Dipartimento di Management

Cattedra: Entrepreneurship And Venture Capital

Under the eye of Cyber criminals: a business adaptation perspective

RELATORE

PROF. FEDERICA CECI

CANDIDATO

MANFREDI LUCHETTI

MATR. 683011

CORRELATORE

PROF. ARTURO CAPASSO

ANNO ACCADEMICO 2017-2018

Under the eye of Cyber criminals: a business adaptation perspective

INDEX

INTRODUCTION

During my academic career, I have worked for three large companies, through which I understood how it is possible, having economic and technological resources, to cope with the risks arising from the surrounding environment. On the other hand, I created two startups which gave me the spirit to discover what was still unexplored and in particular, they have allowed me to recognize that often there aren't sufficient resources to solve a problem, and therefore, the survival is given by the possibility to combat drawbacks in a different way from what the standard proposes.

The purpose of this thesis is to investigate how, given the lack of assets of small companies, it is feasible for startups to face Cyber threats going to exploit their advantages in terms of the possibility to change rapidly their business model in front of external pressures, indeed, the topic of my final work focuses on how Cyber threats drive the change of the business model in small firms.

Since there are no literary data about this topic, I decided to do an experimental thesis based on the Eisenhardt method, then I created three cases studies, and using the existing theory I have the intent to find a recurring "pattern" to be applied to all the existing small companies.

In line with Glaser and Strauss (1967), the close connection between reality and case studies allows to generate a valid theory, giving, according to Kuhn, to the findings a scientific relevance.

At the beginning of the discussion, I wondered if the Cyber space could really be considered a danger for startups; according to Barak Obama "Cyber threats were one of the most serious economic national security challenges that we face as a nation, and I made confronting them a priority", confirming this opinion,in 2007 Estonia was hit by a distributed denial of services(DDoS) which blocked the internal banking system of the country. Also the companies are target for hackers, McDonald Japan was hit by a Ransomware called "WannaCry" that obstructed the electronic payment system of the firm driving a collapse of the company's value in terms of both credibility and profitability.

Having decided to observe the changing dynamics of startups, the second step is to examine whether even small firms can be a target for hackers, therefore, I want to discover the real goals of Cyber criminals, to see if these are in match with the resources that a small company can offer. In order to give strength to the existing literature, I ask to the 3 startups interviewed questions about their experiences in terms of Cyber attacks, this allows me to measure the degree of risk that startups face.

Going forward with the discussion, I explore about the resources that a company needs in order to be protected, then, taking into account the existing literature I conduct a research about the methods of attack used by hackers and the related defense strategies of the target firms, this allows me to understand if the Cyber defense was viable only for large companies or even for startups. I asked to the interviewed firms if they felt adequately protected and if they have the necessary resources to increase their investment in IT security.

According to Darwin through transformations and mutations, living species, finding the right solutions, have adapted to the environment, therefore, in the second chapter I tried to apply this aspect to startups, asking me the following question: If small companies do not have the adequate resources, what tools could they use in order to be protected?

With the purpose to observe the ability of small businesses to react to Cyber threats, I focus on the dynamics of the business model in order to see if startups were likely to change in line with the environmental threats.

Teece defines business models as the logic by which firms create and deliver value to customers.

The first step is to observe the propensity to change the business model; from the existing literature it is possible to see that small companies, unlike large ones, are more favorable to tranform their internal structure due to the lower presence of fixed assets. Another key factor in order to drive the business model renewal are the dynamic capabilities for which I mean the company’s capability to build, integrate and reconfigure its internal resources to accommodate change in the external environment; for this reason, they are vital components of the business model, in fact these represent the opportunity for small companies to redesign their business model in front of cyber risks.

Doz & Kosonen in order to highlight the concept of business renewal, have built a strategic agility framework which conceptualized strategic agility as the "thoughtful and

purposive interplay on the part of the top management" between three meta-capabilities: strategic sensitivity, leadership, unity and resource fluidity. At this point, applying every single component to the interviewed startups I am able to verify if there is a common factor that suggests a propensity of small companies to change.

To give more strength to what emerged, I ask the startups interviewed if their annual investment in Cyber security feels them to be adequately protected, and if they have the possibility to increase it. So looking at whether the Cyber Defense is sustainable for small businesses, I can deduce if they are forced to change business model or not.

To conclude this first discussion, I investigate about the number of members of the interviewed teams and their education level, in fact, as stated by Helfat the level of education of team meambers influence the dynamic capabilities that in turn drive the change in the business model. The dynamic capabilities increase proportionally with the level of instruction of the firms partners.

In order to understand the possible drivers behind the change, observing what was expressed by the existing theory, I focused on two models: business model innovation and business model adaptation. In the first case I consider it as a process that involves the decision of the top management to innovate its business model, so in this occasion the distinctive element is the internal will of the company to make a change to bring a surplus in terms of corporate performance. In the second case, for business model adaptation, I mean the process by which startups change their business model due to external threats. In line with Saebi, business model adaptation consists in the continuous research, selection and improvement based on the surrounding environment. In order to understand which of the two models determins the change, I analyze the possible drivers of the three companies interviewed asking them a series of questions aimed at the observation of the internal factors, such as the top management previous entrepreneurial experiences, and the external factors, such as the adaptation to national regulation.

