its way as companies are using a variety of procedures and big data tools to connect more closely with suppliers, improve sourcing, enhancing collaboration, aid the planning process and actively manage supplier risk.

In fact, organizations are everyday facing six major sources of risk linked to supplier activity:

- **Execution,** related to the fact that the buyers have to stop the production because they do not receive the requested services or tools on time or in the correct location and other risks could be linked to the disrespectful conduct of suppliers towards safety and environmental regulations.
- **Commercial,** linked to the failure of the buyer of keeping track of suppliers' activities in particular if they bill properly and comply with contractual terms.

[8] Bill McDermott, CEO, SAP 2016

- **Continuity,** because a great source of risk is certainly suppliers' financial stability.
- **Competition,** in fact there is risk that some suppliers can have conflict of interest or they could steal intellectual property rights from their buyers or other competitors.
- **Compliance,** connected to the importance of knowing that suppliers must conform to legal and regulatory requirements, such as tax laws, labour laws, anti-corruption legislation, and domestic government requirements.
- **Cyber,** correlated to the increased use of interconnected devices that facilitates the loss of data, privacy problems, the spread of viruses and malware and will influence the IoT development. I will go back on this topic later on in the next chapters.

Another important advantage of digitization is how it allows purchasing to reallocate resources in a more efficient way by eliminating the non-value transactional work necessitated by traditional paper-based processes. That will enable organizations to use their more strategic resources, their people, to completely focus on their core competencies and consequently increase competitive advantage.

However, the evolution of the supply chain system will have numerous other consequences for the procurement function as well. Indeed, the transition to the Industry 4.0 will require firms to buy not only physical goods like sensors and electronic components, but also digital inputs and services like digital platforms, software maintenance contracts and developers.

Therefore, the biggest challenge will come as software and services become a core and always more essential feature of the outputs that an enterprise produces. Already, the software embedded in many different products, is more valuable than the physical materials by which them are created.

Moreover, many organizations are now transitioning to the cloud because it enables to mitigate the risks linked to the paper-based system and the 24/7 real-time visibility of all data that the cloud provides allows procurement to analyse and use the gathered information results to focus on supply chain improvements and flexibility reducing the risks throughout the system.

Thanks to this visibility, procurement can answer to different questions immediately instead of guessing possible answers. Human resources could know which suppliers are the most reliable and which ones are not in line with contract terms, if they are over or under purchasing and when deliveries will occur and if it will be necessary to order new raw materials.

In this way, they can fulfil calendar-based demands programming all the different steps of the production process and the efficient connection and management of inputs is a critical building block in the digital supply chain network.

## 2.4: Smart warehousing – logistics

Industry 4.0 is enabling warehouses to be always in line with the progressive changes of the entire market transforming them in one of the most strategic tools that a firm can use to create its strategic advantage.

The final goal of this transition is the improvement of safety and efficiency through the automation of almost every warehousing activity. Indeed, the increasing focus on multitasking abilities creates great pressure on organizations to keep up with a higher number of orders, and the necessity of rapid processing and management of the spaces, to improve economies of scale and ensure high throughput.

In the last several years, there has been a migration from warehouse-based storing to the application of very fast and flexible operations that allows pushing down overall costs. This new model is known as distribution centres (DCs), fundamental component of the supply chain infrastructure no longer seen as costs creator, but rather as strategic facilities, that can allow to increase the competitive advantage.

A distribution centre can be defined as a transhipment point, a facility where inputs are received, stocked and selected according to customer needs.

Some of its functions are:

**"Stockpiling"** or the storage of inventories to protect the production against the seasonality of demand and supply and **"Production support"**, because a warehouse activity is dedicated to storing components and parts needed to support production operations.

The transformation of the warehouse begins with the renovation of inbound logistics.

"Logistics typically refers to activities that occur within the boundaries of a single organization and supply chains refer to networks of companies that work together and coordinate their actions to deliver a product to market. In addition, traditional logistics focuses its attention on activities such as procurement, distribution, maintenance, and inventory management. Supply Chain Management (SCM) acknowledges all of traditional logistics and also includes activities such as marketing, new product development, finance, and customer service"[9].

In particular, inbound logistics refers to the transportation of inputs and raw materials from suppliers to your firm. In contrast, outbound logistics refers to movement of outputs and finished products from your company to the final customers.

The entire digitalized warehouse system will be principally governed by the utilization of sensors. For example, trucks that are coming to the distribution centre will communicate their position (thanks to the use of GPS) and arrival time to the intelligent warehouse management system, which will choose and prepare a docking slot, in order to optimize delivery.

RFID (Radio-Frequency Identification) sensors will reveal what has been delivered, and will send the data across the entire supply chain. The inventory will be updated constantly by the management software, which will automatically designate the different storage spaces and give input to the autonomous machineries to move the products to the right location.

This can be defined as a **"track and trace"** (T&T) system that allows companies to be always informed about the status of any given shipment of good at any moment of its travels, by any transport mode. The ensemble of data will be captured from ERP systems (enterprise resource planning systems) through direct connections or via third-party portals. However, an important technological barrier is represented by the fact that because data are arriving from

[9] Essential of Supply Chain Management by Michael Hugos

many different sources such as distributors, suppliers, warehouses and transporters their value, quality and interoperability are critical.

This is possible thanks to the use of sensors implanted in goods and the distribution centre itself and ultimately different organization are using drones and augmented reality to map the entire facility and aid in assessing the storage spaces.

Software and robots will also control the entire warehouse environment. This include shutting off or on the lights in an established moment of the day, setting the level of heat and humidity according to defined requirements (dependent for example to the stored inputs). All this system can allow firms to reduce energy consumption and pollution.

Furthermore, firms in agreement with suppliers can decide to apply different strategies related to inbound and outbound logistic and dependent on the covered area structure.

In a **"Break-bulk strategy",** suppliers, adopt a market area consolidation strategy trying to reduce transportation costs. They send in this way large shipments to the warehouse that then conducts a break-bulk separating the inputs into individual orders and preparing them for a local delivery to customers.

In a **"Warehouse consolidation strategy"**, the distribution centre receives raw materials, components and goods from a series of different sources and combine them in one big shipment going to a single location. This can give the opportunity to the customer to receive a varied assortment of products in the same day and can exploit transportation economies.

Finally, in a **"Cross-docking strategy"** there is a combination of break-bulk and consolidation activities. Large shipments from many sources are scheduled to arrive at the warehouse facility where at the same time at the shipping docks a set of trucks are positioned to ship the received inputs to different destination. This approach makes easier the process of unloading and reloading and is often used by mass merchants and grocery.

Naturally, this strategy is not always feasible with the organization structure because requires a particular attention and precision in scheduling processes not always easy or possible to do.

After the transformation of raw materials in finished goods, it is the turn of the outbound logistics. Products are picked and packaged for shipment through the work of robots, able to manage different product sizes and that consider the data connecting the product to the customer that is requesting that defined output.

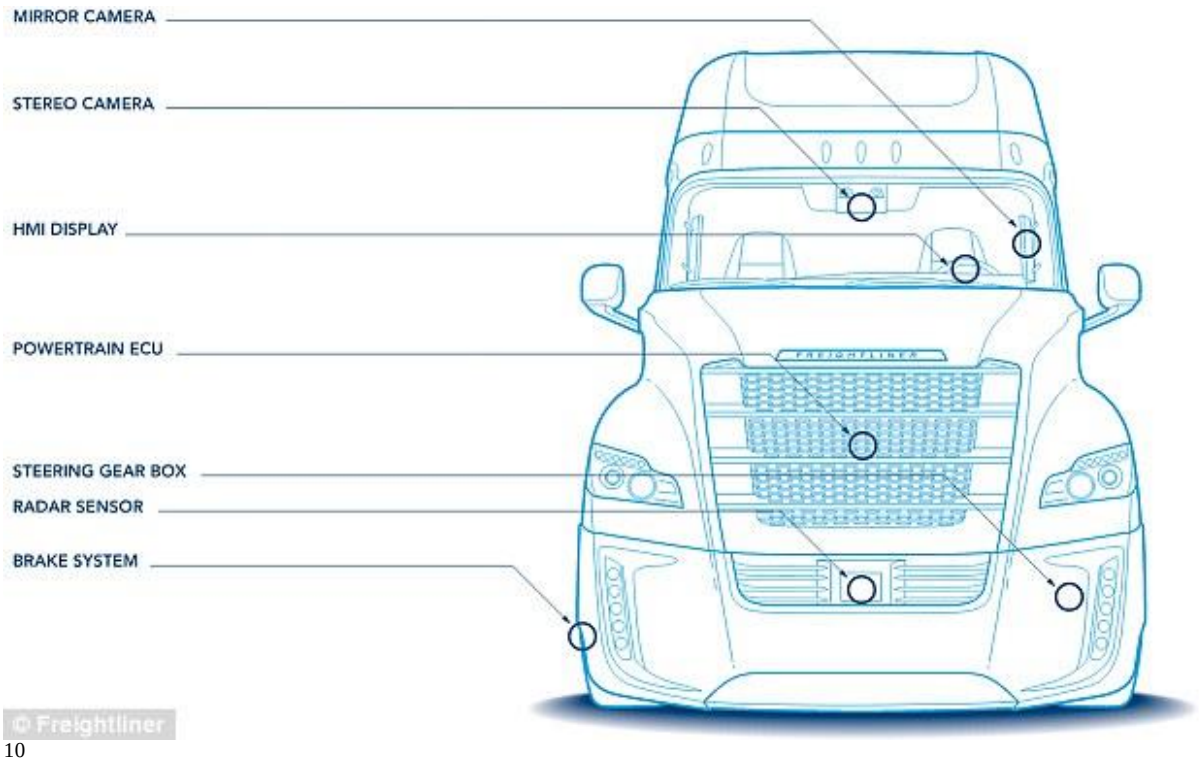
### 2.4.1: Robotic transport

Deepening the concept related to the use of sensors in transportation, we can say that the most common used autonomous vehicles in logistics are driverless trucks.

These self-driving trucks are dependent on a software that uses maps and short-range radars to guide the vehicle on different roads and assess the environment surrounding it.

This innovative system and the wireless connection to other vehicles can create a flow of data and information that allow reducing accidents and traffic jams as well as speeding up the traffic flow. There is a reduction in needing of human drivers, trucks can drive closely together thanks to proximity sensors and their internal system will determine when it will be necessary maintenance interventions.

The advantages that these innovations bring are manifold, lower labor costs, reduced emissions thanks to the increased efficiency of operation, the elimination of human error and faster and more reliable delivery times.



[10]

With the tight integration with the organization's ERP system, these vehicles will have the ability to determine by themselves, which inputs need refilling within the production process, when it is time to pick up loads from storage site and drop them off in the identified space, and gather returnable packaging. They can move around parts, components and raw materials within the same organization choosing autonomously the best route without human interference.

Another important element is "last-mile delivery" referred to the step in which the product arrives into the hands of customer. This is a labor-intensive logistic phase with really high costs because it requests a great interaction between firm and customer.

Different ideas have been analyzed and implemented for lowering costs and create a better and different customer experience. Examples of them are self-driving delivery robots monitored by human operators able to distribute packages along predefined routes (here we can certainly talk about Amazon's idea of using drones to deliver packages from the sky in front of

[10] Figure 5- Self-Driving Truck: The truck that drives itself! Freightliner Trucks takes its first autonomous vehicle on the road in the US, Kate Pickles, 5 June 2015

customer's houses) and another idea is related to Uber-like apps that can employ nonprofessional drivers to bring packages to the customer.

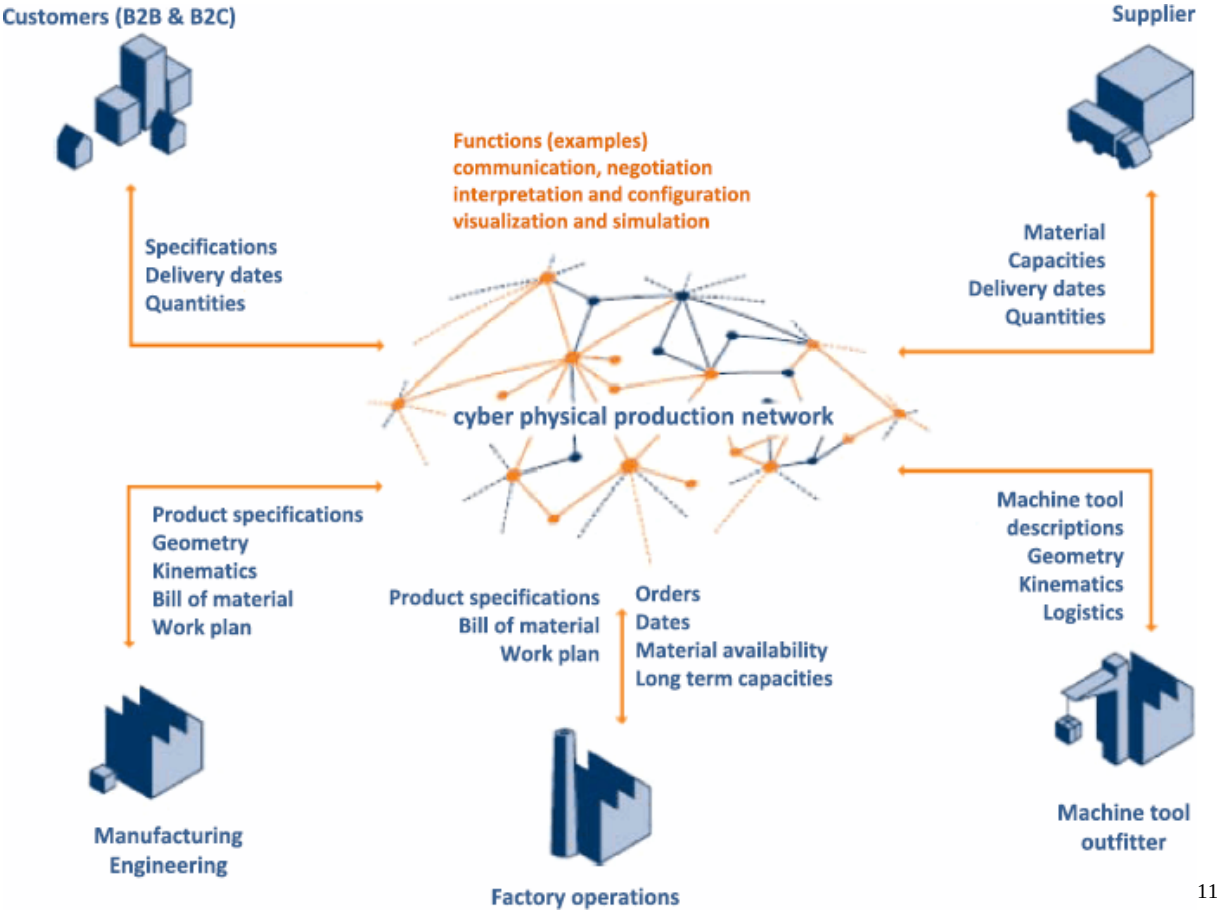
In some particularly specialized companies is even possible to work with vehicles that operate as a team, provided with technologies that enable them to coordinate with one another to identify the best and less busy roads and to determine the most proficient use of group's assets.

## 2.5: Information and communication

The key factor that can lead to success any supply chain is certainly the efficient exchange of information: communication. The traditional supply chain is primarily slowed by a lack of timely and complete information. Sudden shifts from the demand side, natural disasters and lack of raw materials, can create not few problems to the supply chain plans and activities. Furthermore, the outsourcing of many fundamental steps only makes it harder to understand the supply chain in its entirety and makes difficult to solve problems as they occur.

B2C markets are continuously demanding for information to companies about shipment and delivery with real time updates, obliging firms to provide this or an even better level of transparency. In B2B networks, communication is fundamental because producers base their entire production schedule and program on information regarding their supply shipments. Furthermore, reliable and constantly updated information related to transportation can significantly increase the producer's ability of planning with a higher consequent customers' satisfaction.

Benefits that an organization can reach with a high level of communication and information transparency are significant. They are not just limited to costs savings planning improvement and a better inventory management, they regard the entire structure of the firm its internal and external environment. If there is a good level of communication, there is no need to repeat or clarify notions and detail wasting precious time for work.




[11]

In addition, it has been demonstrated that when a manager effectively communicates his/her expectation and goals, his workers will be more motivated and will perform in the best way they can.

Furthermore, an effective communication can help improve the development of team works because the organization will be focused on well-identified goals and the workers of different departments will share their information to reach those targets. The overall morale of the workplace will improve and a positive environment will develop because of the clear expectation.

Obviously, a high degree of transparency is not easy to obtain, because it requires a well-oriented human intervention and a specific technological structure.

[11] Figure 6- Organization of the interconnected network

Information and Communication Technology (ICT) refers to technologies that provide access to information thanks to telecommunications. It includes the Internet, television, instant messaging, video-conferencing, cell phones, voice over IP (VoIP), wireless networks and other communication mediums that allow people to communicate in real-time with others in different countries. Furthermore, the new digitized supply chain is usually based on a unique central hub of data storage that collects information from different access points, in this way it results easier to gather data and review those necessary communicating eventual results.

The Internet plays also an important role in electronic commerce today, it empowers the supply chain through vehicles such as e-mail, the World Wide Web, intranets, file transfer protocol (FTP) and extranets creating in this way an interconnected infrastructure certainly more flexible, efficient and global.

## - 2.6: Production 4.0

The future of production will be based on the development of efficient manufacturing systems and structures in which products are able to control their own manufacturing process.

As we said, we are having a strong and quick increase in mechanization and automation. In the development of a production process, always more technical instruments will be used to support physical work. There is a progressive introduction of automatic solutions able to execute different versatile operations, such as "autonomous" manufacturing cells, which can independently improve and control manufacturing process in various steps.

The advanced digitalization of the different manufacturing-supporting tools is giving as result the recording of a growing amount of data regarding sensors and actors, which can support functions of management, analysis and control. Digital processes are evolving together with the ensemble of technical instruments and machineries that can be use inside the warehouse such as augmented reality, 3D printer, wearable technology and sensors creating in this way a completely digitalized environment.

At the same time, nowadays, there is an interesting trend towards miniaturization.

Devices with a comparable or even extremely better performance than the past ones can be installed, today, on few millimetres or cubic centimetres. This empowers completely new chances of development and fields of application, especially in the context such as logistic, and production.