After having learned, through the existing literature and the interviews conducted, if due to the cyber threats, the business model of small companies tends to change and which are the drivers to push this transformation, I will answer to my research question going to observe what are the principal tranformations within the following business model areas: Key partners, Channels, Value proposition and Cost structure.

For key partners I consider all the actors outside the firm, such as suppliers and distributors, that contribute to create value. In order to observe what happens in this area, I ask the companies interviewed about their cooperation with other companies and what they think about the privacy of their data held by the partners. This allows me to see if, with the advent of the Cyber threats, the degree of openness to the external environment increases, leading companies to adopt forms of cooperation to face the risks deriving from cyber space or decrease, leading companies to hide their own protection systems in order to safeguard, in case of attack, their image.

The business model channels are the tools used by the corporation to reach its market segment; in order to measure what happens in this area, I ask the companies interviewed if, in order to feel more protected, they would be willing to sell on third-party channels deemed more secure.

In line with Koufaris and Hampton Sousa, "the risks the internet consumer appears to have to face are extremely high", so often companies to avoid holding confidential information, decide to treat the smallest possible number of information by adopting strategies aimed to ensure greater protection for themselves and their customers.

The third area of the business model that I analyze concerns the value proposition, which represents the reason why customers choose the product of a company rather than that of another one. In order to determine the changes in this area in the questionnaire I insert a question that allows me to understand if, in the companies interviewed, it has ever happened that some customer has felt discouraged from making an online payment. Obviously this would lead to a reduction in profitability for companies and therefore ensure adequate measures of Cyber Defense would fall within the value proposition of small companies.

The last area of the business model observed concerns the costs structure, so my goal will be to understand how it changes as a result of IT risks. The analysis will include both visible costs and hidden costs.

CHAPTER 1

THE CYBER DOMAIN

1.1 The concept of Cyber Space

The Cyber Space represents the conceptual place where people interact telematically exchanging informations, it could be considered as a complex network that today groups and manages individual's life; just consider when we send an email to another person, the correspondence passes from a computer to another through the Cyber Space. As stated by Lance Strate, the World Wide Web should be considered as a collective concept which takes in consideration all the different experiences connected to internet technologies. The data superhighway have entered in disruptive way in our daily routine, the essential distribution services like energy, transport and health care are part of this virtual space and today, both public and private sectors are highly dependent on the information system to bring forward their quotidian functions.

Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data".

According to Barak Obama "these cyber threats were one of the most serious economic national security challenges that we face as a nation, and I made confronting them a priority", indeed, repercussions of Cyber attacks proved to be really tragic, in 2007 Estonia was hit by a distributed denial of services(DDoS) which blocked the internal banking system of the country, causing serious inconveniences for the population. One of the peculiarities of this phenomenon is that not only public facilities are affected, but there are also many private companies which were attacked, for example McDonald Japan was hit by a Ransomware called "WannaCry" that obstructed the electronic payment system of the firm driving a collapse of the company's value in terms of both credibility and profitability.

The economic losses related to Cyber crime amount to $345 billion each year, on average large companies suffer 100 attacks per year and around 1/3 of them is successful despite the Cyber Security spending is $70 billion per year; these numbers don't seem to stop, in fact, with the advent of IoT(Internet of things), by 2020 online devices are projected to outnumber human users by a ratio of six to one, creating a huge opportunity for cyber criminals to manipulate connected appliances.

Although there are many differences between space and Cyber space, there are also several similarities, in fact the two components complement each other; in line with Madelyn R. Creedon " The bit of data may ride on fibre for a while before being directed up through a satellite and back down to another terrestrial network". The principal divergence between space and Cyber space is that it presents low barriers to entry, making it more democratic but also more dangerous. Under the point of view of the State control's power, the Cyber space, for its characteristics, is much more difficult to restrict, in fact it has developed very quickly becoming a system characterized by openness and interoperability.

1.2 Customer perspective about Cyber security

Today, online sales lead to companies a large percentage of profits, over the years in fact, many firms have started to hire designers and computer engineers with the aim of creating an online infrastructure as high-performing as possible. Online sales channels are used mainly by small businesses, in this way they have the possibility to reduce the fixed costs related to the opening of a physical store for the sale of their products. The customer trust revolves around a series of factors related to the seller (Coulter, 2002), in fact when the customer puts in being an online purchase, he is in an uncertain environment, where, not having a physical interaction with the vendor he is not able to evaluate the quality of the product, verify the identity of the supplier and the protection of personal information. In this section we will isolate this last aspect, then the one related to the protection from Cyber risks. "It would be fair to say that the risks the internet consumer appears to have to face are extremely high" (Koufaris and Hampton Sousa, 2002).

With the advent of IT risks, costs for these small companies seem to increase, indeed, the customer's security in making the purchase is a determinant factor for the success of the sales department, for this reason startups are dedicating more and more attention to customer perception during the payment process.

To define the situation, it is necessary to outline the two main factors that tend to create fear for the client: privacy and security.

Regarding privacy, we can say that it concerns the ability of the individual to control the use of his information (Westin). Today, with the advent of the internet, information tends to circulate much faster and has become a business opportunity for Cyber criminals. On the other side, the concept of security is reflected on the reliability of the payment method used, therefore on the fact that information is not used for purposes unrelated to the pre-established ones.

According to the Gartner Group study, 95% of online customers are concerned about the privacy and security when they make online payments. This data shows how important it is for online businesses to ensure adequate security in order to survive. The internet business man finds himself having to demonstrate his honesty on one hand on the quality of the products offered, on the other hand on the technical and finance skills in order to guarantee the success in the payment process. In line with the pwc research, following the success of a cyber attack against a company, customers tend to forget but the trust lost is only redeemable if companies implement real changes to prevent attacks. In this direction, further measures can be adopted: compensation for victims, a description of the privacy policy and an explanation of what has happened.

To discourage people in making online purchases are mainly the news heard by media, which shows that even the state, symbol of strength and power, become victim of the hackers. An important distinction must be made between real security and perceived security, in fact, the majority of customers do not have technological skills to assess the safety of a website, thus they tend to rely on what appears immediately visible, then the user interface. “To attract and retain e-payment users, it is vital to enhance consumers’ perceptions of security and to maintain customers’ trust during e-payment transactions” (Chellappa and Pavlou, 2002).

The factors that influence client perception for online purchases are: security statement, transaction procedures and technical protections. As stated by Changsu Kim “security

statements refer to the information provided to consumers in association with EPS operation and security solutions. Technical protections refer to specific and technical mechanisms to protect consumers' transaction security. Transaction procedures refer to the steps that are designed to facilitate the actions of consumers and eliminate their security fears".

According to Culnan and Armstrong, customer perception of security is positively correlated with both technical protections and security statements. In line with Taylor Nelson Sofres Interactive, two main factors tend to block people from making purchases online: disincentive to give data related to credit cards and the idea that it is less risky to buy in a physical place than online. On the contrary, CIB (2013) say that most people do not buy online because of the spam. According to the study conducted by Carlo Flàvian, the level of customer confidence depends on the proper management of legislative, technical and business measures. According to what emerged, the priority of companies must be to increase the security and privacy of communication. There are two main actors in this work: public and private. The former with legal measures and communication policies, the latter through technical measures aimed at "security in e-mails, coding or anonymous surfing, among other issues" (Carlo Flàvian).

1.3 Cyber weapons and related damages

In line with the research conducted by the FBI, 90% of companies received an attack in the previous 12 months and 80% of them suffered financial losses, this data is really important because stresses the success rate of cyber criminals. The 78% of companies interviewed said that the attack was due to the human error of their employees, demonstrating that the weapons used, to a greater extent, tend to exploit the lack of cyber training within firms. The impact of a cyber attack in small businesses is devastating, the average loss is $180.000 and 60% of them fail within six months from the attack.

"Executives have difficulty gauging potential impact partly because they are not typically privy to what their peers struggle with as they work to get their businesses back on their feet. An accurate picture of cyberattack impact has been lacking, and therefore companies

are not developing the cyber risk postures that they need," said Emily Mossburg, principal, Deloitte & Touche LLP.

Companies can receive different kinds of attacks, partly for this reason it is difficult to defend themselves; "malware" is the main tool used by Cyber criminals to steal resources from firms, it includes different category of software that behave like vehicles to access, control and compromise the information contained inside a computer. In order to operate, malwares need to be installed, thus attackers can use different methods to reach their goal such as bring the user to click on a link or open an attachment, this strategy considers that in order to induce someone to open a link, trust is necessary, so hackers usually send an email that appears to be from someone that the user trust.

SQL is a programming language used in database management, in fact many servers host critical data and through SQL is possible to put all of this data inside databases. The second type of attack analysed is the "SQL injection", in this case malicious codes are introduced into these servers enabling the divulgation of critical information to the attacker. Similar is the Cross-Site Scripting(XXS) which introducing a malicious code in the website, has the objective to hit the user accessing to all his private records. Usually websites are built to keep a certain amount of traffic; another category of weapon is the Denial of Service(DOS), in this case the traffic increase to unsustainable levels making the website unavailable for users.

The last kind of weapon mentioned is the "Session Hijacking"; when a user browse on internet, a binary relationship is created between computer and remote web servers, in this way, information and authorization are exchanged by recognizing the computer ID, with this kind of weapon, the attacker can capture the ID and freely approach to the user data.

The incumbency of these threats can cause firms an innumerable variety of damages, first of all the loss of electronic data, indeed, inside the infected computer there could be confidential information of the company, such as lists of suppliers and customer or in case of hi-tech startups proprietary algorithms, whose spill could put at risk their business. In this set of impairments are included the extra expenses such as the physical damage of the hardware or the restoration of the network infrastructure that remains broken from the incident; the previously mentioned Denial of Services attack makes the network unavailable for as long as necessary to be restored, in this circumstance clients cannot

take advantage of the products or services and usually contact someone else, bringing inevitably for the firm a loss of both income and customers.