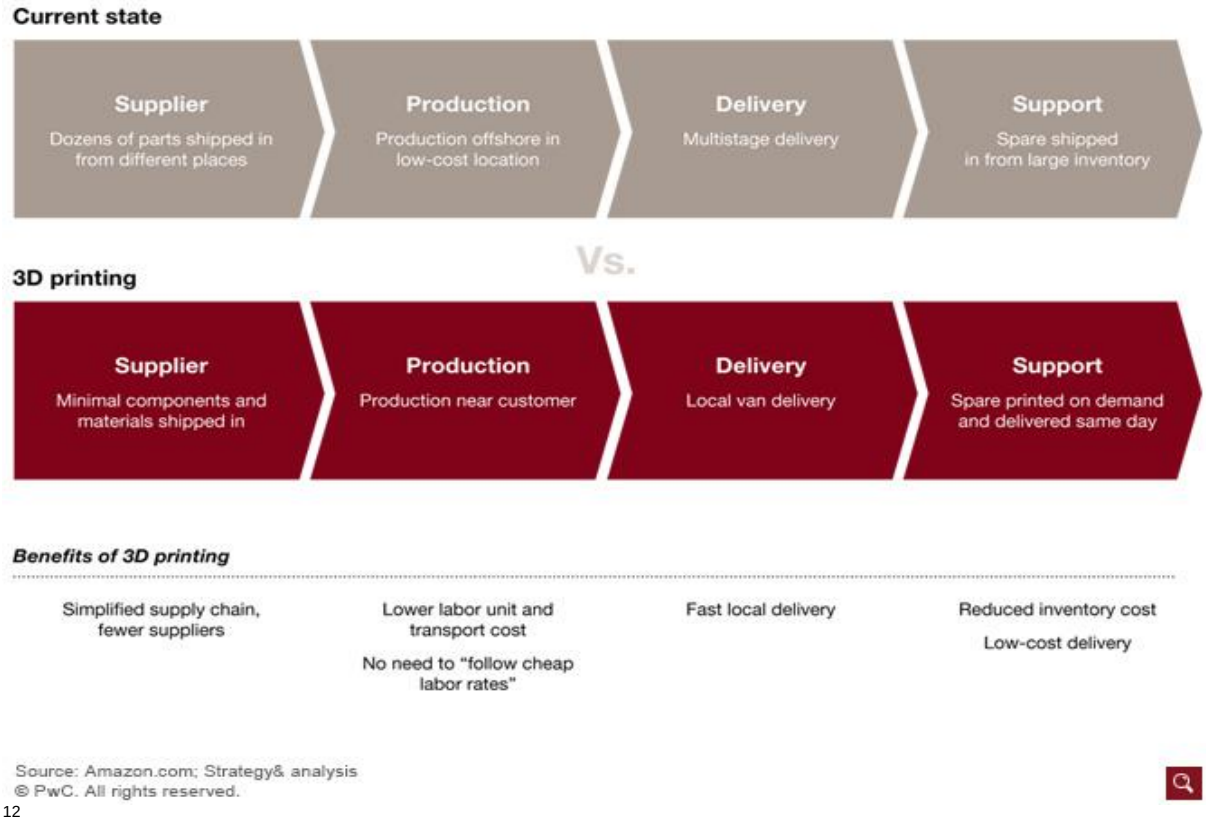
### - 2.6.1: 3D Printers

As previously mentioned, 3D printing means the realization of three-dimensional objects using additive manufacturing techniques, starting with a digital 3D model.
This model is made with a particular developed software and subsequently elaborated and composed, layer by layer, through a 3D printer.
Therefore, the goal is no longer create surface but volume.
Going deeply, this production process starts from a three-dimensional virtual model of the object that, processed by specific programmes, is decomposed into layers of a few hundredths of a millimetre thick, which deposited by printers able to compose and consolidate, layer by layer, give the finished product.
The procedure can take place for selective laser sintering (SLS) or heating up the appropriate material, usually metal or thermoplastic substances then place them in the correct location or through Fused Deposition Modeling (FDM), which uses a heated nozzle that goes to raise the temperature of the material before depositing it. In this case, plastic or metallic filaments are used, rolled up on some sort of bundle that is progressively rolled out during printing.
The origins of this great innovation, date back to 1980, when Chuck Hull, American engineer, co-founder and President of 3D Systems, invented Stereolithography, a technique that allows for the creation of three-dimensional objects from digital data, processed by a CAD (Computer Aided Drafting, or Computer-aided design) and CAM (Computer Aided Manufacturing) and who first made a processing additive.
3D printing technologies, include three main categories such as Stereolithography, selective laser sintering, melting filament with a dozen of derived categories, all united by the production of objects layer by layer, that allows to realize plastic or metal parts using only the required material.

A 3D printer can also create just a single object, starting from the idea and CAD design. This concept is changing the perception of the importance of economies of scale, which become something closely tied to the past. In the coming years, could then emerge new industrial model: the 3D printing industry, which include machinery, goods, services, software and new materials.

Now that 3D printers have reached affordable prices for professional undertaking, and even for many consumers, these scenarios are multiplying, combining with other existing technologies such as the Internet, the cloud, social networks and other digital tools of shared creativity.

Now that 3D printers have reached affordable prices for professional undertaking, and even for many consumers, these scenarios are multiplying, combining with other existing technologies such as the Internet, the cloud, social networks and other digital tools of shared creativity.




[12] Figure 7- Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused, Stefan Schrauf, Philipp Berttram, September 7, 2016

The examples of industrial applications of this technology are increasing, both on the part of large international companies, and both by smaller companies. Such examples are classified into four different areas: prototype/pre-series (Rapid Prototyping) which means that the application of this type of technology is aimed at creating prototypes of finished products or components, thanks to the functional and aesthetic evaluations.

The benefits are related to the compression of the development time, the ability to print different elements in a single process, giving the opportunity for engineers to evaluate the best combinations to meet market demands. Indirect production (*Rapid Tooling*) which means the realization, inside the company, of instruments, tools and equipment needed for production.

The direct production (Rapid Manufacturing) that thanks to 3D printers, gives the ability to obtain more complex forms and shapes not necessarily achievable with subtractive methods, and allows the increase of some mechanical properties of the products.

Finally, the spare parts, in fact a major benefit of working in 3D is the ability to print "on demand and on site" the various parts needed to replace worn parts of machinery or durable consumer goods without having to own large storage spaces and avoiding the risk of obsolescence.

The materials used are many and depend on the type of printer available. These are mainly Thermoplastics substances (FDM technique) and photopolymers. In selective laser sintering using instead compounds that have a metal as base, ensuring a higher resistance of the final result.

Thanks to the evolution of technology, new materials such as carbon fibre and materials identified by the acronym PLA or ABS are quickly developing. The first (PolyLactic Acid) are derived from corn-starch and thus biodegradable, while the latter (Deverwerking) are petroleum products that emit potentially harmful fumes when heated to health.

The latter are sometimes preferred for their greater resistance to mechanical stress. Moreover, while the 3D printed plastics have limitations in terms of final quality the printed metal components, for example, has the same mechanical properties of what worked in the traditional manner, with the addition of infinite geometric and new possibilities offered by digital and additives production methods.

Particularly delicate topic in this case is the "copyright" as the control on these types of activities, it will be nearly impossible. In fact, the ability to print anything in domestic/private scope could have serious effects on the economy of certain areas.

The definition of "copyright" should clarify the distinction between original and copy, setting limits and rights on one and on the other side, with rules and laws dictated by market requirements and stakeholders. There will probably be the necessity to legislate to prevent any propagation or source file sharing network, but the exchange platforms, communities, and peer-to-peer networks make Challenger the work of lawmakers, as information systems are hard to harn.

The 3D printing industry has enormous growth potential, currently worth about 6 billion dollars, while that of global watchmakers' worth between 12 and 20 trillion; It will also be difficult to predict the impact of technology on the world of work and processes of distribution, warehouse management and logistics activities.

### - 2.6.2: Wearable technology

With this terminology, we do refer to a category of innovative electronic devices, equipped with one or more sensors with various and numerous processing capability. We can define wearable technologies, belts, bracelets, watches and electronic smart glasses and helmets, fabrics and clothes cyborg, HMD (Head Mounted Display), tattoos as bar codes or RFID and much more.

Each of them is modelled around people's body, which is used as a natural support to their functions. They are useful to capture data, simple or complex, making them understandable and readable in order to share, analyse or communicate them. These data may refer to the detection and monitoring of body signals such as heart rate, the number of steps during a walk or electromagnetic waves that accompany brain functioning.

This kind of technological aids becomes a viable form of support to the needs of the user, facilitating the expansion of its sensory capacities and control, which can have on your health and vital functions. Form of communication used by these devices are different in fact they can work wirelessly, and everything depend on the type of device and display used.

Communication can happen through intermittent flashing, vibration or a composed and articulated message similar to a text message or an email. New forms of computerized objects are able to provide connectivity and continuous interaction with the user, applications and sensors that turn the device into a Wearable Technology Assistant are always available and integrated with practical skills and cognitive abilities.

Some technological devices allow you to communicate (CommBadge), to take photographs or to film (Google Glass) and synchronize with other devices like tablets and Smartphones. Still others are smart objects rich in applications (smartwatch, smart glasses, etc.) that work as small computers.

The wearable technology is evolving today towards objects with increasingly large storage capacity and processing keeping the same dimensions, the evolution is possible thanks to the increasing miniaturization of processors and above all the development of chips that combine the processing component, with part of the sensors and with other functions. In this way, you can create objects to wear more comfortable, small and powerful.

However, the miniaturization of components has also the goal to make "disappear" and hide the sensors by integrating them into objects of common use as personal accessories (jewelry, bags, etc.). In parallel, another evolution is handing out wearable in different parts of the body, or a dress, for example, by splitting them into smaller components and keeping in contact by conductive fabrics or wireless connections.

Several projects of this kind are carried out in sports and fashion. Wearable are also smart glass, glasses, which integrate the operation of a small camera and a micro-projector which, through a front panel optical Prism, brings up text and images in the field of view of the wearer. This device allows the creation of augmented reality applications that go to "enrich" the information available to the user.

The field, which takes greater advantage from the evolution of wearable, is the medical one: the miniaturization of components and the evolution of sensors allow creating wearable devices that keep track of various vital signs without being a hindrance to the wearer, thus reducing the need to go to the hospital or by a doctor to perform regular checks.

The implications and uses of wearable technology are far reaching and they can affect many areas and models of production and prototyping. In 2014, about 19 million wearable technology devices were sold worldwide and in Italy over 600 thousand. Certainly, a number that is expected to grow.

Covers all topics and technologies that turn production into a cyber physical system characterized by self-organizing, autonomous manufacturing processes. The optimum lot size does not need to be calculated and is no longer fixed, it is done on the fly by the system. Supporting production through augmented reality and instruction-manual videos on mobile devices directly in the production line empowers people to conduct every step in the

production line without making mistakes. This means that the efficiency of Taylorism, which aims for maximum machine utilization, is transmitted to highly customized production, all the way down to a lot size of one.

Customers get their customized product and the producer enjoys maximum efficiency. The fact that this vision is becoming reality has been shown at Bosch Rexroth in Homburg. Their system allowed them to reduce inventories by 30% while increasing output by 20%. Digitization technologies are making mass customization feasible.

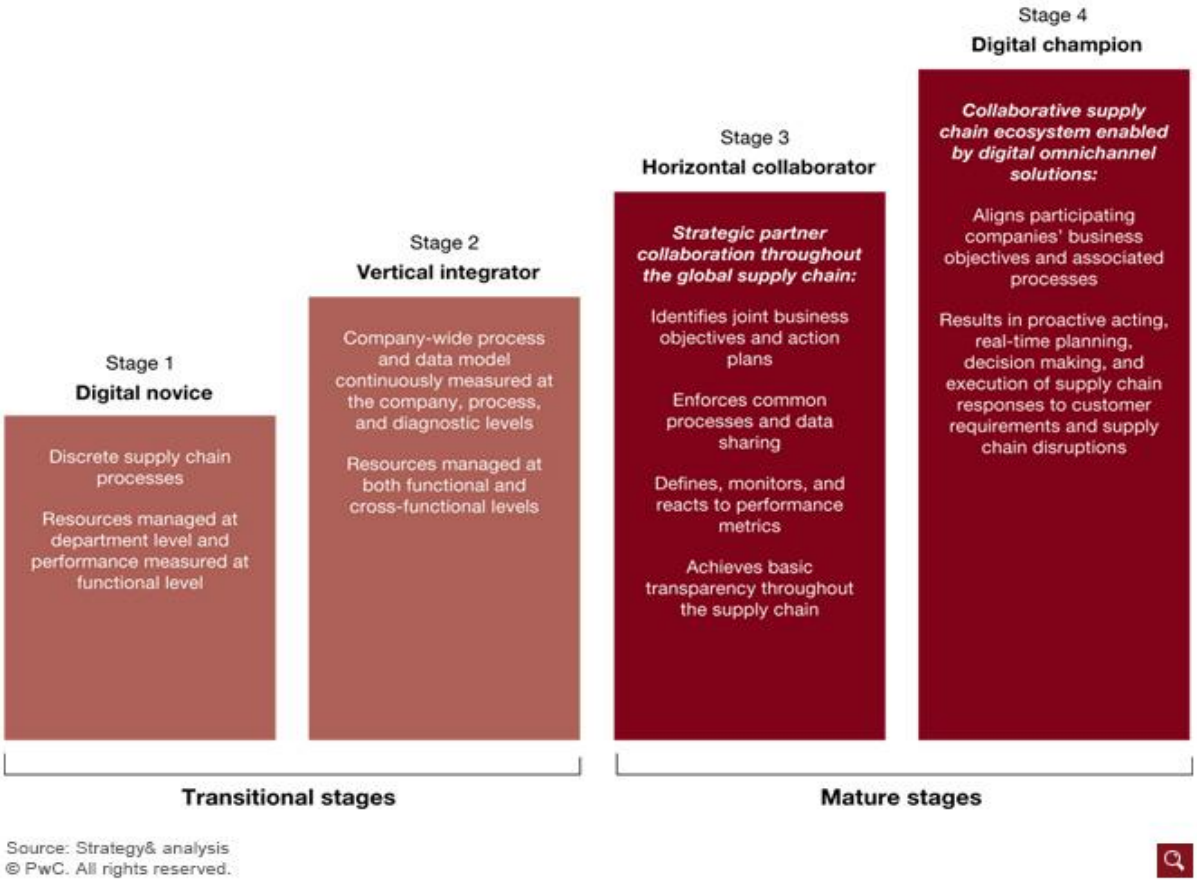
## - 2.7: Supply chain stages

To develop an efficient supply chain strategy and organize its subsequent activities in a coherent way, it is fundamental that organizations understand their stage position in the development scale. The process leads through four stages of maturity:

1- **Digital novice,** these companies supply chain processes are still at a basic development level, remain disconnected, carried out by separate departments and business units.
2- **Vertical integrator,** companies at this stage have accomplished to integrate internally, across functions and departments, their supply chain processes.
3- **Horizontal collaborator,** here, companies have learned to set business goals and reach them working with their supply chain partners. They can delineate and carry on common projects, and achieve a fair degree of flexibility and transparency into the chain.
4- **Digital champion,** at this final level firms have achieved the highest level of integration and collaboration with partners and a full transparency into operations.
   At the same time, they can develop, improve and integrate their processes obtaining common benefits and analytical techniques to optimize their entire supply chains.

Supply chains are exceptionally complex organisms, and no company has yet succeeded in building one that is completely digital. Indeed, many of the essential technology and applications are not yet widely used. However, this will radically change over the next five to

ten years, with different industries implementing digital solutions at different levels and speeds. [13]




Organizations able to reach this high digital level for first will gain a difficult-to-challenge advantage in the fast race to Industry 4.0. Furthermore, they will be able to set and influence technological standards for their industry combining productivity and quickness in responding to market.

Obviously, who will not undertake this path will progressively be excluded from the global competition.

[13] Figure 8- Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused, Stefan Schrauf, Philipp Berttram, September 7, 2016

## 3: Critical aspects of Industry 4.0

To each period, you can attribute defined aspects that characterize and differentiate it with respect to others; and together they can grasp the sake of continuity.

A first production period is identifiable in the time between the two industrial revolutions, where manufacturing takes a vital role in the economic and social context. The sequence of the first and second industrial revolution over an economics century (1840-1970) contributes to the emergence of different organizational paradigms, fruit progressive affirmation of many scientific and technological ones, which will mark the path of progress until the birth of modern industry.

The booming inherited from the years of industrialization, the rise demand and the expansion of markets over time trigger a thrust to increase size of enterprises: the factory becomes the temple of the development.

Economic and the most tangible representation of what we now call industrial capitalism.

The growing interaction between science, technology and the world of production leads to define the second industrial revolution as Scientists Revolution and at the same time, just due to the mechanization of the manufacturing sector, it causes an increase in the so-called technological unemployment.

The expansion of company size, the advent of big business and mass production require a new organization production, capable of obtaining the maximum production at the lowest cost and with the least use of labor. Companies focus their attention on achieving economies of scale through the specialization of production and standardization of production processes and behaviors related to manual work.

The labor market, for its part, is dotted by presence of low wageworkers, mostly intent to meet those Maslow (1954) it defines primary needs.

With the third industrial revolution, of the end of 1960's we have the first programmable logic controller (PLC) that marks the introduction of electronics and information technology for increased automation of production.

Meanwhile, the unstoppable evolution of ICT and the Internet radically changes the way to communicate in everyday life and in many organizations; it is thus creating new challenges and new opportunities both in the production world of manufacturing and in that of human resource management and work organization.

Since 2014, we have now shifted into real-time connected and auto-optimizing production systems.

The production is always more focused to the end customer; firms are seeking to provide products customized and diversified. The role of marketing is becoming more relational and interactive, in order to create a thread that constantly bind the production with the network, or better, that binds the network of producers to the consumers.

At the dematerialization of the manufacture is then accompanied the industrialization of the service sector, which it is now able to offer standardized services through the use of replication technologies that allow to increase of the volumes and reduce the costs of replication.[14]

Business service sector absorbs a large part of the workforce, while in manufacturing factories robotic automation becomes a widespread reality, up to it no longer requires any human intervention except for reprogramming actions.

It follows a rise of the "threshold skills" required in order to operate in modern factories, and a consequent rethinking of training and education policies in order to identify innovative formulas, the enhancement of human capital based on closer cooperation between institutions, businesses, universities and research centers, in line with the new demands of the manufacturing knowledge.

## - 3.1: Robots will steal our jobs?

Digital Transformation is progressively changing the way of how industrial workers perform their jobs, with the increasingly diffused use of robots and machineries entirely new job families will be created while others will become obsolete. It is certain that robots and humans will increasingly have to work alongside one another in the workplace. Indeed, robot sales are expected to grow at 12% per year for at least the next two years.