Data theft is not always aimed at acquiring information regarding the company, but often it is directed to the theft of information held by the company about third parties like customers and suppliers, inevitably this creates them a serious damage and a lot of times they decide to sue the company, thus among the costs related to Cyber attacks we need to take into consideration also the privacy lawsuits.

The lost of reputation is the main collateral effect of IT risks, indeed, Cyber attacks can seriously damage the health of startups because customers can decide to switch to a competitor because they feel more secure. The CEOs of Clinkle, HB Gary and Snapchat have been vilified in public following the theft and publication of embarrassing emails.

Beyond those listed there are a number of other costs incurred by companies following the Cyber attacks, these are expenses that are not visible from the outside, in line with Deloitte the main hidden costs are: insurance premium increases, increased cost to raise debt, loss of intellectual property (IP) and the value of lost contract revenue. The visible costs associated with data breaches represent only 5% of the total cost, in fact for 95% they are represented by hidden costs.

Usually after receiving an attack, the target companies declare a share of figures that is only 10% of the total, in fact, according to Deloitte, 90% of the damage is visible after a period of 5 years.

At this stage the role of marketing is fundamental in restoring trust to customers.

1.4 Cyber defence strategies

Traditional policies don't cover any more companies from the risks related to the Cyber Space, in fact the concept of property is changed: while until the period before the advent of internet, firm's asset revolved around infrastructures, desks and other movable and real estate assets, with the advent of E-business the main resources held by companies are information and software, for this reasons traditional protection tools no longer have an effect.

As stated by Bruce, Hick and Cooper, information represents the most valuable commodity, in every industry the right data is priceless. According to the IBM's study of 2015 the costs related to a computer intrusion have risen by 6% from 2014 to 2015; unfortunately protecting company's information is really expensive, principally because a good protection mechanism requires the combined use of multiple systems such as employee training, strong networks and different levels of authentications in order to access to the information system. On the other side, information's exchange among companies gives the possibility to reduce security expenses, having the opportunity to be aware of a weapon or a mode of attack from those who suffered it, gives the possibility to prepare an efficient defensive strategy. This methodology seems to be in line with small firms business model for two reasons, the first one is the cost factor, the second is the locations in which startups operate, usually co-working places where information sharing is favoured. One of the main aspects for companies to start cooperating is the mutual trust, since data about internal security systems is often disclosed. However, information sharing needs to be structured and coordinated and for this purpose standardization bodies, including NIST, ITU-T and ISO (2012) have established national cyber security centers.

In line with this view Tankard said that "Typical commercial off the shelf(COTS) virus scanner and firewall systems appear incapable of sufficiently protecting against APTs",

NATO and European Union have signed an agreement for the exchange of information and best practices to better face the risks associated with the Cyber space; the attention given by the US to this issue is highlighted by the document "Future years defence program" in which was stressed that Cyber security spending requires more

consideration. It is realized that for many companies, especially small and medium sized ones, due to the lack of resources necessary to face the problem, a state intervention is indispensable.

On the other hand, David Cowan emphasizes that SMEs would be advantaged from adopting Cyber defence practices being able to boast a smaller attack surface and a manageable number of devices to track. In line with this view, in order to better cope with IT risks, it is fundamental a strong corporate Cyber security cultures and startups with small teams would be better able to guarantee a culture of high awareness and focus on security, "Thousands of decisions are made every day. Culture is how you, as say a leader of the company, are confident that every one of those decisions is the right one", Jeff Lawson, founder of Twilio. According to this school of thought it is vital to integrate cyber security both in planning and implementation activities, investing in employee training, especially taking in consideration that most of the attacks derive from human error, for this reason every company should teach its employees how to prevent the attacks and how to respond in case of accident. The third step is to place emphasis on data privacy, each firm should conduct a privacy impact assessment classifying the data held and implementing for each data category defence measures. "Our users do that by default, they ask a lot of questions about how we store data, how we process it and so on. That's why we are very transparent regarding these topics, we make the way we deal with data public, both in our FAQ and our Transparency Report" Robert Knapp, CyberGhost.

Hackers, before every attack, make a cost-benefit calculation in order to understand if the potential victim is profitable; it is due to this fact that the "deterrence" is a defence tool particularly discussed in recent years, indeed, it represents a procedure designed to discourage Cyber criminals from carrying out attacks. Deterrence is a relatively cheaper system that would not only benefit states and large companies but also small businesses that have limited assets to deal with Cyber risks. This approach is articulated in different elements: first of all the "interest" from keeping the attackers away, the assumption is the cyber awareness inside the company, the second element is the "deterrent declaration" in which are expressed the consequences deriving from the violation, the third element are the "penalty measures" that are set by the state, the fourth element is the "credibility" for which we mean the ability to enforce the deterrent declaration and finally the "cost-benefit calculation" in which possible losses are weighted.

The Israeli information security office, proposes a cyclical defense model for companies, in fact the external environment tends to change continuously and therefore a constant change is required by startup to assess the existence of new risks. The cyclical process is divided into 3 parts: "Planning and assessment", in which are assessed the objectives and resources that are available for the defense, "Execution of the plan", in which the scheme previously established is adopted and developed inside the company and, to conclude the last step, "Maintaining up to date defences", in fact given the changing environment, the weapons used by Cyber criminals change constantly and therefore the same must be done for the firm's defense tools.

From a practical point of view, the first step to ensure a good defense system must be on the management side, in fact the company's managers need to possess a strong awareness about Cyber threats. Secondly, a series of technical measures must be adopted in order to implement the plan established by top management, including: protection against malicious code through the use of technologies to cope with malware and the ecryption of remote access of employees and suppliers using commercial encryprion means. Especially for suppliers it must be requested to comply with software and data protection standards.

Another fundamental step is to protect the company's existing data from external theft through measures to avoid the theft of startup's personal information. With regard to hardware devices, computer protection is possible through the periodic change of access passwords, the removal of unnecessary software and the exclusion of superfluous admin accounts. On the other side, regarding human resources, given that most attacks derive from human error, it is crucial to educate the employees and remove former dependent's authorizations. To conclude the last two key acitions stressed by the istralian ministry are: to ensure the security of the network to prevent it from being subject to denial of service attacks and the cancellation of superfluous information.

1.5 Barriers to good security behavior

In this section, I decided to analyze what are the main barriers that would brake small firms from adopting appropriate behavior for the Cyber space.
The first factor that I want to observe is the risk awareness of companies, in my opinion, it is directly correlated to the technological skills of the startup, in fact, the lack of knowledge of the Cyber threats leads to a wrong assessment and therefore to a lack of adequate measures for Cyber protection. On the other side, there may be a risk awareness, but also a lack of information about the tools to prevent breaches, even in this case, it is possible to talk about low awareness.
In line with Adams and Sasse, insufficient awareness of security issues directs small firms to adopt inefficient protection models.
The second key factor that I decided to analyze, following the paradigm of Sauvik Das, is the lack of motivation. This aspect tends to be more present in startups, where every resource, being scarcely available, must be directed to the core business. For this reason an investment in Cyber defence is usually seen as an inefficient investment. To make a comparison, imagine to insert in your e-mail account a password of 20 characters, this certainly makes the system well protected, but on the other hand it would makes the access slower, in fact, the probability of error in entering the password would be greater and therefore it would increases the time required to access in your e-mail.
Harley argues that another factor that undermines company's motivation to adopt cyber security practices is the cost-benefit consideration. For costs I mean both money and time, for benefit I intend the probability of expected loss, which being considered very low, would discourage companies from adopting instruments of production.
The third element to consider in order to measure the Cyber security sensitivity, is the firm's knowledge, in fact often the tools that need to be used are complex and therefore companies, even if motivated, do not possess the specific knowledge to be able to put them into practice. According to Sauvik Das, the security sensitivity of companies could be increased through games for Cyber defence education and more effective user interfaces for security tools. Particularly interesting is the relationship between social influence and security adoption, according to Sauvik Das, Social factors are the key

drivers for behavioral change in Cyber secuirity, for example a partner that changes its standards could act as a social catalyst for security related behavior.

1.6 Legal framework and regulations

On one hand, regulatory interventions can result in friction for startups, forcing them to use resources for activities not directly correlated to their core business; on the other hand could be very useful for small businesses, which due to the lack of resources to defend themselves, need a state mediation.

Among the interventions in Europe aimed to protect the data systems security, the NIS directive emerges, it is directed to suppliers of essential services and digital services with the goal to create standard requirements for the management of information services; this will allow European companies to operate in a non-fragmented environment facilitating their adaptation to the directive.

The subjects considered by the ordinance have to adopt technical-organizational measures aimed at managing IT risks. The European framework revolves around three pillars, the first consists in “National capabilities”, which underlines that each state must have certain specific national cyber security capabilities such as national CSIRT and cyber training practices. The second pillar involves the “Cross border collaboration” between European countries and aims to exchange the best practices, finally the third pillar revolves around the state’s supervision activity towards critical market operators.

In order to stimulate the strengthening of the Cyber Defence, the European commission, investing 450 million, has established a Contractual Public-Private Partnership(cPPP), organized both in a public part, represented by the European commission, and in a private division, characterized by the European Cyber security organization. The cPPP is instrumental in the coordination of resources for the Cyber defence in Europe, with the main purpose of stimulate the cooperation between public and private companies; within this partnership are included research centers, innovative SMEs and critical infrastructure operators.

On 25 May 2018 the GDPR legislation came into force with the aim of standardizing the policy of personal data within the various European Union countries. The objective is to regulate not only information's management but also the conservation, the confidentiality and the cancellation if requested by the interested party. The legislation speaks about objectives to be achieved but leaves wide discretion to companies as regards the tools to be used. Companies are required to have an expert in the field of data protection, the data protection officer (DPO). Being aware of the fact that make 100% data secure is really hard, especially if we are talking about small companies, GDPR's goals are aimed to reduce the risk exposure pushing firms to collect only strictly necessary data, using them only for specific purposes and deleting them when they are no longer useful. Failure to comply with the law brings sanctions of up to 20 million euro or up to 4% of the turnover of the previous year.