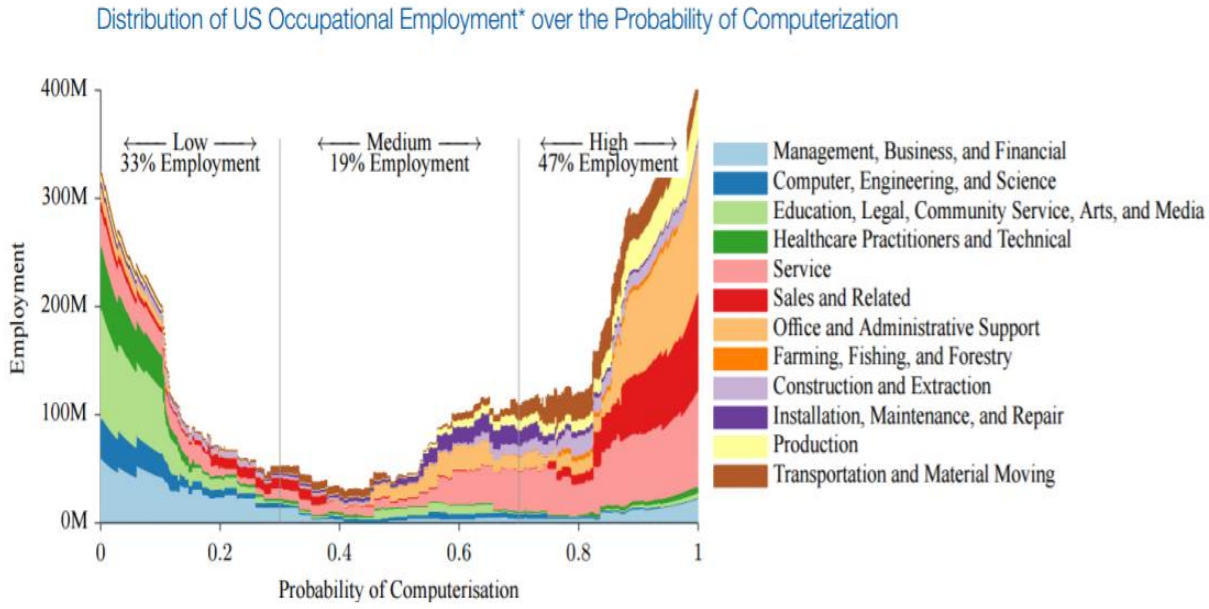
The number of routine and physically demanding jobs will decrease, to perform effectively with Industry 4.0, workers will need to apply a variety of “hard” skills and employees will have to be even more flexible and open to change because always more jobs will require quick responses, problem solving, and customization. The adoption rate of technological

[14] Rullani, 2014

advancements will lead to significant productivity gains, thereby reducing the number of employees required to achieve a given level of output.

Economists are worried about the phenomenon of **"job polarization"** characterized by the decline of middle-skill jobs and the increase of low-skill and high-skill jobs.

In this way, the workforce is divided into two groups, the first doing non-routine work such as skilled and highly paid workers the second one doing routine work such as unskilled low-paid workers.




[15]

Furthermore, other kind of jobs will be progressively eliminated;

first of all, **high routine occupations** like clerks, accountant, or desk officer being characterized by high level of routine in their performance, and in general jobs where employee sits in front of a computer and interprets data are at a high risk, these jobs will be progressively done independently by software.

According to a study conducted by ING-Diba in 2015, the probability of the relevant job being eliminated is 89%.

[15] Figure 9: Distribution based on 2010 job mix. Source: Frey, C.B. and M.A. Osborne, "The Future of Employment: How Susceptible Are Jobs to Computerisation?", 17 September 2013

**Selected projections of job losses associated with digital technology**

| Country | Projected job loss | Time horizon | % today's workforce | Source |
|---|---|---|---|---|
| **Australia** | 5 million | 2020-2025 | 40% | Committee for Economic Development of Australia, 2015 |
| **United Kingdom** | 10 million | 2035 | 35% | Deloitte, Frey & Osborne, 2015 |
| **United Kingdom** | 15 million | Next few decades | – | Bank of England, Frey & Osborne |
| **United States** | – | A decade or two | 47% (based on 2010 data) | Frey & Osborne, 2013 |
| **United States** | 22.7 million | 2025 | – | Forrester |
| **United States** | 80 million | Next few decades | – | Bank of England, Frey & Osborne |
| **Global** | 2 billion | 2030 | – | Thomas Frey, Futurist |
| **Global** | ~1.25-1.5 billion | 2020-2025 | 40-50% | Gerd Leonhard, Futurist |

[16]

## - 3.1.1 Simple physical and manual work

Characterized by the use of physical strength, in the future will mostly performed by machines but never completely carried out by them.

Indeed, the proficient use of a robot or machine rather than a human employee is conceivable only if they can work independently and the job they are programmed for is repeated with certain regularity. Therefore, the critical and discriminating criterion remains the level of **routine**.

In addition, the minimum wages problem may be a reason to introduce robots and many firms' operations have already been planned in such a way that brings the organization to eliminate different jobs (usually in production) and have the work performed by machines.

Even low-labor-cost countries, such as China, are applying this kind of scheme, traditional factory employees are progressively being replaced by robots and are transferred to other available position within the company.

[16] Figure 10: World Economic Forum White Paper Digital Transformation of Industries: In collaboration with Accenture Societal Implications.

When the retraining of employees for a highly qualified job is impossible, because of their lack in competences and skills in digitalization, unfortunately their dismissal is often the final result.

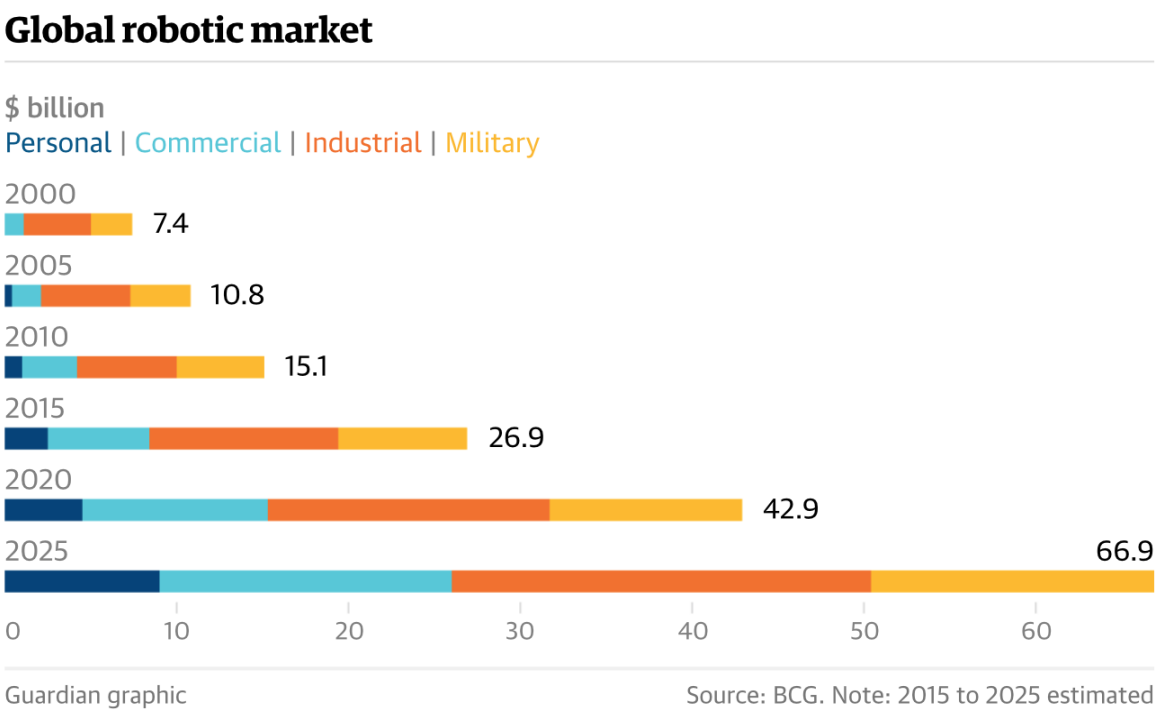
Naturally, labor law and rules vary from country to country, for example, China or US apply the rule of "hire and fire", according to which there is no particular reason for dismissal.

By contrast, there is usually a high level of protection for workers in Europe because both labor authorities and employee representative bodies must be consulted and informed in advance.

### - 3.1.2: Robots related issues

The advantages of robotization are persuasive but there is a flip side in bringing robots into your manufacturing process, there are some disadvantages that we should take into consideration.

- **The high initial investment:** Robots at the beginning usually require large investments in hardware and software, as well as the costs related to the install and workforce training.
- **Ongoing costs:** While robots reduce a part of labor costs, they introduce other kind of ongoing expenses, such as programming and maintenance because they are related to productivity in the long term.
- **Expertise is often scarce:** Industrial robots need particular and sophisticated programming methods, and also if the number of people with this kind of skills is growing, it is currently limited. Therefore, it is important to consider the personnel investments and expenses a firm will need to make regarding expertise and programmers.
- **Safety issues:** going towards the introduction of robots in the supply chain, workers will have to learn to work with them becoming an integrated system and not depending completely by them.




[17]

Unpredictable risks can appear at any time, some of them could involve the workers, others the final product. That is why is necessary to train employees to have confidence with robots.

Furthermore, employees need vigilance especially consequently to the put in motion of automatic procedures, that can have as result accidents at work because once started are difficult to stop.

Even if the procedure is readily interrupted, it cannot be excluded that all of the risks have been averted. Other not foreseeable events could happen if the autonomous system suddenly and uncontrollably interrupts its procedures. There have been cases in the US in which an employee suffered relevant injuries resulting in death because of the shut-off of the system.

- **Lack of safety standards**: Most accidents at work are caused by the lack of integration and coordination between robots and workers it is fundamental that each organization meets international safety standards.

  Many European companies follow the EU minimum standards requirements used also by other non-European countries that do not have particular codified rules.

[17] Figure 11: BCG analysis 2015

According to different and individual circumstances, policies should be adapted to the local site and the consultation or/and preventive examinations of experts is necessary, together with the check of supervisor and relevant officers.

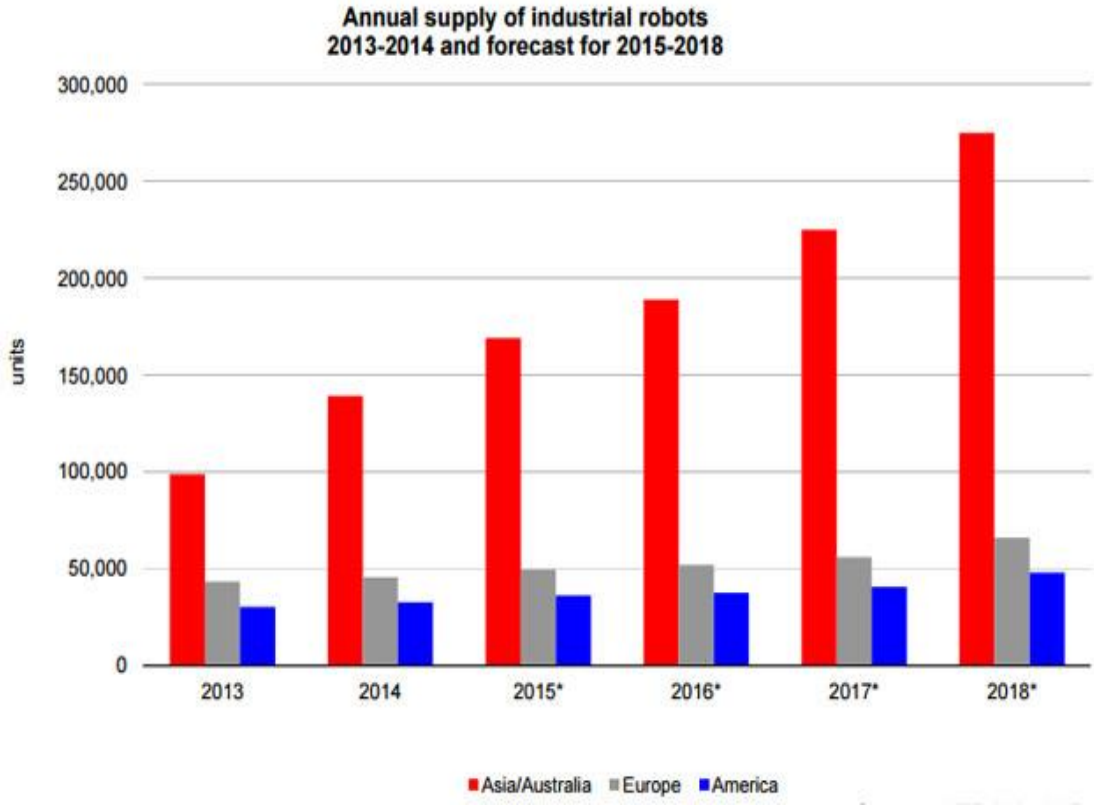
Penalties are usually the consequence for companies that violate safety rules also because the main cause of accidents is human negligence.

It will be necessary to weigh the pros and cons for each different scenario and situation, but for many companies, robots have a fundamental role to play in the entire value chain. Gerlind Wisskirchen, IBA GEI (International Bar Association and Global Employment Institute) Vice Chair for Multinationals says: "Certainly, technological revolution is not new, but in past times it has been gradual.

What is new about the present revolution is the alacrity with which change is occurring, and the broadness of impact being brought about by artificial intelligence and robotics. Jobs at all levels in society presently undertaken by humans are at risk of being reassigned to robots or AI, and the legislation once in place to protect the rights of human workers may be no longer fit for purpose, in some cases."[18]

- **Legal responsibility**: Increased mechanical autonomy will cause problems related to the definition of legal responsibility for accidents involving new advanced technologies such as driverless cars. Who will have to pay for the insurance? The owner, the passengers or manufacturers?

[18] **Gerlind Wisskirchen**, IBA GEI Vice Chair for Multinationals, IBA Global Employment Institute "Artificial Intelligence and Robotics and Their Impact on the Workplace", April 2017




[19]

If, as is the case, the industries but not only, the whole world of work, the tertiary sectors included will increasingly reduce the presence of workers, replacing them with robots, with artificial intelligence machines, it is to be asked that it will be "so many "(more and more) expelled from production activities and replaced by robots. In addition, what is it together, that it will be of state finances, how to support them? (For services, for welfare, to help growing unemployed ...?). If from one side the reduction of human labor forces could lead to a significant cut in production costs, on the other hand, it is leading to significant social and ethics consequences.

From here, according to Bill Gates, the celebrated US businessman, Microsoft founder and philanthropist, machine work should be taxed as that of human workers as he said to an online newspaper on February 17th. Gates thinks that if governments break up the work done by the machines, they would reduce the negative impact of the progressive replacement of human labor with that automated. Governments in the meantime could make investments to train

[19] Figure 12: IFR-International Federation of Robotics 2World Robotics 2015: Annual supply of industrial robots 2013-2014 and forecast 2015-2018

people left without work in areas where human contribution remains indispensable and there are never enough workers, such as older people's care and teaching.

The proposal by some has been seen as an inapplicable paradox, others have seen it as a positive provocation, and have been put in a way to realize it, at least in part.

But it is a consideration, a proposal (also coming from the authority of someone who has expressed) that has "hit the mark": work is drastically diminishing for all (young people in the first place) and the cause is not only the global economic crisis, but it is true that there is a progressive, dramatic and inevitable replacement of limbs and crafts for the increased productivity of animated robots of artificial intelligence.

The use of robots in the factories is increasingly widespread, replacing the work of the workers more and more. And this is happening all over the world: even in developing countries where so many productions have moved in these years, or have been set up to bring the country out of poverty (as in China).

Returning to the idea of taxing robots, they increase labor productivity but remove "human" labor and this idea is difficult to implement because it is complicated and difficult to define what a robot is and in what cases substitute a specific job. After all, all the tools applied to every activity have replaced work (we only think of agriculture in machines that have finally replaced the very hard work of farmers and animals used in the fields).

Many have expressed a negative opinion about the proposal to tax the robots, saying that what Gates proposes is in fact another business tax. Since taxing something means usually to get a reduction, taxing production would make it diminish causing damage to the economy.

We can affirm, that automation makes many people losing their job, but that at the same time allows to develop new highly qualified professions, new "worlds" that can be opened; and can give life to a new collective and positive effort to (re)put into effect the personal entrepreneurship of those who will remain unemployed.

Things may be true but, in this historical phase, the transformation of work and the expulsion of workers is so fast that it makes it very difficult to have an immediate "substitution" for other new activities. It is certain, unlike all previous revolutions, the new jobs created are far lower than those lost.

Among those who are in favor of taking precautions against the progressive automation of the industry is the socialist candidate at the upcoming French presidential election, Benoît Hamon, although his proposal is not exactly the same as Bill Gates.

Hamon proposes as solution to job losses a minimum citizens' income partly funded by a robot tax (Gates proposes to use the robot tax money to make investments to train people left without work in areas where the human contribution remains indispensable).

What is certain is that we need to reflect on a different distribution of incomes and opportunities among all men.

And then we need to give a definition of what a robot is if we want to tax it, if we talk about their future application to production systems. Because there are so many advanced technologies that reduce work, from lasers to sensors, to everything that makes life easier and perhaps we have to find and tax, something different, probably machines that in a pure and simple way do the work that many people did before.

In this logic, we must begin to establish (as the European Parliament has provided for a resolution) the ways and means of recognizing the legal status of robots: sophisticated autonomous robots should be considered as "electronic persons responsible for compensate any damage they make as well as the possible recognition of the electronic personality of robots who make autonomous decisions or who interact independently with third parties "(...)[20].

## 3.2: Winners and losers of the fourth industrial revolution

### - 3.2.1: Losers

For a long time, Brazil, Russia, India and China, the BRIC countries, were considered the future of the global economy.

However, actually, the demand for raw materials by is decreasing and these countries are becoming always less attractive. This route change is transforming the BRIC in the possible losers of this fourth industrial revolution.

[20] Part of a European Parliament Resolution proposed by the awareness raising campaign on this issue of the Member Luxembourgish Socialist Mady Delvaux, resolution adopted by a large majority on 16 February.

In fact, with the progressive and efficient development of machines and production robots, different organizations that outsourced their production in low labor-cost countries are relocating their plants to the countries where they originally came from.
Also, other developing countries as the ones of Central and South America or the North African ones will not profit from the advantages of this fourth industrial revolution because they are not ready and not equipped to face the process of digitalization. There is a strong lack of digital investments due to the absence of infrastructures, education of a part of the population and a not always clear legal framework.

### - 3.2.2: Winners

The possible winners of the development of Industry 4.0 are, on the other hand, the highly developed Asian countries characterized by excellent education systems, such as Hong Kong, Singapore, South Korea and Taiwan side by side with the Scandinavian countries.
These countries have been studying and working on the development of digital solutions for a long time creating in this way an increasingly advanced interconnection of systems and people.
Indeed, only the 6% of the population is exposed to the risk of unemployment.
India and China are probably the perfect candidates for participation to the digital transformation process due to the fact that their population have high competences in English and IT and because they are progressively becoming western oriented countries whose population is mainly working in the tertiary sector.
As they are the most populated countries in the world their consumer demand is really high, their cities are growing so fast that they need for sure new logistics and environmental technologies solutions to increase the quality of life of their citizens over the long term.
Furthermore, when the production through robots becomes cheaper than human production in low-labor-cost countries, the Western developed countries will have higher profits and revenues from the relocation of the companies' production.
This will progressively create new jobs in these countries and destroy many others routine jobs in the low-labor-cost countries.

Finally, we can certainly say that the digitalization progresses will be initially focused on Southeast Asia and Western developed countries and we can consider them the winners of this Industry 4.0 revolution because of their technology, creative and financial possibilities.

## - 3.3: Education

The evolution of Industry 4.0 is progressively changing the way the society perceives different kinds of jobs; new cross-functional roles are arising for which workers will need particular skills and knowledge in both IT and production.
Consequently, the fluctuating employment landscape has numerous implications for organizations, industrial companies, education programs, and governments.
How they can manage the changing conditions in an efficient way promoting at the same time productivity and competitiveness?