In US, regulation is fragmented by industry, health care providers are expose to a series of requirements when they threat confidential information about patients, in fact they are subject to the Health Insurance Portability and Accountability Act ("HIPAA"); on the other side bank customers with the Gramm-Leach-Bliely Act have different privacy rules regarding banking data, while with the Fair Credit Reporting Act ("FCRA") is regulated the protection of financial data.

In Italy the national plan for cyber protection aims to update the DPCM Gentiloni by easing the methods for responding to cyber crisis in order to streamline the decision making process. In order to strengthen the defence mechanism, the Computer Emergency Response Team(CERT), the structure that deal with prevention and assistance on the risks deriving from the Cyber space, is unified. The main features of this model are the certification of ICT tools, the cooperation between public and private sectors and the creation of academic programs directed to innovate existing defence systems.

1.7 Game theory applied to Cyber Security

The World Wide Web, due to the multiplicity of holes in which hackers can creep, presents high vulnerabilities to cyber threats. Using the game theory the aim is to find the perfect allocation of resources and time between the different tasks in order to prevent attacks. This approach describes the possible multi-person decisions that can be made in order to ensure the best possible reward for self, anticipating the rational decisions of the other actors involved. The basic characteristics of each game are: multiple players, competitive in nature, rules that guide every game and payoffs for players. The objective of applying the game theory to cyber security is to identify the nature of the conflict since the attacker's decisions are related to the choices of the defender. What is difficult to estimate to traditional defence mechanisms are all the possible combinations of threat scenarios; on the other side the game theory allows to do it through computers that analyse the different combinations to find exceptions in the general rules. Theorists have adopted several applications of this approach: Markovic and Reither analysed a sample of attacks(DDoS) and related strategies in order to find recurring patterns in these attacks, this can help startups to organize prevention activities, concentrating the available resources on systems where the attacks are most likely to occur. Differently, Syverson uses game theory to analyse the errors made by Cyber criminals when they try to enter inside a computer network, this would allow network administrators to create a strategy that can put even more in trouble the hackers. Hamilton, Otto and Sydjari using game theory created a series of scenarios suggesting several courses of actions with predicted outcomes and what if scenarios, in this way companies will be able to evaluate, making a cost-benefit analysis, in which cases defend themselves is economically efficient. Chen applies the game theory to design the response to the importance-scanning internet worm attack. The defender has the goal of minimize the propagation speed of the worm, so he will look for the best way to deploy an application; on the other hand, the attacker must aim to maximize the propagation speed of the worm by choosing the optimal scanning distribution. This is a zero-sum scenario featuring two players, "the optimal solution for this problem is that defender should deploy the application uniformly in the entire IP-adress space or in each enterprise network, so that the best strategy that the attacker

exploits is equivalent to random scanning strategy, this work gave a game theoretical framework to design the locations of vulnerable and high value hosts over a network". Sum et al. decided to focus on the need of companies to invest in Cyber security, then develop a scenario characterized by two companies investing in cyber security, presenting a pay off matrix, he did the analysis of the Nash equilibrium and introduced a penalty parameter associated with the not investment option. Using the Sum et al. model, startups that operate in different industries are able to understand which business sectors may require greater investment in cyber defence, this would help them to increase the resources focus only where necessary.

CHAPTER 2

BUSINESS MODEL DETERMINANTS

2.1 Online business overview

In order to understand how startup's business model changes in front of Cyber threats first of all I need to identify the concept of business model, for which, in line with Amitt e Zott, it is the unit of analysis that captures the value creation potential deriving from the design of transactions between the company and all the other outsiders such as partners, suppliers and customers. As stated by Teece, business models represent the logic by which firms creates and delivers value to customers, according to this view, the value captured by companies is the essence of the business model. Business models are characterized by three principal vectors: customer interaction, asset configuration and knowledge leverage. All of these pillars design the strategy of the company. Timmers classifies business model as an "architecture for the product, service and information flows, including a description of the potential benefits for the various business actors, and a description of the sources of revenues".

Today the greatest percentage of enterprises operate in the "E-business", for which I mean the online business, therefore the business that is done through the Cyber Space. The growth of E-business was without precedent, the greatest share of companies that 10 years ago operated offline today have an online store, in fact by 2002, 93% of U.S. firms have some fraction of their business on Internet. There are several returns in operating online, Lord, et al. said that E-business gives the possibility to reduce overhead expenses and small scale inefficiencies increasing the efficiency; furthermore it drives a huge increase in the scalability of startups, just thinking about the unicorns born less than 15 years ago, such as Facebook, Uber and Airbnb, all of them is an online business. On the other side, the main threat related to online firms is the Cyber risk, that can destroy the main element related to the business survival, the "customer trust"; in emerging entrepreneurial realities it is the principal reason of low electronic commerce adoption, in fact often startups, given the lack of necessary resources, are not able to defend themselves with the traditional

Cyber defence tools adopted by large companies, thus they are forced to adopt more drastic solutions, such as changing their business model.

2.2 business model adaptation versus business model innovation

There are two central theories that allow me to measure the degree of propensity to adopt disruptive business model solutions in order to take into account all of the possible firm's behaviour.