### - 3.3.1: What governments should do?

Governments are responsible not only for making education accessible to everyone on their competence area and help companies to hold as many workers as possible, but they must help improve coordination among different stakeholders in business organizations focusing young people's interests on technology and always more technical jobs.
To allow the maximization of the number of jobs created by the Digital Transformation and the options offered by the involved firms, the government effort will need to focus on promoting the efficient implementation of Industry 4.0, which is a prerequisite to generate economic growth and create new employment opportunities.
Government and academic leaders should work together with job agencies to help students understand that IT competences will be needed for all types of future employment, not only for Industry 4.0 jobs.
They should formulate an education system that is able to support the progressive requalification of the industrial workforce, recognizing the importance of training for employees at all levels.
Furthermore, Industry 4.0 accelerates the need for new types of leadership abilities and intensifies the competition for high-qualified jobs in several countries.

Unions and employee representatives are asking governments to create better educational programs and specific trainings for actual and future employees preparing them to be ready to face the evolution of job market. That is why governments and organizations should analyze the jobs categories that will become performed by robots or automated in the next few years and based on such analyses foster the improvement of education system.

The biggest challenge that employee representatives will have to face is to be able to integrate these low skilled employees in the advanced, modern labor market trying to move them to other workstations within the same company in order to keep their promise that no employee will be fired because of operational changing conditions.

Companies should work with governmental job agencies to prepare for the shifting job requirements of Industry 4.0, developing requirements and a set of specific competences for each role and design ways to evaluate individuals' skills to respond to them.

If governments and companies expect their workers to become more cultured and have important qualifications, it seems inevitable that they must also give the employees the opportunity to obtain them even outside the framework of internal advanced training.

Consequently, it will no longer be possible to conceive the world of employment without educational leave. The right to paid educational leave is established by law in some European countries and will become progressively imperative in the lifelong learning area.

### - 3.3.2: High schools and universities

To be able to meet the new high standards set by Industry 4.0 revolution, the educational system must be adapted to these new technology trends and quickly changing conditions.

Schools should encourage students' interest in subjects such as science, information technology and mathematics.

Teachers need to be formed with digital competences, they must teach students how to think in a different and critical way when using new technologies and help them to understand the real meaning and dangers of new digital and information devices.

For instance, there was an agreement at the World Economic Forum 2016, according to which both schools and universities "should not teach the world as it was, but as it will be".

Several current educational programs at all levels provide courses that offer limited interaction among fields. To foster cross-functional learning, universities should intensificate the number

of interdisciplinary study programs integrating IT and engineering with traditional courses, such as mathematics and physics.

Extended degree courses in the area of big data will be necessary together with the ones in cybersecurity and robotics. However, uniform education in this area is still not available.

They have to foster the development of soft skills that are becoming always more important and example of them are the ability to work in team, to improve communicative skills and reliability and accept critics.

At the same time, students should focus on building specific skills and capabilities to increase their employability and meeting companies' expectations.

Probably, the academic community should start develop interdisciplinary competences also for students who are still in high school, creating internationally recognized hybrid programs as superior approaches for students' professional future.

These competences could include for example access to free courses at "open" universities providing online-learning platforms.

Academic leaders should start to work with business leaders collaborating to create new business models for their organizations discussing their companies' specific training needs.

Universities together with industry associations, governments and companies should try to further integrate business elements with engineering skills including mandatory classes in digital literacy (that goes from basic theoretical knowledge of computers and communication devices to how to use them in a correct way) IT, programming, data science and coding.

### - 3.3.3: What companies should do?

The revolution of Industry 4.0 is creating something that will have several impacts on the nature of work and organizations, new kinds of interactions between people and machines.

Companies should start to consider changes in their production schedules, create new work and organization models in order to get fit with the continuously evolving conditions of the general economic environment that includes flexible schedules and the adaptation to new rhythms of work dictated by machines and robots.

"Mobile-assistance systems and smarter machines pave the way for a much-needed flexibility in work schedules. Production shifts can have different starting times for each worker. In the

future, machine operators might even work for different companies on different days of the week, thus enabling them to maintain full-time employment." [21]

Another issue that should be analyzed by firms is the need to rethink the decision-making authority. For example, some kinds of advanced robots, as robot coordinator could not need to wait for commands from a human supervisor.

The robot advent is changing the way an organization structure is composed and managed. With the digital transformation, firms, need a closer integration among the operational departments and the IT department one, in a way that allows software developers to fully understand if their solutions are efficiently used and if and/or how they could be improved to better adapt to the organization's needs.

Probably a flatter organization of work would allow the organization to control and gather data in a more efficient way increasing the information interchange.

As given the importance of data in Industry 4.0's, we can say that industrial data scientist will probably be the job function experiencing the highest growth of request together with the user interface designer and IT solution architects. As the use and development of robots becomes more diffused organizations will deserve to create the new role of "robot coordinator" that will handle the management and supervision of machines.

The regular advanced training of an organization's own employees, is certainly important from an entrepreneurial perspective, because the lack of education can cause a deep lack of motivation.

Moreover, the flow of knowledge can counteract the "social downgrading" of employee groups and companies are somehow forced to provide retraining to their employees because people are working longer and longer.

### - 3.3.3.1 Strategic workforce planning

Another aspect organizations should engage in is the "strategic workforce planning".

This is a process that should repeated annually and that starts with gathering information related to the organization workers and subsequently categorizing them into different job families.

[21] Stefan Gerlach, researcher at the "Fraunhofer Institute for Industrial Engineering IAO".

On the demand side, this quantitative modeling can be used to simulate recruitment requirements assuming as given the company's forecast rates related to Industry 4.0, productivity, revenue growth and development otherwise on the supply side, could be useful to obtain information and insights referred to employee retirements and problems.
The data gathered form supply and demand sides can then be combined together to produce a complete and detailed gap analysis. This analysis gives advices and useful insights regarding the necessary measures that the firm should adopt associated to employees' allocations or development, eventual insourcing or outsourcing and if it is necessary to build new recruiting goals.

### - 3.3.3.2: Recruiting evolution

With the progressively changing conditions of the job market and the evolution of organizations' structure and workstations, companies should start to adapt their recruiting methods to the digital revolution.
New approaches to recruiting should be developed; they should be more focused on soft skills and capabilities rather than on qualifications determined by degrees and certificates.
Recruiters should look beyond formalities to understand the real value of a candidate and comprehend if his/her skills are adequate for the future role because the task on which the future employee will have to work are usually far from his/her core education.
Because employees will be working on a greater variety of tasks unrelated to their core education, recruiters will often have to look beyond formal degrees to identify workers with the relevant skills for specific roles.
It is fundamental for companies to find not only recent graduates but also experienced workers from other companies that could bring new capabilities and tools for definite jobs.

### - 3.3.3.3: Retrain Current Employees

Additionally, organizations will necessary have to retrain their employees because they must be flexible, be able to learn, adapt quickly to changes and have access to new fundamental skills.

Structured training programs should be created to offer workers job related skills with courses taught in classes and with experience on-the-job, observing how older workers perform.
Essential will be also to offer online learning programs to give a flexible way of learning for the employees that do not have enough free time to follow detailed courses or are not able to plan their job schedule.
Training should not be only focused on one subject but should give a broader set of competences because employees will have to work on many different tasks and activities.
It will be fundamental to foster a positive perspective of change among employees; it will be essential to create a lifelong learning progress that enables them to adapt to new processes.
The augmented use of assistance systems means that the qualitative changes brought about by Industry 4.0 will likely be constructive for the workforce.

## - 3.4: Environmental changes

"The environmental impact of digital technology has grown rapidly; from increased consumption in terms of volume of content and number of people connected; as well as quantity of services. Businesses must think beyond the systems and infrastructure to address the environmental impact of this growth."[22]
Another consequence of digitization is the creation of possible environmental damages and two challenges in particular are under governments' attention; the increasing energy consumed by data centers and the growing quantity of e-waste produced.

## - 3.4.1. Energy consumption by data centers

The growth in size and number of data centers is resulting in new elevate environmental costs. Data centers are contributing through their high-energy consumption and usually inefficient cooling systems to the increase of worldwide emissions level. They are actually consuming between 1,5% and 2,0% of global electricity, this rate is growing at a 12% per year and their consumption is forecasted to increase to 140 billion kilowatt-hours per annum by 2020.

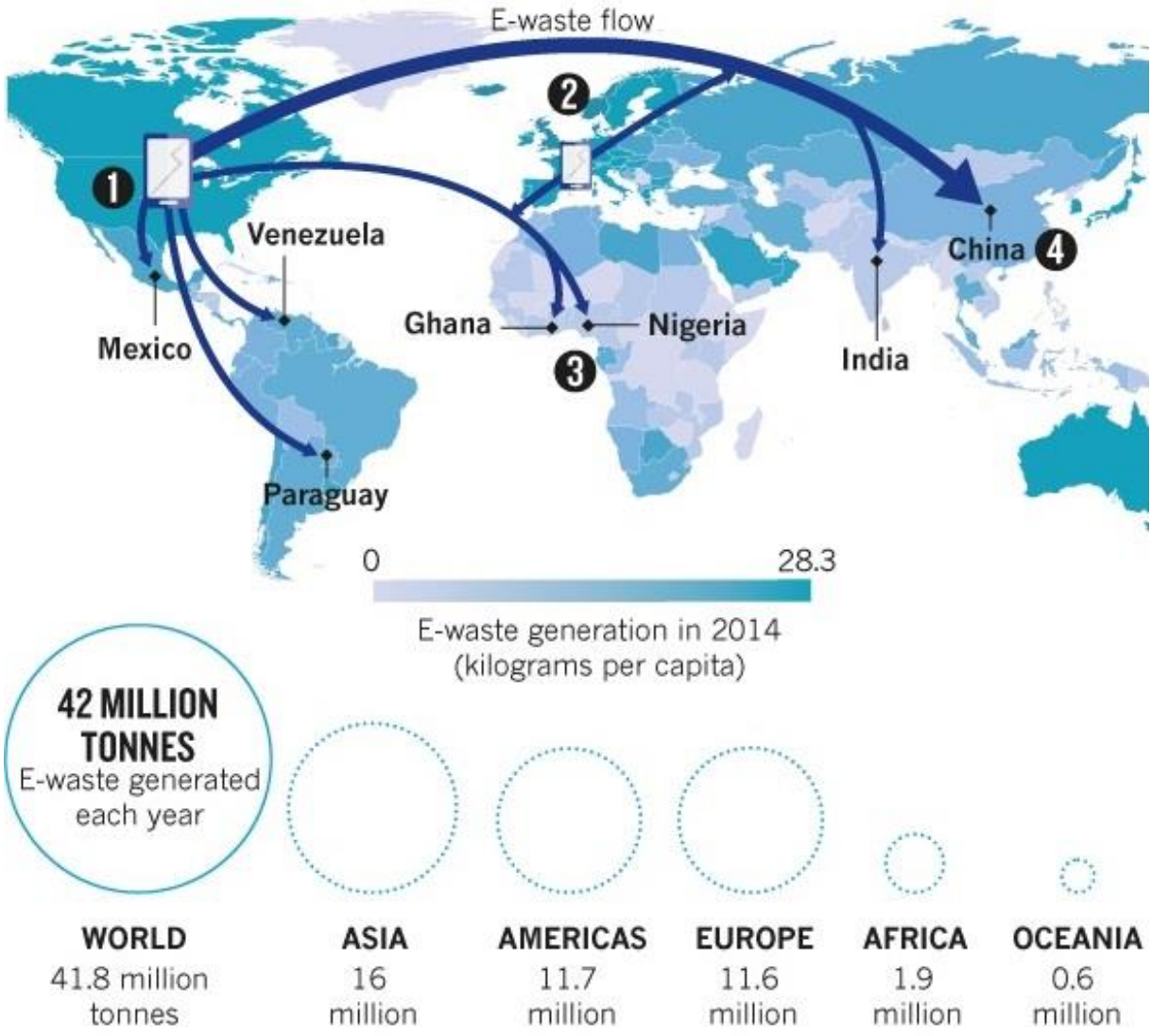
[22] Julia King, Vice-Chancellor, Aston University 2016

The high costs related to the sector are interesting data centers' companies to search for the causes and possible solutions to improve the current situation.
Unfortunately, the inefficiencies of data centers are caused by the necessity to satisfy the need of users that are always demanding more processing power and by the necessity of industries to avoid to fail and to lose customers.
That's the reason why a high number of organization are running their data center 24 hours a day for all the week at full capacity and they are installing supplementary banks of generators that are emitting diesel exhaust to be safe against possible power letdowns.

### - 3.4.2: E-waste

Electronics have always been source of waste, but recently the speed and the quantity of dispose has increased uncontrollably. With changes in technology and consumer demand, is nearly impossible that any device will persists for more than a couple of years in the hands of the original owner.
E-waste is continuously rising, according to a United Nations study, "40 million metric tons of e-waste was discarded in 2014, of which 7 million metric tons alone were from the United States and 6 million from China. The American Environmental Protection Agency estimates that only 29% of e-waste tonnage was recycled in the United States in 2012".
The biggest part of our e-waste is sent to developing countries, where recycle procedures are usually informal and not appropriately regulated. Rich nations are sending the biggest part of their waste to developing countries because they do not have strict legislation. China's system for example is poorly coordinated with just some regulations but other poorer countries such as Africa do not have laws on e-waste at all.
This results in the loss of potential value that can derive from recycling or reusing different devices, growing foothills of garbage and increasing volumes of toxic substances and chemicals being released into the environment.
The exposure to these fumes can lead to skin diseases, pneumonitis, breathing difficulties, eye irritations, convulsions and stomach disease. Therefore, the inadequate recycling of e-waste, usually carried out by poor and young workers in the underdeveloped economy, can cause significant health problems.

An International Labor Organization (ILO) survey found that India is one of the primary countries worldwide where recycling workers are exposed to the digestion and inhalation and of poisonous substances and approximately 1.5 million people each year, one sixth of all deaths in India, are result of environment pollution. As result of this elements and its poor water and air quality, India is the world leader for deaths attributed to asthma and breathing illness.




[23]

[23] Figure 13: Nature report "Take responsibility for electronic-waste disposal", 30 august 2016

A new global tactic line is immediately necessary to manage the amount and increasing flow of e-waste. An e-waste protocol together with a major awareness among consumers and customers and national import export legislations could be the answers to this problem.

The recycling system should be implemented and regulators should create a global e-waste flow system that can manage the entire life cycle of electrical products starting from production straight to the use, disposal, eventual recovery and remanufacturing of goods.

The ultimate and highest goal should be the creation of a circular economy, based on a cleaner and less polluting production that creates less environmental, health and society problems. Cloud based technologies could help to reach this goal together with the sharing economy.

If robots and machines will continue to replace firms' employees and human labor, it won't matter anymore how many final products and services will be commercialized because no one will be able to afford them.

## - 3.5: Digital transformation and cybersecurity

Another element companies and governments should take in consideration is the central issue of data security prevention and protection, known as cybersecurity.
The numerous raids by hackers within corporate and public networks have shown the fragility of the computer system.
Companies wishing to ride the digitalization wave will have to deal with the need to ensure the information security of their customers' personal data. This factor is more accentuated by the fact that customer data and information will be key elements for business companies.
Opening up systems to the data sharing can bring a number of risks associated to digital security and the protection of privacy, both to the infrastructure and the data itself.
The IT security market has experienced a surge in value over the last decade, reaching the estimated value for 2017 at around 120 billion, to exceed 200 billion in 2021.
As a result, startup and M & A operations designed to create synergies for data protection have reached interesting values, prompted by a casualty that is far from reassuring: in 2016, an

attack on three caused an actual security breach that translated means that on average a company has suffered two or three intrusions per month[24].

An example for all: the December 2016 attack on Yahoo that theft of over 1bln accounts.

Another thing to consider is the affirmation of the Internet of things, the connection of devices dedicated to the monitoring of personal information, and often of biometric nature; this leads to an exponential increase in the risk of personal data being stolen.

The issue is current and recently addressed at Community level through the adoption of Parliament's and Council Directive 2016/1148/EU of 6 July 2016 on measures for a high common level of security of the Union's networks and information systems CD NIS Directive.

The Directive requires Member States to work to strengthen cooperation between them in the interests of greater information exchange through the European Network and Information Security Agency (ENISA).

According to the Directive, Member States must have the technical and organizational skills necessary to prevent, detect, respond and mitigate the risks and incidents of networks and information systems. In this context, it is also important to monitor the incidents by identifying organizations that are willing to receive such news.

Significant impact is found in recital no. 49 where it is specified that digital service providers must ensure a level of security appropriate to the degree of risk, given the importance of their services for the operations of other undertakings within the Union. Member States will therefore have to make use of digital service providers to identify and take risk-proportionate organizational measures.

The NIS (Network Information System) Directive is not the only intervention at Community level in this area: Regulation (EU) 2016/679 already imposes a special obligation on the data controller in case of Data Breach.

In such a case, the data controller will report the breach to the competent supervisory authority and, where possible, within 72 hours from the moment when he becomes aware of it.

It can be said, therefore, that Cyber Security will no longer be a purely technical and almost "bureaucratic" aspect in the change of business organization but is intended to become a key aspect in business strategy. This will necessarily have a significant impact on the choices

[24] The State of Cybersecurity and Digital Trust 2016 Identifying Cybersecurity Gaps to Rethink State of the Art- Accenture 2016

regarding the professionalism to be entrusted to this segment and with the investments that will need to be addressed.

That is why the next chapter will be completely focused on this last topic that I will analyze in a deeper way.

# 4: Cybersecurity and Italy

As mentioned previously we can consider the cybersecurity one of the new challenges of Industry 4.0 framework.
In this final chapter I will analyze how this subject should be faced by organizations and how important it will be for the Italian scenery.
Traditional risk management models are based on a well-defined ecosystem. Internet and smart working, however, indicate that the boundaries of organizations are no more clearly identifiable.
That is why it is necessary to develop the correct capabilities within the business.
Industrial Revolution 4.0 and Exponential Growth of the Internet of Things (IoT), intangible infrastructures and interoperable organizational system are just some of the trends that are changing the operating and technological models of businesses as well as the cyber risks inherent in the continuous evolution of business ecosystems.
The huge number of devices, universal access and the large amount of data to be handled poses significant challenges on privacy, data protection and security issues.
These scenarios open up new areas of risk not to be underestimated, such as identity theft of information and other attacks from new computer threats.
Computer criminals are working on new ways to exploit organizations' vulnerabilities in order to access sensitive data and steal intellectual property.

## - 4.1: Cyber Risk, IoT and Supply Chain

Businesses can no longer worry about monitoring cyber risks only within their organization. The integration and interconnection of supply chains entails both new opportunities, such as real-time communications, greater efficiency and new synergies, as well as new risks.
Usually when firms think about safety, their goal is to safeguard their systems, digital assets and software against data breaches and cyber-attacks. But it is important to consider that also the supply chain, whether a simple manufacturer or service provider's supply chain or the "data supply chain" trusted on by most organizations, is susceptible to security jeopardies.

Supply chain security is a highly multifaceted, embryonic function, and needs more attention from the business executives as the risks they are facing and that are affecting supply chains are becoming progressively clear.

**Supply chain security is every company's responsibility.**

In terms of liability, regarding the handling of personal data of customers, it does not matter if these are compromised with a hosting or cloud storage provider: it is the company that having obtained those data from customers, must respond of a possible data breach.

The supply chain as a whole can be considered safe only if all actors involved in the supply chain operations are behaving in the right way, being careful of how they carry out harmonized and effective security measures to safeguard the integrity of data, goods, and of the general economic structure of the organization.

If a robot is hacked or undergoing technical damage, a production line may remain for hours or days, with potential costs of tens of millions of dollars a day. If an algorithm is incorrect or an IT system fails, global supply chains are interrupted and losses affect many other countries and sectors.

The set of analysis and evaluation practices for mitigating, accepting, transferring or eliminating risk options goes under the name of Risk Management. Risk management related assessments cannot be delegated: they are a key component of an organization's conduct; their approval is an inalienable responsibility of top management.

Cyber Security Risk Management is an application of risk management discipline within the cyber space. Since the three fundamental features of cyber risk (vulnerability, threats and harm) are often strongly related to other domains of risk, cyber security risk management, like other types of risk analysis and management, cannot and should be seen as a Discipline itself, but as one of the key components of the "Risk Management Entity".

In addition to interfacing with the foregoing elements, the single organization should implement the best technology practices typical of IT risk management such as: systems and networks for disaster recovery and business continuity systems, audit, system vulnerability testing and certification Security of their systems.

This ecosystem of measures that go seamlessly from the public to the private, in addition to protecting our national economic interests, it can be of crucial importance in legal disputes between businesses or international disputes between states, due to cyber attacks.

In fact, the relieving or aggravating of the position will depend on the "duty-of-care" or "negligence" that a state, a company or both will follow over time to minimize the risk.

According to the World Economic Forum, "Hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car would be a threat to a life."[25]
And we can connect this sentence to the self-driving trucks I talked about in the second chapter.
The Internet of Things (IoT) offers companies concrete and immediate opportunities to reduce costs, increase revenues and transform their business.
However, many companies hesitate to distribute IoT in their organizations due to security, privacy and compliance issues. One of the main concerns is the peculiarity of the IoT infrastructure, which unites the physical world and the computer world by adding the risks of both. IoT security is to ensure the integrity of code running on devices, authentication of users and devices, the clear definition of device ownership (as well as the data generated by those devices) and the resistance to physical and computer attacks.
Companies require transparency in the collection of data, type and reason for which data is collected, users accessing data and controlling access, and so on. Finally, there are general issues related to the safety of equipment and users who use them, as well as problems in compliance with industry standards.
According to Gartner: "The IoT redefines security by expanding the scope of responsibility to new platforms, services, and directions. In the future, organizations should consider re-modeling IT and cybersecurity strategies to incorporate the goals of digital business".[26]
**In 2020 according to Gartner we will have 13.5 billion connected devices and more than half of the new most important business processes will depend on the IOT.**
And it is known that these smart devices are in many cases unsafe and offer an excellent occasion to hackers.

[25] World Economic Forum, March 2015

[26] Gartner 2016

Many attacks of 2016, regarding IoT, have not even been declared and have involved devices such as printers, smart tv, videoconferencing cameras and a coffee machine. Many of these attacks have used IoT devices as a starting point for attacking more vulnerable areas of the supply chain network.

At the same time as they are adopting IoT technologies, businesses are pro-actively aware of the need to protect their business. More than 20 percent, according to Gartner, plans to provide by 2017 digital security services to protect business activities using IoT devices and services.

Given the characteristics of the devices, the introduction of IoT technologies represents a significant drop in security. IT department and the Chief Information Security Officer (CISO) will have to be on the forefront to handle more and more complex governance.

Compromised industrial or commercial IoT devices can be used to modify production plans, and industrial control systems. Operating technologies often control physical systems, and not just the bits and bytes of traditional IT networks, and even the minor disadvantage can have important, potentially devastating consequences.

IoT communication is integrated into critical infrastructures such as transport systems, refineries, waste water management systems, power generation plants, drinking water and communication networks make use of IoT devices.

The reality is that the IoT cannot be seen from the point of view of security as a separated and independent network, the waterfall effect is a potentially huge problem.

**"The Internet of Things will become the Internet of vulnerabilities"[27].**

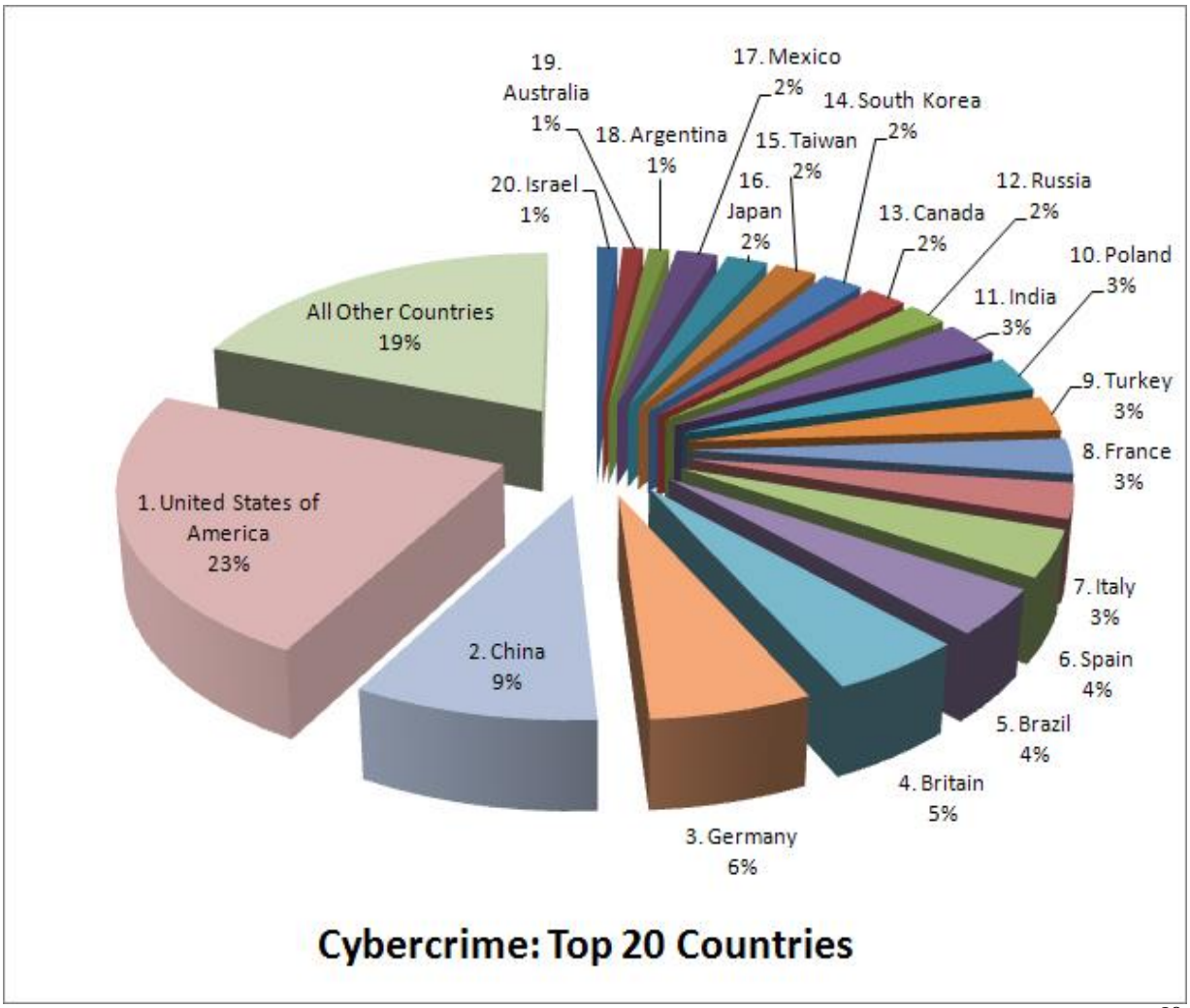
Cybercrime will be one of the factors that will affect companies over time, regardless of their size. Each company must take the road that takes it to more secure areas, punishing the disruption of activities and serious repercussions on operational capability.

## - 4.2: Cyber threats

The 2016 has been the worst year for cyber security, and among the world's most affected country there is Italy. For the first time, our country is in the top ten of the most serious attacks and the number of casualties. This is the evidence presented with the "**Clusit report 2017"**, the well-known association for Italian IT security.

[27] Gartner 2015

According to the "Clusit report 2017" last year, Cybercrime's serious attacks increased by 9.8%: only phishing attacks grew in the order of 1166%.




[28]

But which are the most dangerous cyber risks an organization should be aware?

## - 4.2.1: Malware

A malware is a software that, once executed on a computer system, can make any undesirable changes or damage to the system itself and its users. Malware can do the most diverse actions

[28] Figure 1: Top 20 Countries with the highest rate of Cybercrime BusinessWeek/Symantec 2015

on the victim system: they can subtract stored information and damage them or modify them in a weighted way, capture victim device screens by violating privacy of its users, stealing credentials of users who use the system, and more.

Not necessarily malware creates visible effects to the user; indeed, malware is normally programmed to not be detected and do not cause immediate user problems, just to be able to persist for long time on devices and to reach its ends as fully as possible.

Many malwares are designed to hit many people as possible but this is not always necessarily true: in some cases, a malware can be specifically designed for a victim and be the attacker targeted.

Malware uses a variety of methods to enter systems: they can be hidden in an e-mail attachment (Pdf documents, executable files, Microsoft Office documents, etc.) into a file contained in a pen drive USB, on web pages that can be visited while browsing from a browser, and more. Unfortunately, new malware more and more complex are born every day, and there are no immune devices: all the systems operated, all types of devices can be affected by this serious threat.

Using anti-malware software is necessary to protect devices from known attacks (which are the most significant part of the threats). The installation of such software is strongly recommended on all devices that allow it. To also protect devices for which anti-malware software is unavailable, it is recommended to use secure security solutions (software for checking and filtering of emails, web-firewalls, etc.

To cope with the constant emergence of new threats, such software needs to be kept constantly updated. The periodic update is the only tool that allows to detect and block new malware. Although the use of anti-malware software is necessary, it is important to point out that they cannot offer total protection, especially with regard to targeted threats.

Therefore, it is essential that all staff are properly trained to maintain, using them IT tools, a behavior that does not expose the company to easily avoided risks.

### - 4.2.2: Ransomware

Ransomware is a specific type of malware whose purpose is to prevent the victim access and use of documents and devices. The attacker then crushes the victim by asking for one "Redemption" for the release of inaccessible resources.

2016 was the last year he saw the utmost spread of this kind of attacks that have impressed their incredible numbers extensors the major cybersecurity research centers expect 2017 to see a further growth of this phenomenon, with more complex attacks aimed at extorting more and more quantities of money.

Fortunately, the malware is typically designed to hit the bigger number possible victims, anti-malware software is readily updated by manufacturers, so to recognize even the latest known variants in a timely manner. From this point of view the software anti-malware are, today, a useful barrier to stem this phenomenon.

The installation and configuration of devices and systems is a typically complex activity that requires specific skills and has important safety implications. For these reasons, should not be improvised, but rather delegated to staff internal or external consultants to ensure their proper execution. It could be led to think that the default configurations of systems acquired by third parties offer an adequate level of protection and therefore should not necessarily be subject to review and of any adjustments.

Unfortunately, this is rarely true, indeed, for many devices, information criticisms of "factory configuration" are publicly available and are on a regular basis object of study by cyber-criminals.

In principle, all factory default (default) devices on the devices should be modified non-nominal accounts should be replaced by nominal accounts or alternatively assigned to a single responsible person. The unnecessary default utilities should be disabled. For devices that allow such functionality (typically personal computers), it must automatic startup of software loaded onto external media is disabled.

Where credible it is threatening unauthorized physical access to systems (theft of a smartphone or a personal one corporate computer) it is advisable, in addition to protecting with a robust password access, enable it secure encryption of mass storage (hard drive or flash drive).

In order to ensure the availability of all the data, configurations and critical information for the Proper functioning of the company must also have an appropriate backup strategy that allows rapid and effective restoration in the event of an accident.

Backups must be done with one periodic cadence, defined on the basis of the specific requirements of the data to be safeguarded allow to go back to several copies of the data at different times, and must be saved in different systems, which allow proper preservation.

In particular, it is suggested to define at least two destinations, a local and a remote (off-site backup), so that the right one is guaranteed, preserve at least one of the two copies even in case of disastrous events. The remote destination, where the regulations allow it and the option is economically advantageous, it can be expected a cloud service provider.

In this case, the data under the procedure should be protocols through encryption to prevent a system compromise from the provider itself directly jeopardizing the confidentiality of company information.

The backup process must be automated through appropriate tools available on the market and past backups must be periodically verified in order to ensure that their content can actually be used in case of an accident, for any restoration.

This is the case of the recent ransomware named WannaCry that affected more than 100 different nations. More than two hundred thousand computers were hit on May 16 in at least 99 countries, making it one of the largest computer-related infections ever.

Ransomware is spread through fake email, and after it is installed on a computer, it starts infecting other systems on the same network and those vulnerable to the Internet, which are infected without any user intervention.

When infecting a computer, WannaCry encrypts files by blocking access and adds the .WCRY extension; Also prevents the system from restarting. At that point, a file called @ Please_Read_Me @ has a redemption request initially of $ 300 but then raised to $ 600, which the user has to pay in bitcoin to get the files unlocked.

[29]

The attack was greatly slowed when a 22-year-old British researcher found that before infecting a computer, WannaCry tried to contact a web address that was not registered at that time. The investigator assumed this was a kill switch, a mechanism inserted in the virus code by its creators if they wanted to block it. After registering that domain, a rapid decrease in virus infections was noted. There is, however, the fear that a new version of the virus, lacking the kill switch, may be widespread and used for a new attack.

### - 4.2.3: Phishing

Phishing is nothing more than a fraud attempt put into practice through the Internet, which has as its sole purpose the burden of sensitive and delicate information such as username, password, access codes, current account numbers or credit card data (it comes from the English term "fishing" which, refers literally "to fish" data).

To implement this attempt of fraud, malicious people using phishing techniques do not use viruses, spyware, malware, or other types of malicious software, but rather use social

[29] Figure 2 - WannaCry effect reflecting on pcs screens

engineering techniques through which they come study and analyze the habits of people, that are potential victims, in order to capture possible useful information.
The preferred technique for ending a phishing attack is to send normal emails in the form of spam messages with features very similar to those found on authoritative and particularly popular websites such as banking institutions, postal institutions, and online payment services. In addition to this particularly widespread technique, there are several others that are less frequent but still effective, such as spear phishing, sending smarter SMS messages (such a technique is called smishing jargon), or maybe even simple phone calls.

### - 4.2.4: Botnet

A botnet (a "robotic network" contraction) is a network of maliciously-infected computers that is under the direct control of a single attack author, known as a "bot manager". Individual computers under the control of the hacker are called bots.
The attack author is able to control every computer in the botnet from a central point to simultaneously perform coordinated criminal action. The size of a botnet (many of which are made up of millions of bots) allow attackers to perform large-scale actions that could not be done with malware before. Because botnets remain under the control of a remote attacker, infected computers can receive updates and change their behavior quickly. As a result, it is not uncommon for bot managers to be able to allow black market operators to access, with a remuneration, to segments of their botnets in order to obtain financial compensation.
Since this is one of the most advanced types of modern malware, botnets are one of the major security concerns for governments, businesses, and individuals.
While the elder generation of malware consisted of independent agents that were just infecting computers and replicating, botnets are network-coordinated applications that leverage networks to gain control and endurance. Because infected computers are under the direct control of a remote bot manager, being infected by a botnet is like hacking directly into your network, unlike a simple malicious executable program.

## - 4.2.5: Distributed denial of service (DDoS)

A Denial of Service (DOS) attack is an attack aimed at halting a computer, a network, or even a particular service offered or to completely disable the server or even an entire network.

A Distributed Denial Service (DDoS) attack is a variant of DoS and uses tens of thousands of infected computers, which form a botnet, to complete the attack. The large number of infected machines, involuntarily controlled by the Command and Control center, generate requests to the target and in a short time make it unavailable saturating all its resources.

DDoS attacks are much more insidious to lock because:

- The power of the attack (volume of data transmitted, busy band, etc.) is greater of many orders of magnitude than the one that is possible through a DoS;
- It is practically impossible to block the attacker's view that tens of thousands of infected computers are perpetrating the attack if they do not subscribe to a mitigation service;
- It's pretty much impossible to recognize authorized traffic from unauthorized traffic, as the computers participating in the botnet are located virtually all over the globe.

## - 4.3: How to protect the business from these risks?

Protecting an organization is a challenging mission itself, without even thinking about all the risks and vulnerabilities that affect the supply chain. Nevertheless, it is important nowadays also to evaluate what happens outside the corporate walls.

How to prepare to manage third parties correctly? What are the steps to take into consideration?

The National Cyber Security Framework, published at the beginning of 2016, may be the tool used by large organizations to define minimum "standard" security requirements to be applied to their supply chain. This will boost overall cyber security throughout the supplier's Italian ecosystem (consisting mostly of a large number of small and medium-sized companies).

In the report "Combating Cyber Risks in the Supply Chain" (SANS Institute, September 2015) is said that one of the most important thing to do is to define the most critical vendors, those that could lead to the worst consequences in case of data breach or malfunction.

In recent years, many of the highest-profile data breaches, involving millions of dollars in losses to the organizations involved, have seen a source in the supply chain.

An organization ready to deal with computer attacks takes a completely different mental approach, looks ahead and prevents problems by responding in a way that computer criminals would not expect. No organization or government can predict or prevent all (or even most) attacks; But they can decrease their target attractiveness, increase their resilience and limit injury from any attack.

A state of readiness embraces:

1. Designing and instigating a cyber threat intelligence plan to sustain strategic business decisions and leverage the value of security;
2. Defining and extending the organizations' cybersecurity ecosystem, involving partners, sellers, amenities and business networks;
3. Taking a cyber economic tactic understanding which are the core resources and their value and investing precisely in their defense and fortification;
4. Using "forensic data analytics" and "cyber threat intelligence" to examine and antedate where possible threats are coming from and when, increasing the readiness;
5. Guaranteeing that everybody in the organization comprehends the necessity for durable governance, user panels and accountability.

Firms may not be able to predict when information security incidents arise, but they can control how they reply to them intensifying detection competences and capabilities. A well-functioning **security operations center** (SOC) can represent a good strategy to create a strategy of effective detection.

The emphasis of the SOC must be the management of cyber threats according to business priorities. The SOC can have an important role in enabling a more efficient decision making processes producing related reporting and risk management and business endurance allowing the information security department to respond faster.

The level of readiness of firms in contrasting cyber threats cannot fail from their unexpected discovery. In this regard, the Global Information Security Survey shows that 44% of the globally questioned companies do not have a SOC and that only 28% of relevant IT incidents have been stopped by the SOC. This settles the strong need of the evolution of the procedures

used by organizations and the enhancing of their capabilities that are still not sufficiently disseminated. An increasing diffusion and development of the Security Operations Center can be the right key to detect threats in real time and diminish response time to security-related functions, enhancing collaboration and sharing knowledge within and among organizations.[30]

### - 4.3.1: How to handle suppliers?

In an increasingly global and interconnected world, several business processes are nowadays shared by companies with their own supply chain, made by third parties such as product providers, service providers, and distributors.