On one hand the threat-rigidity theory argues that risks lead managers to apply existing routines while opportunities stimulate risk taking actions. In these occasions, the past behaviour tends to influence the decisions of the company, which will coincide with solutions already used and internalized by the firm. The better fit with this theory is find in large companies, which being equipped with both past experiences and resources are less disposed to change their business model in front of IT risks. On the other hand the prospect theory supports the opposite, in fact in this case, in risky situations managers tend to make resolutions that involve more hazard. According with this view, people are more susceptible to losses than risks of the same scope, so in situations that can lead to losses, they are more driven towards a risk taking behaviour. This kind conduct is seen more in companies that have poor returns, in fact they would adopt this behaviour because have little to lose (Bowman, 1992). In line with Teece, companies that are constantly looking for new business opportunities are better able to adapt to changing their business models when they encounter threats; in fact many firms fail precisely because use the same model for too long while today there are many discontinuities and disruptions and it is required more often to change really quickly business model. According with the prospect theory, startups, having less to lose in terms of resources and not being able to count on routines like big companies, ahead of a Cyber risk are more prone to vary their business model.

The changes in the business model is not only driven by the management's decision to innovate it, but also from its adaptation to external factors like Cyber threats.

For business model adaptation we mean the process by which startups change their business model aligning it with the external factor. Rapid learning and the capability to adapt to market changes are the basis of the business model adaptation, which in accordance with Saebi, consists in the continuous research, selection and improvement based on the surrounding environment. Two key elements describe the business model adaptation: “effectuation” and “experimentation”. The effectuation theory holds that given the uncertainty and the unpredictability of the environment startups are not able to plan the adaptation process, subsequently small companies usually take decisions step by step. Supporters of the experimentation research see the business model as the result of a trial and error process. Although startups, in relation with the prospect theory, are simplified in changing their business model in front of Internet menaces, they may fail before they have the possibility to change. The ability to adapt to Cyber risks depends on two main circumstances: first of all the awareness that companies have about the threats related to Cyber space, second both routines and strategic orientation developed over time can restrain this change. In order to survive to external threats firms can employ as well as adaptation also business model innovation, in which

top management plays a more active role creating disruptive business models that influence market conditions. Business model innovation is often used by firms to overcome periods of crisis due to both external and internal factors, through innovation for example is possible to reduce costs and acquire new customers. The main difference between the two models is that in occurrence of business model adaptation, the change is driven by surrounding factors deriving from the external environment; in the case of business model innovation, the change can derive from both internal and external factors. The main drivers behind the business model adaptation are the external stakeholders, regulatory forces and technologies; furthermore the more drastic is the threat and more likely companies are inclined to business model adaptation. The transition from one model to another implies a temporary decline in performance for companies, also because often they have to change market segment, value proposition and value chain; business model adaptation is a “risk taking behaviour” since it often involves changing routinely patterns of action often with an uncertain outcome. Especially startups, have “little to lose” and then reconnect to the prospect theory, in front of a threat they will have a more

risk-taking behaviour and then respond with the business model adaptation (T. Saebi et al.).

2.3 Strategic agility

According to Miles et al. (1978) and Chattopadhyay et al. (2001) is possible to differentiate the strategic operation of a company in market development and domain defence. In the first case, companies are more active in exploiting market opportunities and therefore tend to collect a greater number of experiences and routines that allow them to change their business model following the needs of the environment. This vision is in contrast with the threat-rigidity theory, which stresses that routines hinder business model change.

"In contrast, firms that emphasise domain defence attempt to maintain their territory by engaging in competitive pricing and developing a single core technology that is highly cost efficient" (Miles et al., 1978), so in this case companies will try to lower prices and minimize operating costs. In line with this view, "Domain defence" and objective relationships with suppliers, customers and partners are the main obstacles to business model change. Doz & Kosonen in order to highlight the concept of business renewal, have built a strategic agility framework which conceptualized strategic agility as the "thoughtful and purposive interplay on the part of top management" between three meta capabilities: the "Strategic sensitivity" which represents the attention that companies place on the opportunities and changes that the market put in front of them. This factor, is principally driven by the location in which the company operates, in fact be close to research centers or technology poles can question startup's business model by molding to what the surrounding environment offers. Startups compared to large companies present this factor to a greater extent, this is due to the fact that they largely work in accelerators and co-working spaces in which the exchange of feedbacks and information make them to acquire "Strategic sensitivity". The second meta capability is the "Leadership unity" for which we mean the ability of top management to make quick decisions. Finally

"Resource fluidity" that is the ability to transform the structure of internal resources in order to implement changes.
In line with Doz & Kosonen, small companies tend to present these three meta capabilities more than large companies because of their light organizational structure and thus are more prone to change their business model in front of Cyber threats.