In this context, the launch of new products, mergers, acquisitions, market expansion and the introduction of new technologies inevitably complicate the definition of the perimeter to be protected and require a company's cybersecurity dynamic and predictive approach, with a strong adaptation capability to change.

For their own survival, companies rely on these players by purchasing essential products (such as raw materials and semi-processed) or essential services for the same operational continuity (network services, cloud storage and software-as-a-service).

Today's increasingly dependence on the own supply chain requires companies to consider the associated back-up, the possibility that an error or a malfunction with third parties has serious repercussions on their business.

More and more integrated supply chains simplify cooperation among the different actors involved, but at the same time offer larger opportunities for cyber-criminals to infiltrate and commit their abuses. The vulnerabilities generated by the supply chain are many: in some cases, vendors have credentials to access networks, data and business applications, and therefore potentially have the potential to spread malware or commit infiltrations.

Other possibilities are represented by cases: a software vendor might have suffered a cyber-attack, the product code he could contain could therefore contain malware that would then be distributed to all customers.

Vendor credentials could have been subtracted and reused by a hacker.

Then it is important to define the role of the Vendor Owner, a figure in the organization responsible for the management and reporting of many aspects, including any legal issues, audits, review procedures, and documentation provided by the vendor. He/she also handles all

[30] Global Information Security Survey, 2014

the contracts and defines all the appropriate security assessment questionnaire for critical suppliers.

That is why organizations should take into consideration the idea of adding important information of vendors to easily identify sensible data and possible attacks and emerging threats.

The first thing businesses should do is to ensure that all the supply chain suppliers have codified, validated and certified security guidelines and measures. Validation and certification can be confirmed through legal documentations like HIPAA Business Associate Agreements or accredited auditor reports like a PCI Audit.

Different actors may compromise the less defended vendor network and this can have repercussions on the parent firm. Obviously, the awareness of these situations allows the parent company to put in place countermeasures before the involved vendor has the chance to enter completely into the network.

Fundamental is to define guidelines, rules and periodic controls to implement the security, establish data handling requirements, timelines and parameters, require product integrity and assimilating all these activities with existing business processes. Vendors, sub-contractors, and critical partners must meet or those standards as terms and conditions of recognized business agreements.

Furthermore, the rationality and reliability of security procedures can be proved through third-party or in-house testing of systems and procedures and contracts between firms and their relevant suppliers should clearly define rights, duties and use strategies necessary to allocate in the correct way the responsibility in case of breach. These agreements should also necessitate supply chains managers to notify as soon as possible partners or vendors of breaches in order to avoid additional incursion or hacking of business data.

Moreover, security can be further enhanced through the launch of a scheme of restricted network access for related sellers. Indeed, access should be as limited as much as possible and supply chain vendors or partners should be monitored and checked to guarantee the entire network safety. Therefore, all the involved stakeholders are requested to respect and establish the most appropriate mechanisms of access, security, monitoring, examining and supervision considering the fact that all these measures need to be continuously implemented and analyzed to individuate the necessary changes.

But safety measures shouldn't just be applied to third parties, the internal security is important as well.

The company has the obligation to apply standard IT solutions such as firewall, anti-spyware and antivirus. But that's not enough, the firm should go further than that adopting advanced IT technologies like network access control, business continuity solutions, bake-up systems and all the possible assets that could guarantee the structure safety.

Organizations' employees must also respect and apply the established rules for a proactive and self-protective strategy.

Sector studies also found that most of the attacks on computer systems are caused by a human factor component, whether it is conscious or unconscious.

In both cases, however, it is crucial to successfully complete an attack. Even a seemingly marginal subject within an organization but not equipped with adequate security guards can be used as a basis for bringing attacks to the heart of the organization itself. Once the attack is triggered, a dangerous domino effect can start to affect affiliated organizations even though they have advanced defenses.

Technology and capabilities should be evaluated with Security Assessments, Source code and binary validation. Necessary is also an IP Protection to determine if the firm's Intellectual Property has direct access by any third-party and the Information Sharing, if there is a threat information that can protect many companies, share it.

**That is why cybersecurity requires commitment and collaboration.**

## - 4.4: Cyber resilience

A possible solution to contain the risk of attacks is the so-called Cyber Resilience, which is the continuous examination of resistance to possible threats and the time needed in trying to recover the original status prior to the event or adapting to the new condition trying to find efficient alternatives of carrying on the business.

It is therefore essential for businesses to define a pathway towards **Cyber Resilience** by developing the following capabilities:

- Through "Threat Intelligence" tools companies should try to forecast and detect cyber threats, with particular procedures and measures that should has a goal the unremitting monitoring for an efficient defense, such as the Security Operations Center (SOC);

- Understand which are the risks and the entity of them they are willing to accept and which should be mitigate;
- Create e strong and centralized framework ready to face possible crisis, crashes, cyber breaks that answers in the most quick and efficient way to problems facilitating inquiries for eventual violations.

Obviously, none and no system could guarantee the perfect functioning of the entire structure and that there will never be a problem of cybersecurity like a breach. Some kind of failure will certainly occur at some point but with the right measures and vigilance, the risk could be mitigated. According to this statement, the system resilience goes to define how quickly the system can restore the correct status of operations eliminating the problem.
In conclusion, a Resilient Cyber Company needs to develop a flexible, proactive and agile mentality that can adopt a shared strategic address to tackle cyber-crime, design and implement an effective cyber threat intelligence strategy;
define and understand cyber security boundaries including partners, suppliers and businesses that are part of a firm ecosystem;
understand what assets are vital and invest in protecting them through an integrated risk assessment that involves the business and not just technologies;
use survey tools and cyber intelligence to analyze and anticipate future threats to ensure that the whole organization understands the need for strong and structured governance.

## - 4.5: Changing insurance conditions

At the same time, new technologies can bring problems of civil responsibility. For example, in the event of damage, compensation claims may be filed against maintenance software developers and vendors. How can the growing computer risks in the industrial sector be effectively prevented and reduced?

With respect to Corporate Responsibility and Third Party Responsibilities, compliance requirements are already in place for aspects such as vendor due diligence, supply chain risk management or purchase contract requirements. The theme is how to extend these activities taking into account the potential cyber risk.

The need for an integrated risk management process and the role of insurance underlines the need for firms to be responsive and alerted. To cope with these threats, Companies must structure an integrated Risk Management process, that includes the Cyber scope. This approach guarantees the most effective method for preventing and mitigating the impact of computer risk by developing adequate awareness, together with the optimization of the risk transfer process to the insurance market. The insurance coverage of these risks is, in fact, the last step in a structured process, that starts with the analysis of the specific reality of the company: from the type of business it conducts to the kind of activity it implements to the features of the infrastructure IT.

The Cyber Policies on the Italian market today are few and varied among them: by language, structure and scope.

Typically, we will find ourselves in front of a number of sections that can be activated or not, which will take into account: damage to ICT (machines) assets and proprietary data or third parties; damages related to the violation of privacy (personal and/or commercial data) of your own or of third parties; damages caused by computer crime and those from a fault and human error and damages affecting business activity.

Ordering a set of costs associated with these damages is not always provided by traditional policies.

Once comprehended what is cyber risk and that it can be analyzed, mitigated and ultimately transferred, and defined the possibility of covering damages and costs, it may be useful to better understand and decide if we may need a cyber policy and what features this must have to protect a business.

Cyber-insurance can of course not prevent the computer attack from happening, but it can help the accident victim to endure the resulting damages, particularly the costs associated with the damage caused to third parties, for which the company is responsible: it can be, for example, legal costs, costs to notify consumers about data breaches that led to the release of private information, costs for restoring the pre-attack situation or for providing services, credit tracking, public relations costs, and advertising campaigns to rebuild the reputation of the company.

Some policies may also cover the responsibility of corporate administrators and managers or the discontinuation of assets resulting from an attack that may reduce revenue, as well as losses suffered by so-called "ransomware" (increasing) or the systems blackout of a company if the sum of money is not paid.

In the future, digitization will shift the nature of business assets to a domain that will become more immaterial by the physical. Reputation and brand value, but also intellectual property, technology know-how and supply chain networks will become increasingly important assets. Bruch adds: "A factory's insurance coverage will always require more business-related indemnity damages due to immaterial, information and reputation damages, to protect intangible assets adequately. Perfecting and developing new and existing services is essential for both insurers and companies, to prepare together with the next industrial revolution".[31]

In order to reduce the risks of the supply chain, insurance must be more than just a policy: it includes a range of services including risk analysis, benchmarking, and consulting that help to analyze quality and flexibility.

## - 4.6: Italian position in facing the cybersecurity risk

In recent times, public opinion has been exposed to numerous cases of cyber-attacks even with some important effects. In some cases, they were attacks by government-related actors, in other cases it was the use of the cyber dimension for activities and mixed attacks (terrorism, espionage operations, military operations). Even small and medium businesses are beginning to understand that there is a problem that might involve them, but not always understanding that the consequences could be disastrous.

## - 4.6.1: Italian Cybersecurity Framework

The level of awareness has increased accordingly and Italy begin to wonder what its level of preparation is. This process of growing consciousness, still extremely acute in our country, must necessarily be supported by methodological tools.

[31] Michael Bruch, Head of Emerging Trends, AGCS Alliance Global Corporate and Sociality

These tools must be simple, suitable for any type of user, providing a roadmap to achieve a minimum level of preparation in protecting your own information and/or reputation and your business. The National Framework is born precisely in this regard.
Finally, it is critical to note that the cyber threat requires a primarily coordinated public and private response. None of the two actors can respond to this threat individually, as the private cannot control threats that can come from anywhere in the world and the public needs the private as many essential services are now managed/provided by the latter and an attack could lead to with direct consequences for citizens.

As noted in the White Paper on "The Future of Cyber Security in Italy" published in November 2015, and followed by the "2016 Italian Cybersecurity Report Controlli Essenziali di Cybersecurity" the **National Cyber Security Framework**, is one of the key elements to increase domestic resilience of systems and networks against this threat.
It is necessary to identify gaps in the management of the cyber security of an organization, both in the public and private sectors, and in defining a risk management path that will continue to change the threat and technology.
Adopting a Framework is therefore a key step in improving its reputation and encouraging international investment in our country.

### - 4.6.1.1: Benefits

The benefits of a cybersecurity framework for the Italian landscape: SMEs, Large Enterprises and Industry Regulators can be summarized as:

- Small-Medium Enterprises.

The Italian landscape is mostly made up of small and medium-sized businesses, (at least 136.114) most of which have never faced the problem of IT security. This is mainly due to the man-made cyber risk assessment: small businesses are sometimes convinced that they do not have the information they need to protect, otherwise they are not aware of the innumerable means the modern hacker can put in act.
The main problem of small businesses, when they look at the world of security, are the costs. They cannot, independently assess what are the "quick-win" practices, that is to say, those with the least amount of effort guaranteeing a level-of-stage protection.

Consequently, these companies run the risk of improperly estimating the cost of putting their assets in safety, with the result that often the idea of increasing their security is put aside, running enormous risks, of which they are not aware.

The Framework provides a series of security lawns that, especially for SMEs, are both basic and economic at the same time.

These practices have been called "high priority practices" and correspond to that set of operations that allow a firm to bring level of awareness, protection and therefore security at a basic value, sufficient for most Italian SMEs.

- Large Enterprises

The National Framework does not have the claim to drive Large Enterprises and replace the complex risk management of these. It can, however, be very useful in copying, through a unified methodology, business risk management processes and programs, in order to make them evolve in a coherent and structured way.

In addition, Large Enterprises can benefit from the presence of the Framework in two key aspects: the internationality of this and the ability to require security profiles to its contractors. The Framework, being based on the NIST (National Institute of Standards and Technology), preserves the full compatibility of security profiles and therefore inherits internationality.

As a result, it can facilitate the communication of security levels as well as known standards (such as those issued by the ISO International Organization for Standardization), but in an extremely cheaper way. From a Contractor's point of view, Large Enterprise and Critical Infrastructures can use the Framework to require certain levels of security for all or some of the actors that make up their supply chain, or only to those who will have to interact with certain resources.

This mechanism allows to increase the safety of the whole ecosystem of the enterprise and to minimize the vulnerable surface of the attack.

- Sector regulators

As far as sector regulators are concerned, the National Framework provides a unique interface to work on consistently with both regulating companies and other regulators. The Framework can be used as a tool for defining standards in a structured and compatible manner with other regulators. It allows to verify the existence of specific national, European and international disciplines, general and domain disciplines, avoiding imposing additional burdens and supporting the dialogue between regulated and regulated entities.

Industry standards, as well as all other standards, remain in force after their release for extremely long times when compared to the evolution of cyber threats. It is therefore important to institute review processes especially for areas where security management is particularly critical (banking, public administration, etc.).
The Framework can be used for a preliminary revision of the regulations at first, and then it is possible to follow the evolution of the Framework itself to update its practices and regulations. Establishing a mapping between its sectoral rules and framework practices rap-presents a very useful exercise to highlight any shortcomings that inevitably extend the attack territory for companies in the industry.[32]

This is one of the first documents, that, in addition to addressing the essential security methodologies, considers the costs. Small and micro businesses are the heart of the nation, creating the bulk of our wealth. These companies are also an integral part of the national cyberspace, and are therefore part of the country's attack surface. Increasing the level of cyber defense of the country means, therefore, making cyberspace more secure, as the latter is increasingly a clear factor in the country's economic competitiveness.

The state should therefore facilitate the adoption of essential cyber security controls by companies based on production chains, through appropriate support and incentive policies.

A policy, for example, of tax relief for those who have decided to protect themselves and invest in their own protection. This would be an effective aid for the entire Italian economy and for national security.[33]

## - 4.6.2: Industry plan 4.0 – Piano Calenda

"The success of Industry Plan 4.0 will depend on the extent to which each individual entrepreneur will use the measures made available." With this statement, the Minister for

[32] CINI Italian Cybersecurity Report- un framework nazionale per la cyberscurity, 2015 Roberto Baldoni, Luca Montanari

[33] 2016 Italian Cybersecurity Report-Controlli Essenziali di Cybersecurity, Sapienza Università di Roma Laboratorio Nazionale CINI di Cybersecurity, Consorzio Interuniversitario Nazionale per l'Informatica; Versione 1.0, March 2017.

Economic Development, Carlo Calenda, announces the online guidance that provides a direction on all the benefits for companies falling within the National Industry Plan 4.0.

In the document are presented all the measures that each company can activate automatically and without any dimensional, sectoral or territorial constraints to promote innovation and competitiveness with hyper and super depreciation, R&D tax credit, startup measures and Innovative SME.

The industry 4.0 goal must be to combine cybersecurity with the concept of cyber-resilience. Cybercrime works with technologies and evolves often by playing in advance: companies know that it is impossible to guarantee total security. Protecting data, machines, programs, products, people must be part of an expanded strategy, where convergent monitoring sensors, video surveillance systems, tele control, intrusion, anti-burglary converge, but also protection from all sorts of cybercrime strikes users in the company or in mobility, at home, like by car, train or foot.

No matter with security, lawyers and certification bodies, the Privacy Guardian and the responsible authorities, the HR and the facility management personnel are involved.

It is necessary to work in a three-phase mode, implementing a strategy that can reason before, during and after an attack. Cybersecurity means designing predictive and reactive systems that, on one hand, are able to anticipate threats and, on the other hand, are able to implement timely and effective intervention plans.[34]

In the report presented on September 2016 on the major factors affecting the dynamics of public debt, the government estimates that the mix of super/hype amortization and "bonus" research can push investments by 0.9% per annum on average between 2017 and 2019.

With regard of super-amortization, the allowance consists of an increase of 140% of the cost of acquiring new instrumental material assets for the purpose of determining amortization and rental rates: companies may benefit until December 31, 2017.

The hyper-amortization, also available by December 31, 2017, provides a 250% increase in the depreciable tax cost of specific new high tech material assets.

[34] Baskerville R., Spagnoletti P., J. Kim: "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response, Information and Management", Vol. 51; 2014;

Among the easy-to-use goods:

- goods whose operation is controlled by computerized and/or managed systems through appropriate sensors and actuation;
- quality assurance and sustainability systems;
- man-machine interaction devices and improved ergonomics and workplace safety in logic 4.0.

As far as hyper and super-amortization is concerned, the Guide of the MISE (Ministero dello Sviluppo Economico) also provides useful FAQs, which explains that if a digital asset falling within the definition of "Industry4.0" is purchased at a unit price including the software required for its operation, all the consideration to be eligible for the 150% tax increase.

It should also be noted that an instrumental tool, including those that can be facilitated with the hyper-amortization according to the annex contained in the budget law, cannot benefit from an increase of 150% if delivered in 2016 as the subsidized period only takes effect from 2017. But can benefit from the "old" 40% increase, or the over-amortization that was already in place last year. The same is true even if the digital instrumental device, purchased in 2016, comes into operation and is interconnected in 2017.

The MISE also recalls the applicability of hyper-amortization to professionals as well, "regulatory elements suggest that the 150% increase applies only to business owners".

As far as software is concerned, the MISE clarifies that it is possible to benefit from a 140% increase only provided that the enterprise benefits at the same time of 250% depreciation, irrespective of whether or not the intangible asset is specifically linked or to the material benefit.

Lastly, it is confirmed that, for the purposes of hyper-amortization, an asset must have two requirements: exchange information with internal systems (for example other plant machines) or external (customers, suppliers, etc.) and be recognizable in a unique way through an Ip address. The sworn certificate on interconnection, required for equipment worth more than 500,000 euros, must be made for a single asset acquired.

Both the hyper and the super-amortization, are cumulative with the old and new industrial policy elements such as "bonus" research, patent box, New Sabatini, Ace, startup incentives, Guarantee Fund.

As regards Sabatini-ter, provides the granting of a contribution to SMEs to partially cover interest on five-year banking loans for the purchase of machinery, plant and equipment and is valid until December 31, 2018.

ACE encourages self-financing by making it fiscally equivalent to financial debt and risk capital. The Guarantee Fund, is useful to "support businesses and professionals who have difficulty accessing bank credit because they do not have sufficient guarantees". It consists of providing a public guarantee of up to 80% of the loan, for both short and medium to long-term operations, and to meet liquidity requirements and to make investments. The Fund guarantees a maximum of € 2.5 million for each company or professional, usable for one or more transactions without a number limit.

The biggest contribution is made to digital technology investments in case of investments in digital technologies, including big data investments, cloud computing, ultralight bandwidth, cybersecurity, advanced robotics and mechatronics, increased reality, 4D manufacturing, radio frequency identification and waste tracking and weighing systems.

Since 2017, the relevant tax credit discipline and research has been changed, which can be used until 2020 by companies that will carry out research on behalf of foreign buyers.

In the package of measures, the incentives for those who invest in SMEs and start up innovative types of businesses, which, since 2017 become more and more stable:

- a single rate is set at 30%, regardless of the type of innovative start-up beneficiary;
- the maximum investment limit to calculate the tax deduction for the Irpef subjects is increased to one million euro;
- the exemption from stamp duty and secretarial rights is introduced for the constitutive act of innovative start-ups and the possibility that the constitutive act is signed, as well as with digital signature, even with authenticated electronic signature.

While on one hand the incentive, plan seems to work perfectly, on the other hand, the road that leads to an improvement in skills within the companies is still complicate.

Inside the Industry Plan 4.0 there is an entire chapter, which provides for the diffusion of a 4.0 culture the entire training cycle, from school to university, from technical institutes superior to doctoral courses. And it is on this point that the Ministry of Economic Development is running to shelter with the National Industry Network 4.0, a new tool to spread knowledge about the real benefits of Industry Investment 4.0.

A platform, which will serve to promote and disseminate the benefits to businesses "deriving from investments in technologies in Industry 4.0". Industry Plan 4.0 is not just exhausted in introducing or reinforcing various tax measures to support investment and spending in Research and Development: today's major ambition is to be able to propose and disseminate a new business culture focused on Industry 4.0 expertise essential to maximize the benefits of new technologies.

In order to meet these requirements, a **"national network of Industry 4.0"** is created, consisting of numerous points distributed over the national territory, which pursue in various declinations the common goal of accompanying and supporting businesses in digital transformation. The aim is to spread knowledge about the benefits that technologies can make to industrial processes, to assist companies in identifying areas of intervention and to stimulate them in the realization of industrial research projects and experimental development.

The activities carried out by the national network, will have as their object:

- The assessment of digital maturity of businesses, by identifying areas of priority intervention and the development of high education courses;
- High education through the promotion and dissemination of expertise on demonstrative production lines and the development of use cases;
- Industrial research projects and experimental development, through the concentration of business study plans and experimental progress on existing or near marketing technologies and solutions, and support for potential contractors in the implementation and monitoring phase of the results.

## - 4.7: Final considerations

To successfully implement 4.0 organization, the workforce itself should also adopt a 4.0 mentality.

A successful cultural transformation assimilation process can span over a significantly long time period, and, if the time available is limited, the change must be guided by leaders empowered by a great vision and endowed with imagination.

Organizations must therefore be ready to face a process of structural evolution by adopting an enlightened, "proactive" mindset devoted to change, progress, and risk taking.

It is consequently essential that the entire corporate organization must be aware of the need to dare, to play. CEO, CISO, CIO, (formerly discussed above) general managers and administration should lead in first-person the reorganization of the company, through the creation of the flexibility and openness desired aimed at responding effectively to the need for innovation.

If a company wants this transformation to become a sizable portion of business culture, it is desirable that top management and Governments develop greater awareness of their role, as well as the implementation of new education programs aimed at the re-qualification of the current workforce. They have to pave the way for the preparation of future employees projected towards a continuously changing labor market landscape.

When digital transformation project is started, it is certain that it is not just limited to the choice of the most innovative, cutting-edge technologies available on the market. Adapting to the new digital world involves a careful review of processes, media and information flows that can generate value not only for its customers, but also at different corporate stages and for other actors in the Digital Supply Chain.

However, when it comes to adaptation, we should also keep in mind the flip-side of the coin, since the adoption of robotics, mechatronics, increased reality, 3D printers, and in general of the Internet of Things could lead companies to face many challenges among which significant job losses (which will be counterbalanced by the birth of new professional figures).

Digital Transformation also seems to bring with itself the wonderful perspective of a barrier-free world embedded in an intricate network of interconnections, but the analysis of the innovations that it involves, lead us to say that we must be able to protect our boundaries. They are represented by our personal sphere (privacy), by the economic interests of our companies (data retention), and by protection of the interests and security of our States.

Indeed, industrial espionage, robbery of sensitive data and cyberattacks can lead firms to the decision of pulling themselves out from the corporate market with the consequential disruption of countries' economies.

From the ability to protect our multiple boundaries, derives the ability to expand them.

To continue the creation and carry on the accumulated momentum for change, it is therefore necessary to grab the challenge of IT security.

This theme is becoming so essential that it has received a response both at political (Piano Calenda) and regulatory level (Council Directive 2016/1148/EU) and not only at the

technological development level, but also at the one concerned with the expansion of market competition.

In the industrial transition processes, that take place through the application of new technologies, IT Security is consolidating the structure of the new product and service space that is emerging at the intersection between Cloud, Big Data/Advanced Analytics and Mobile Devices.

Compared to the process of conversion of individual organizations, Cybersecurity is in fact a key, pivotal factor in the digital transformation processes that are embarking on many companies to implement the structure of their supply chain, aimed at the survival in a context of sophisticated international competition permeated by increasingly aggressive cyber-attacks.

In the Italian sphere, where many difficulties still persist, especially for SMEs, there aren't many available choices: in order to keep their competitive advantage and remain alive, organizations need imaginative capabilities. These are necessary to be able to catch the train already (in the race) of the Industry 4.0.

We are at the dawn of a historic challenge, for which we cannot even begin to comprehend its short or even long-term developments, in which the typically Italian creativity could play a key role in favor of our economy.

Current competition and strong changes create new, more unstable and harder to govern scenarios, which require our country to have an active and conscious presence, strong in a scientific, technological and cultural history of absolute moral relief.

## Bibliography

Accenture: “Industry X.0” 2017;

Accenture: “Digital Transformation Re-imagine from the outside-in”, 2014;

Accenture: “Security Technology Vision 2016: Più strumenti nelle mani dei responsabili della Cyber Security per sostenere il Digital Trust”, 2016;

Accenture: “World Economic Forum White Paper Digital Transformation of Industries”, 2016;

Albert Meige: “The chief innovation officer should be in charge of new territories not more not less”, Thursday March 10th, 2016;

Alessandro Di Fiore: “A Chief Innovation Officer’s Actual Responsibilities”, November 26, 2014;

Antonio TETI: “Cyber Security e Investimenti. Quali scenari?”, February 2016;

Baskerville R., Spagnoletti P., J. Kim: “Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response, Information and Management”, Vol. 51; 2014;

Benjamin Grynol: “Disruptive manufacturing. The effects of 3D printing”; 2016;

Brenna Sniderman, Parker Baum and Vikram Rajan: “3D opportunity for life. Additive manufacturing takes humanitarian action”, 2016;

Capgemini Consulting: “Digital Transformation: a roadmap for billion-dollar organizations”, 2014;

CINI- Roberto Baldoni e Luca Montanari: “National cybersecurity Report - Un framework nazionale per la cybersecurity” 2015;

CINI: “2016 Italian Cybersecurity Report- Controlli Essenziali di Cybersecurity”, march 2017;

Cornelius Baur and Dominik Wee: “Manufacturing’s next act”, June 2015;

Deloitte: “To have or not to have Cyber security Kompetencer”, 30 August 2016;

Deloitte: “The new CISO. Leading the strategic security organization” Taryn Aguas, Khalid Kark and Monique Francois, 2016;

Deloitte Global SAP: “Alliance Supply chain management”, 2017;

Deloitte University press, Kelly Marchese, Jeff Crane, Charlie Hayley: “3D opportunity for the supply chain”, Additive manufacturing delivers, 2015;

Deloitte University press, Brenna Sniderman, Monika Matho, Mark J. Cotteleer: “Industry 4.0 and manufacturing ecosystems”, 2016;

Deloitte University press, Michelle Canaan, John Lucker, Bram Spector: “Opting In: using IoT connectivity to drive differentiation”, the internet of things, 2016;

Deloitte University press: “Industry 4.0 and distribution centers - Transforming distribution operations through innovation”, 2016;

Deloitte Review: **“**Safeguarding the Internet of Things - Being secure, vigilant, and resilient in the connected age”, 2015;

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016;

Ernst and Young: “Cybersecurity and the Internet of Things”, March 2015;

Ernst and Young: “Is the business world ready for the internet of things?”, 2016;

European Parliament: “Industry 4.0”, 2016;

European Union Agency For Network And Information Security: “ENISA Threat Landscape 2015”, January 2016;

European Union Agency For Network And Information Security: “ENISA Threat Landscape Report 2016- 15 Top Cyber-Threats and Trends,” January 2017;

Fabio Cappelli, Partner EY e Responsabile Cybersecurity per l’Italia “Cybersecurity grazie alla cyber resilience: come proteggere le aziende nel 2017”, 10 Feb 2017;

Fabrizio Carapellotti - Maggioli Editore, Apogeo Education: “Governare l’economia 4.0, il digital data officer per una digital transformation vincente”, 2017;

Galen Gruman, Executive Editor: “What digital transformation really means” InfoWorld, 14 Jun 2016;

Gartner: Supply Chain, “Gartner incorona Amazon e indica le tre tendenze “calde” dell’anno”, 22 June 2015;

Gartner: “Building the Digital Platform: Insights From the 2016 CIO Agenda Report”, 2016;

Germany Trade and Invest: “INDUSTRIE 4.0Smart Manufacturing for the Future”, 2014;

Gianni Rusconi: “Nell’azienda 4.0 l’asset più importante è il personale”, 03 June 2016;

Giovanni Marra, Vincenzo E.M. Giardino: “Cyber Security nell'era della Digital Transformation”, 11/04/2017;

GT Nexus: “The current and Future State of Digital Supply Chain Transformation”, 2016;

Hypen: “Trasformazione digitale: cosa è cambiato per i processi di comunicazione”,2016;

Howard King: “What is digital transformation?”, 21 November 2013;

“Il Cyber Risk della Supply Chain: come gestire i fornitori?”, 30 giugno 2016;

Il sole 24 ore – Bologna Business school: “Il papa ed il lavoro di fronte alla sfida dell’innovazione”, 19 March 2017;

Jason Bloomberg: “Digital Transformation by Any Other Name?”, July 31 2014;

JW Marriott Orlando Grande Lakes #FORRDigital: “The Event for Digital Business Leaders And Technology Innovators”, May 10–11, 2016;

Massimo Menichinelli, “Fab Lab e maker. Laboratori, progettisti, comunità e imprese in Italia” Quodlibet Studio, 2016;

Maietta Andrea: “Stampa 3D. Guida completa”, Edizioni LSWR, 2014;

“Making existing production systems Industry 4.0-ready”- Volume 9, February 2015;

Mckinsey & Company: “Industry 4.0 after the initial hype-Where manufacturers are finding value and how they can best capture it”, 2016;

Mckinsey & Company: “Industry 4.0 demystified—lean’s next level”, march 2017;

Microsoft: “Digital Transformation Report”, 2017;

MISE: “Piano nazionale industria 4.0 Investimenti, produttività e innovazione”, Milano, 21 September 2016;

Nate Lord: Supply Chain Cybersecurity: Experts on How to Mitigate Third Party Risk - - January 26, 2017;

NETMEDIAEUROPE: “Cybercrime-ed-economia-vanno-a-braccetto”, 18 April2017;

OPEN DATA SRL: “Industry 4.0”;

PWC Italia - Team Digital Manufacturing: “Digital Manufacturing. Cogliere l’opportunità del Rinascimento Digitale”, 2015;

PWC: “Industry 4.0: Building the digital enterprise”, 2016;

PWC: “Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused, 2016;

PWC: “Industry 4.0 Opportunities and challenges of the industrial internet”, 2014;

Rapporto Clusit 2016- “sulla sicurezza ICT in Italia”, 2016

Rapporto Clusit 2017- Laura Zanotti: “Per la sicurezza è stato l'anno peggiore di sempre”, 22 February 2017;

Report prepared for a joint G20 German Presidency OECD conference: “2KEY ISSUES FOR DIGITAL TRANSFORMATION IN THE G20”, Berlin 12 January 2017;

Roberta Moscioni: “Network Nazionale Industria 4.0”, 23 maggio 2017;

Roland Berger: “Industria 4.0, la nuova frontiera della competitività industriale in Italia”, 5 May 2016;

Ron Davies: “Industry 4.0 – Digitalization for productivity and growth”, September 2015;

Swink, Melnyk, Cooper, Hartley: “Managing operation across the supply chain”, McGraw-Hill Irwin, second edition 2013;

Stefan Schrauf, Philipp Berttram: “Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused, September 7, 2016;

The economist: “Will robots displace humans as motorized vehicles ousted horses?”, 31March 17;

Valentina Ferrero: “Cos'è il Network Nazionale Industria 4.0”, 24 May 2017;

Wohlers T. Wohlers Report 2011: *"*Additive Manufacturing and 3D Printing, State of the Industry*";*

Wohlers, Wohlers "Report 2014", Wohlers Associates; 2015

World Economic Forum- Klaus Schwab: "The Fourth Industrial Revolution: what it means, how to respond",14 Jan 2016.

*Department of Business and Management*

*Course of Digital Transformation*

# The Digital Transformation of Supply Chains: opportunities and risks in the Italian Industry 4.0 landscape

## Summary

SUPERVISOR

PROF. Paolo Spagnoletti

CANDIDATE

Angelica Craveli

MATR. 671811

CO-SUPERVISOR

PROF. Stefano Za

ACADEMIC YEAR 2016/2017

## Summary

This paper addresses the theme of Industry 4.0, and in particular the relevance of the Italian Industry 4.0 framework. It is composed by four chapters related to each other.

The first chapter describes the positive effects of Digital Transformation; enhancements and innovations such as Additive Manufacturing, Internet of Things, Cloud, Big Data, Machine Learning, Wearable, and Robotics that are becoming an integral part of many industries structures.

The digital revolution is bringing with it the need for development of new professional figures, such as CIO or CISO and is involving in a specific way companies' supply chains.

The supply chain is the fulcrum of the second chapter. Digital Transformation is improving and speeding up the different stages of the production process, including planning, procurement, and logistics. The machines used are increasingly innovative and interconnected, based on robotics and the use of sensors that allow different parts of the warehouse to converse with each other.

In chapter three, starting from brief references to the industrial revolutions that evolved over the years, I went through the analysis of the challenges and problems that Industry 4.0 brings with it. From negative effects, such as job losses to environmental issues, from cybersecurity to the need to retrain the current employees, passing through to the comprehension of how companies, schools, universities and Governments should intervene and invest to exploit the opportunities of Revolution 4.0 we arrive at the final chapter.

In the last part of this paper is considered as a controversial theme and growing risk for an interconnected world: The Cybersecurity.

The number of hacker attacks in recent years has seen a widespread increase, including the WannaCry ransomware attack that struck in May this year. The European Community has already taken steps to increase computer security measures through the 2016/1148/EU directive of 6 July 2016, which urges the Union countries to standardize and increase security levels.

In the top ten of the countries that have suffered more attacks, we can find Italy.

The cyber threat is significant in our country and the creation of a "National Framework for Cybersecurity" was necessary to provide essential guidelines and controls to all companies that must apply them in order to protect themselves and the entire Italian economic landscape.

It is mandatory for our country to take advantage of this deep revolution paying attention to the relative risks.

## 1: Industry 4.0 revolution

We entered the third digital revolution in the world of manufacturing.
New digital technologies that are finally available, often at low cost, allow us to design and manufacture almost everything we imagine, that we would have had and become functional to improve every area where we apply technology.
The evolutionary process of technological-manufacturing sector is leading the consumer towards a new awareness: the ability to be part of the change himself. This is steering industries towards a new production and distribution model, based on the modulation of goods and services, which meets the real needs of each customer through a flexible production structure, interconnected and highly localized. The modern approach to manufacturing is undergoing a "democratic development" as now, through the media and the digital network, the intuition of a single individual can become something concrete, produced at very low cost.

With "additive manufacturing", we refer to the name used to identify the processes that lead to the construction of an object through the superposition of layers (layer manufacturing). Opposite processing, respect to milling or laser machining based instead of "subtractive" processes. The finished products of a company are carried out not more shaping or removing material, but adding the material, layer by layer and it is the process used by 3D printers.
The elimination of transactions, usually required in conventional methods, as pre and postproduction lowers costs, time or labour now become superfluous in the manufacturing process. The additive manufacturing processes, however, work in different ways depending on the technological needs that arise for the realization of a project.
The framework of the Industry 4.0 in our country is basically positive: almost a third of companies have already started three or more projects based on innovative digital technologies such as the Industrial Internet of Things, the Cloud Manufacturing, Advanced Automation, the Industrial Analytics or Advanced Human Machine Interface.
The market value of smart Manufacturing in 2015 in Italy is around 1.2 billion euros, a significant value that represents just a bit less than 10% of the total industrial investments (10-12 billion euros). To create a flexible and responsive digital supply chain firms cannot just gather technologies and build infrastructures. They must also manage the shift to a completely

new culture, finding people with the right skills, able and willing to carry out the effort. In other words, they must rework their entire organization starting from the human resources.
The increasingly important role of HR in a 4.0 Industry sees the emergence, in the last 10 years of new professions, one of those is the CIO (Chief innovation officer). This figure created in enterprises of the Anglo-Saxon countries is characterized by an innovative profile, which embodies a strategist, an IT manager and a market and management of information systems expert.
Another emerging figure is the CISO, with this acronym, we can identity the Chief Innovation Security Officer, a figure that attends the fundamental roles of handling security technologies (technologist) and defend enterprise assets (guardian).
Many people are now interested in technology development and new digital application, but often they do not have the opportunity to get in touch or know how to use them.
A FabLab (fabrication laboratory) is a small workshop of "Arts and crafts" where a set of computerized tools allow flexible and inexpensive personalized services of digital fabrication.
The main objective of a FabLab, it is to be a space for experimenting with digital technologies and understand how they can influence the development of prototypes, innovative objects and solutions for Smart City, using open source software and big data analytics.

The term Digital transformation identifies a set of mainly technological changes, but also social, organizational, cultural, creative and managerial skills, which allow the company to go to redesign the offering of their business to make it more competitive and closer to consumer expectations thanks to digital technologies. Becomes necessary, for a company, to find out whether the technology that is going to apply within its production process, it will be efficient in the long run, that is, his analysis should go to try to understand the way that innovation will evolve over time.

## 2: Digital Supply Chain

To realize the vision of 4.0 Industry, most enterprises need to change and develop a new way of organizing and thinking each of their processes. A critical element is represented by the evolution of traditional supply chains toward a smart, responsive, connected, and highly efficient supply chain ecosystem.

A Supply Chain is defined as the global network of organizations and activities involved in designing a set of goods and services and their related processes, transforming inputs in outputs, consuming and finally disposing the goods and services produced. Therefore, the supply chain involves almost all the different areas of an industry, from the procurement through suppliers (upstream supply chain) to the logistic, from marketing to human resources and from the production to the final customer (downstream supply chain).

Digitization brings down the walls among the different areas, and the chain becomes a completely integrated machinery, completely transparent to all the players involved from the suppliers of raw materials, parts and components, to the transporters of inputs and output, and finally to the customers that buy the final products.

In terms of information, a critical element of Industry 4.0 is big data analytics and to aspire at the highest operational excellence, manufacturers need increased transparence and information from the top floor to the shop floor with the possibility to check the status of inventory and its possible changes, the orders management, and the entire process performance. In particular, it is important to automatize the production process thanks to the utilization of machines, sensors, terminals and measurement tools all connected together.

Industry 4.0 is enabling warehouses to be always in line with the progressive changes of the entire market transforming them in one of the most strategic tools that a firm can use to create its strategic advantage.

The final goal of this transition is the improvement of safety and efficiency through the automation of almost every warehousing activity. Indeed, the increasing focus on multitasking abilities creates great pressure on organizations to keep up with a higher number of orders, and the necessity of rapid processing and management of the spaces, to improve economies of scale and ensure high throughput.The key factor that can lead to success any supply chain is certainly the efficient exchange of information: communication.

Benefits that an organization can reach with a high level of interaction and information transparency are significant. They are not just limited to costs savings planning improvement and a better inventory management, they regard the entire structure of the firm its internal and external environment. If there is a good level of communication, there is no need to repeat or clarify notions and detail wasting precious time for work.

The future of production will be based on the development of efficient manufacturing systems and structures in which products are able to control their own manufacturing process and on the use of 3D printers and new sensors and technologies as the wearable one. As previously mentioned, 3D printing means the realization of three-dimensional objects using additive manufacturing techniques, starting with a digital 3D model and wearable technology; we do refer to a category of innovative electronic devices, equipped with one or more sensors with various and numerous processing capability. We can define wearable technologies, belts, bracelets, watches and electronic smart glasses and helmets, fabrics and clothes cyborg, tattoos as bar codes or RFID and much more.

## 3: Critical aspects of Industry 4.0

In the industrial revolutions history to each period, you can attribute defined aspects that characterize and differentiate it with respect to others; and together they can grasp the sake of continuity.

A first production period is identifiable in the time between the two industrial revolutions, where manufacturing takes a vital role in the economic and social context. The sequence of the first and second industrial revolution over an economics century (1840-1970) contributes to the emergence of different organizational paradigms, fruit progressive affirmation of many scientific and technological ones, which will mark the path of progress until the birth of modern industry. The booming inherited from the years of industrialization, the rise demand and the expansion of markets over time trigger a thrust to increase size of enterprises: the factory becomes the temple of the development.

Economic and the most tangible representation of what we now call industrial capitalism.

The growing interaction between science, technology and the world of production leads to define the second industrial revolution as Scientists Revolution and at the same time, just due to the mechanization of the manufacturing sector, it causes an increase in the so-called technological unemployment.

The expansion of company size, the advent of big business and mass production require a new organization production, capable of obtaining the maximum production at the lowest cost and with the least use of labor. Companies focus their attention on achieving economies of scale through the specialization of production and standardization of production processes and behaviors related to manual work.

Digital Transformation is progressively changing the way of how industrial workers perform their jobs, with the increasingly diffused use of robots and machineries entirely new job families will be created while others will become obsolete. It is certain that robots and humans will increasingly have to work alongside one another in the workplace.

Economists are worried about the phenomenon of **"job polarization"** characterized by the decline of middle-skill jobs and the increase of low-skill and high-skill jobs.

In this way, the workforce is divided into two groups, the first doing non-routine work such as skilled and highly paid workers the second one doing routine work such as unskilled low-paid workers. Unpredictable risks can appear at any time, some of them could involve the workers, others the final product. That is why is necessary to train employees to have confidence with robots.

Furthermore, employees need vigilance especially consequently to the put in motion of automatic procedures, that can have as result accidents at work because once started are difficult to stop. Increased mechanical autonomy will cause problems related to the definition of legal responsibility for accidents involving new advanced technologies such as driverless cars. Who will have to pay for the insurance? The owner, the manufacturers?

If from one side the reduction of human labor forces could lead to a significant cut in production costs, on the other hand, it is leading to significant social and ethics consequences.

In this historical phase, the transformation of work and the expulsion of workers is so fast that it makes it very difficult to have an immediate "substitution" for other new activities.

It is certain, unlike all previous revolutions, the new jobs created are far lower than the lost ones.

This revolution is influencing all the countries around the world, some of them in a positive, others in a negative way. For a long time, Brazil, Russia, India and China, the BRIC countries, were considered the future of the global economy.

However, actually, the demand for raw materials by is decreasing and these countries are becoming always less attractive. This route change is transforming the BRIC in the possible losers of this fourth industrial revolution. In fact, with the progressive and efficient development of machines and production robots, different organizations that outsourced their production in low labor-cost countries are relocating their plants to the countries where they originally came from.

There is a strong lack of digital investments due to the absence of infrastructures, education of a part of the population and a not always clear legal framework.

The possible winners of the development of 4.0 industry are, on the other hand, the highly developed Asian countries characterized by excellent education systems, such as Hong Kong, Singapore, South Korea and Taiwan side by side with the Scandinavian countries.

These countries have been studying and working on the development of digital solutions for a long time creating in this way an increasingly advanced interconnection of systems and people.

The evolution of Industry 4.0 is progressively changing the way the society perceives different kinds of jobs; new cross-functional roles are arising for which workers will need particular skills and knowledge in both IT and production. Consequently, the fluctuating employment landscape has numerous implications for organizations, industrial companies, education programs, and Governments. Those last ones are responsible not only for making education accessible to everyone on their competence area and help companies to hold as many workers as possible, but they must help improve coordination among different stakeholders in business organizations focusing young people's interests on technology and always more technical jobs.

To allow the maximization of the number of jobs created by the Digital Transformation and the options offered by the involved firms, the government effort will need to focus on promoting the efficient implementation of Industry 4.0, which is a prerequisite to generate economic growth and create new employment opportunities.

To be able to meet the new high standards set by Industry 4.0 revolution, the educational system must be adapted to these new technology trends and quickly changing conditions.

Schools should encourage students' interest in subjects such as science, information technology and mathematics.

Teachers need to be formed with digital competences, they must teach students how to think in a different and critical way when using new technologies and help them to understand the real meaning and dangers of new digital and information devices.

The revolution of Industry 4.0 is creating something that will have several impacts on the nature of work and organizations, new kinds of interactions between people and machines.

Companies should start to consider changes in their production schedules, create new work and organization models in order to get fit with the continuously evolving conditions of the

general economic environment that includes flexible schedules and the adaptation to new rhythms of work dictated by machines and robots.

That is why organizations should engage in is the “strategic workforce planning”.

This is a process that should repeated annually and that starts with gathering information related to the organization workers and subsequently categorizing them into different job families.

New approaches to recruiting should be developed; they should be more focused on soft skills and capabilities rather than on qualifications determined by degrees and certificates.

Recruiters should look beyond formalities to understand the real value of a candidate and comprehend if his/her skills are adequate for the future role because the task on which the future employee will have to work are usually far from his/her core education.

Furthermore, organizations will necessary have to retrain their employees because they must be flexible, be able to learn, adapt quickly to changes and have access to new fundamental skills.

Another consequence of digitization is the creation of possible environmental damages and two challenges in particular are under governments’ attention; the increasing energy consumed by data centers and the growing quantity of e-waste produced.

The growth in size and number of data centers is resulting in new elevate environmental costs.

Data centers are contributing through their high-energy consumption and usually inefficient cooling systems to the increase of worldwide emissions level.

Electronics have always been source of waste, but recently the speed and the quantity of dispose has increased uncontrollably. With changes in technology and consumer demand, is nearly impossible that any device will persists for more than a couple of years in the hands of the original owner.

The biggest part of our e-waste is sent to developing countries, where recycle procedures are usually informal and not appropriately regulated. Rich nations are sending the biggest part of their waste to developing countries because they do not have strict legislation.

Another element companies and Governments should take in consideration is the central issue of data security prevention and protection, known as **Cybersecurity**.

Companies wishing to ride the digitalization wave will have to deal with the need to ensure the information security of their customers' personal data. This factor is more accentuated by the fact that customer data and information will be key elements for business companies.

Opening up systems to the data sharing can bring a number of risks associated to digital security and the protection of privacy, both to the infrastructure and the data itself.
The issue is current and recently addressed at Community level through the adoption of Parliament's and Council Directive 2016/1148/EU of 6 July 2016 on measures for a high common level of security of the Union's networks and information systems CD NIS Directive.
The Directive requires Member States to work to strengthen cooperation between them in the interests of greater information exchange through the European Network and Information Security Agency (ENISA).

## 4: Cybersecurity and Italy

As mentioned previously we can consider the cybersecurity one of the new challenges of Industry 4.0 framework.
The huge number of devices, universal access and the large amount of data to be handled poses significant challenges on privacy, data protection and security issues.
These scenarios open up new areas of risk not to be underestimated, such as identity theft of information and other attacks from new computer threats. Computer criminals are working on new ways to exploit organizations' vulnerabilities in order to access sensitive data and steal intellectual property. Increasing digitization, using the Internet and smart working, however, indicate that the boundaries of organizations are no more clearly identifiable.
Businesses can no longer worry about monitoring cyber risks only within their organization. The integration and interconnection of supply chains entails both new opportunities, such as real-time communications, greater efficiency and new synergies, as well as new risks.
Usually when firms think about safety, their goal is to safeguard their systems, digital assets and software against data breaches and cyber-attacks. However, it is important to consider that also the supply chain, whether a simple manufacturer or service provider's supply chain or the "data supply chain" trusted on by most organizations, is susceptible to security jeopardies.
Supply chain security is a highly multifaceted, embryonic function, and needs more attention from the business executives as the risks they are facing and that are affecting supply chains are becoming progressively clear. **Supply chain security is every company's responsibility.**

The 2016 has been the worst year for cyber security and among the world's most affected country there is Italy. For the first time, our country is in the top ten of the most serious

attacks and the number of casualties. This is the evidence presented with the "**Clusit report 2017"**, the well-known association for Italian IT security. In particular the most frequent risks organizations are facing are: malware, ransomware, phishing, botnet and DDoS.

**Malware** is a software that, once executed on a computer system, can make any undesirable changes or damage to the system itself and its users. Malware can do the most diverse actions on the victim system: they can subtract stored information and damage them or modify them in a weighted way, capture victim device screens by violating privacy of its users, stealing credentials of users who use the system, and more.

**Ransomware** is a specific type of malware whose purpose is to prevent the victim access and use of documents and devices. The attacker then crushes the victim by asking for one "Redemption" for the release of inaccessible resources.

**Phishing** is nothing more than a fraud attempt put into practice through the Internet, which has as its sole purpose the burden of sensitive and delicate information such as username, password, access codes, current account numbers or credit card data (it comes from the English term "fishing" which, refers literally "to fish" data).

A **botnet** (a "robotic network" contraction) is a network of maliciously-infected computers that is under the direct control of a single attack author, known as a "bot manager". Individual computers under the control of the hacker are called bots.

The attack author is able to control every computer in the botnet from a central point to simultaneously perform coordinated criminal action.

A Denial of Service (DOS) attack is an attack aimed at halting a computer, a network, or even a particular service offered or to completely disable the server or even an entire network.

A **Distributed Denial Service** (DDoS) attack is a variant of DoS and uses tens of thousands of infected computers, which form a botnet, to complete the attack.

Protecting an organization is a challenging mission itself, without even thinking about all the risks and vulnerabilities that affect the supply chain. Nevertheless, it is important nowadays also to evaluate what happens outside the corporate walls.

How to prepare to manage third parties correctly? What are the steps to take into consideration?

The National Cyber Security Framework, published at the beginning of 2016, may be the tool used by large organizations to define minimum "standard" security requirements to be applied

to their supply chain. This will boost overall cyber security throughout the supplier's Italian ecosystem (consisting mostly of a large number of small and medium-sized companies).
In the report, "Combating Cyber Risks in the Supply Chain" (SANS Institute, September 2015) is said that one of the most important thing to do is to define the most critical vendors, those that could lead to the worst consequences in case of data breach or malfunction.
Firms may not be able to predict when information security incidents arise, but they can control how they reply to them intensifying detection competences and capabilities.

A well-functioning **security operations center** (SOC) can represent a good strategy to create a strategy of effective detection. The emphasis of the SOC must be the management of cyber threats according to business priorities. The SOC can have an important role in enabling a more efficient decision making processes producing related reporting and risk management and business endurance allowing the information security department to respond faster.

In an increasingly global and interconnected world, several business processes are nowadays shared by companies with their own supply chain, made by third parties such as product providers, service providers, and distributors.
The first thing businesses should do is to ensure that all the supply chain suppliers have codified, validated and certified security guidelines and measures.
Moreover, security can be further enhanced through the launch of a scheme of restricted network access for related sellers.
Nevertheless, safety measures should not just be applied to third parties, the internal security is important as well.
The company has the obligation to apply standard IT solutions such as firewall, anti-spyware and antivirus. But that’s not enough, the firm should go further than that adopting advanced IT technologies like network access control, business continuity solutions, bake-up systems and all the possible assets that could guarantee the structure safety.
**That is why cybersecurity requires commitment and collaboration.**
A possible solution to contain the risk of attacks is the so-called Cyber Resilience, which is the continuous examination of resistance to possible threats and the time needed in trying to recover the original status prior to the event or adapting to the new condition trying to find efficient alternatives of carrying on the business.
Once comprehended what is cyber risk and that it can be analyzed, mitigated and ultimately transferred, and defined the possibility of covering damages and costs, it may be useful to

better understand and decide if we may need a cyber policy and what features this must have to protect a business.

Cyber-insurance can of course not prevent the computer attack from happening, but it can help the accident victim to endure the resulting damages, particularly the costs associated with the damage caused to third parties for which the company is responsible.

In recent times, public opinion has been exposed to numerous cases of cyber-attacks even with some important effects. In many cases, they were attacks by government-related actors, in other cases it was the use of the cyber dimension for activities and mixed attacks (terrorism, espionage operations, and military operations). Even small and medium businesses are beginning to understand that there is a problem that might involve them, but not always understanding that the consequences could be disastrous.

The level of awareness has increased accordingly and Italy begin to wonder what its level of preparation is. This process of growing consciousness, still extremely acute in our country, must necessarily be supported by methodological tools.

These tools must be simple, suitable for any type of user, providing a roadmap to achieve a minimum level of preparation in protecting your own information and/or reputation and your business. The National Framework is born precisely in this regard.

Finally, it is critical to note that the cyber threat requires a primarily coordinated public and private response.

As noted in the White Paper on "The Future of Cyber Security in Italy" published in November 2015, and followed by the “2016 Italian Cybersecurity Report Controlli Essenziali di Cybersecurity” the **National Cyber Security Framework**, is one of the key elements to increase domestic resilience of systems and networks against this threat.

The benefits of a cybersecurity framework for the Italian landscape for SMEs, Large Enterprises and Industry Regulators can be summarized as:

- Small Medium Enterprises: the main problem of small businesses, when they look at the world of security, are the costs. They cannot assess what are the "quick-win" practices independently, that is to say, those with the least amount of effort guaranteeing a level-of-stage protection. Consequently, these companies run the risk of improperly estimating the cost of putting their assets in safety, with the result that often the idea of increasing their security is put aside, running enormous risks, of which they are not aware.

- Large Enterprises: the National Framework does not have the claim to drive Large Enterprises and replace the complex risk management of these. However, it can, be very useful in copying, through a unified methodology, business risk management processes and programs, in order to make them evolve in a coherent and structured way. In addition, Large Enterprises can benefit from the presence of the Framework in two key aspects: the internationality of this and the ability to require security profiles to its contractors.

- Sector regulators: as far as sector regulators are concerned, the National Framework provides a unique interface to work on consistently with both regulating companies and other regulators. The Framework can be used as a tool for defining standards in a structured and compatible manner with other regulators. This is one of the first documents that, in addition to addressing the essential security methodologies, considers the costs.

In the "Industry plan 4.0" and in particular in the called "Piano Calenda" developed in our country at the end of 2016 are presented all the measures that each company can activate automatically and without any dimensional, sectoral or territorial constraints to promote innovation and competitiveness with hyper and super depreciation, R&D tax credit, startup measures and Innovative SME.

The Industry 4.0 goal must be to combine cybersecurity with the concept of cyber-resilience.
No matter with security, lawyers and certification bodies, the Privacy Guardian and the responsible authorities, the HR and the facility management personnel are involved.
It is necessary to work in a three-phase mode, implementing a strategy that can reason before, during and after an attack. Cybersecurity means designing predictive and reactive systems that, on one hand, are able to anticipate threats and, on the other hand, are able to implement timely and effective intervention plans.
Industry Plan 4.0 is not just exhausted in introducing or reinforcing various tax measures to support investment and spending in Research and Development: today's major ambition is to be able to propose and disseminate a new business culture focused on Industry 4.0 expertise essential to maximize the benefits of new technologies.

## Conclusions

To successfully implement a 4.0 organization, the workforce itself should adopt a 4.0 mentality.

A successful cultural transformation assimilation process can span over a significantly long time period, and, if the time available is limited, the change must be guided by leaders empowered by a great vision and endowed with imagination.

Organizations must therefore be ready to face a process of structural evolution by adopting an enlightened, "proactive" mindset devoted to change, progress, and risk taking.

It is consequently essential that the entire corporate organization must be aware of the need to dare, to play. CEO, CISO, CIO, (formerly discussed above) general managers and administration should lead in first-person the reorganization of the company, through the creation of the flexibility and openness desired aimed at responding effectively to the need for innovation.

If a company wants this transformation to become a sizable portion of business culture, it is desirable that top management and Governments develop greater awareness of their role, as well as the implementation of new education programs aimed at the re-qualification of the current workforce. They have to pave the way for the preparation of future employees projected towards a continuously changing labor market landscape.

When digital transformation project is started, it is certain that it is not just limited to the choice of the most innovative, cutting-edge technologies available on the market. Adapting to the new digital world involves a careful review of processes, media and information flows that can generate value not only for its customers, but also at different corporate stages and for other actors in the Digital Supply Chain.

However, when it comes to adaptation, we should also keep in mind the flip-side of the coin, since the adoption of robotics, mechatronics, increased reality, 3D printers, and in general of the Internet of Things could lead companies to face many challenges among which significant job losses (which will be counterbalanced by the birth of new professional figures).

Digital Transformation also seems to bring with itself the wonderful perspective of a barrier-free world embedded in an intricate network of interconnections, but the analysis of the innovations that it involves, lead us to say that we must be able to protect our boundaries. They are represented by our personal sphere (privacy), by the economic interests of our companies (data retention), and by protection of the interests and security of our States.

Indeed, industrial espionage, robbery of sensitive data and cyberattacks can lead firms to the decision of pulling themselves out from the corporate market with the consequential disruption of countries' economies.

From the ability to protect our multiple boundaries, derives the ability to expand them.

To continue the creation and carry on the accumulated momentum for change, it is therefore necessary to grab the challenge of IT security.

This theme is becoming so essential that it has received a response both at political (Piano Calenda) and regulatory level (Council Directive 2016/1148/EU) and not only at the technological development level, but also at the one concerned with the expansion of market competition. In the industrial transition processes, that take place through the application of new technologies, IT Security is consolidating the structure of the new product and service space that is emerging at the intersection between Cloud, Big Data/Advanced Analytics and Mobile Devices. Compared to the process of conversion of individual organizations, Cybersecurity is in fact a key, pivotal factor in the digital transformation processes that are embarking on many companies to implement the structure of their supply chain, aimed at the survival in a context of sophisticated international competition permeated by increasingly aggressive cyber-attacks.

In the Italian sphere, where many difficulties still persist, especially for SMEs, there aren't many available choices: in order to keep their competitive advantage and remain alive, organizations need imaginative capabilities. These are necessary to be able to catch the train already (in the race) of the Industry 4.0.

We are at the dawn of a historic challenge, for which we cannot even begin to comprehend its short or even long-term developments, in which the typically Italian creativity could play a key role in favor of our economy.

Current competition and strong changes create new, more unstable and harder to govern scenarios, which require our country to have an active and conscious presence, strong in a scientific, technological and cultural history of absolute moral relief.