2.4 Dynamic capabilities

For dynamic capabilities I mean the company's capability to build, integrate and reconfigure its internal resources to accommodate change in the external environment; for this reason, they are vital components of the business model, in fact these represent the opportunity for small companies to redesign their business model in front of cyber risks. According to Helfat, dynamic capabilities denote the ability of firms to develop new products capable of responding to new market needs. Griffith and Harvey define them as combinations of hard to imitate resources that bring the competitive advantage.
The set of capabilities that these companies possess are divided into two levels, the ordinary capabilities that encompass routines activities which allow to pursue a given production program, and on a higher level, we locate the dynamic capabilities, which are divided into two categories, the "micro-foundations" which consent to make decisions in situations of uncertainty and include the development of new products and the opening of sales in new markets, and the "high order" dynamic capabilities that "devise business models for the future"(J. Teece). Companies that have weak dynamic capabilities are more likely to implement solutions based on past experiences and therefore change their business model is much more complex, according to Argawal and Helfat "Transformation must be a semi continuous activity".
The role of dynamic capabilities varies according with the dynamism of the market; in moderately dynamic markets, for which we mean the markets in which continuous changes occur but in a predictable way, they can be assimilated with the routines through which it is possible to obtain new strategic configurations in line with market movements, in this case the dynamic capabilities are strongly based on past knowledge. In high

velocity markets, dynamic capabilities take the form of a process aimed to quickly acquire, test and adapt new knowledge; the output in this case is unpredictable, therefore in line with Zahra et al. dynamic capabilities are more important. In high velocity markets, dynamic capabilities rely less on prior knowledge, therefore, according with this purpose business model's change is simpler for startups, even Autio et al. argues that younger companies have a learning advantage as they have less to unlearn. On the other side Zahra et al. highlight that the development of dynamic capabilities requires internal resources for the firm and therefore large companies would be more favoured, in fact startups, having less resources to plan carefully, tend to rely more on improvisation in line with Moorman and Miner which claim that the memory organization is inversely proportional to the degree of improvisation.

The creation of new knowledge is highly influenced by the environment and by external relations of the company, Powell et al. (1996) highlights the connection between business alliances and superior R&D performance in biotech firms, in fact the exchange of information leads to the development of dynamic capabilities. On the same line of thought Aldrich shows that imitating the best practices of other companies can lead to compensating the lack of knowledge in startups.

The entrepreneurial activity, more present among components of small firm's team, plays a fundamental role in stimulating the organizational learning and selection of internal resources; this process increases the organizational knowledge and the development of substantive capabilities, which, in turn, through the development of dynamic capabilities, increase the company's performance, influencing positively entrepreneurial choices.

In order to make the transition from a business model to another possible, it is necessary that all the elements within the business model are in line, in this way the implementations within an organization of elements that consistently reduce cyber risks need to be aligned with the company's financial and human resources. Given the presence of less re-engineer assets, for startups the transformation is much simpler and faster, but on the other side according with Teece, multinational companies due to the fact that operate in different states, very often use different business model, sometimes forced by the regulations of each country, and therefore are more likely to validate models and implement them to facilitate transformation.

2.5 A change in the business model components

In previous paragraphs we realized that small companies in conditions of high risk are more likely to switch their business model than large companies, in this section we will try to understand how it could change. Taking into consideration the "business model Canvas", we will contemplate the change of some areas in line with what is expressed by literature, in doing so, the effects of each area on the others are not considered, but according to Doz and Kosonen, components of the business model do not have the characteristic of modularity, so a change of a single element also causes consequences for others.

As stated by the proponents of system theory, the concept of "Key partner" with the advent on Cyber risks will start to include competitors, apart of course the outsiders such as suppliers, allied companies and all the other subjects with which currently firms cooperate in order to create value. In fact, small companies are beginning to give partners access to company information, this give the possibility to cooperate in order to acquire knowledge to better face Cyber threats, according with Steven Jonson "You have half of an idea, somebody else has the other half, and if you're in the right environment, they turn into something larger than the sum of their parts".

On the other side against the system theory the greater share of literature points to a decrease in future cooperation among companies, in fact the share of information with "Key partners" is seen as a potential damage for the firm because a Cyber attack facing a partner, would jeopardize the company's security, thus in line with this view small companies are starting to cut relationships with firms that are not sufficiently reliable and does not respect Cyber defence standards; this theory of thought focuses more on technological defence tools than on methodological ones.

As regard of "Channels", along with a study conducted by Deloitte, shoppers are increasingly hesitant to make online purchases, especially if we are talking about web sites that are not known and that could be poorly protected. Between 2015 and 2016, 31% of US customers have cancelled applications from their smartphones and 27% usually avoid web sites that do not give them an idea of reliability; for this reason many startups have been forced to close their sales channels, putting their products or services on third

party channels like Amazon, this obviously increases the costs for small businesses that now are forced to pay commissions, consequently literature stresses a shift from direct to indirect sales channels, thus driving the business model adaptation due to the external factor.

Companies very often hold valuable information for customers, such as banking accounts, therefore, regarding the "Customer relationship" area is really important to create and maintain shopper trust through careful communication.

According to a PWC study, 69% of customers believe firms are vulnerable to Cyber attacks and in particular startups represent one of the last categories of corporate forms for degree of trust, with an only 5% trust. These data lead small companies to focus more on the relationship with the customer, increasing marketing costs thus the goal will be to communicate with the community that you are protecting both his information and privacy in line with the CEO of Rock Security "think about people as people, they want answers and want to know their company is being forthright and careful about information". The trend is to manage the relationship with the shopper, moving from a self-service approach to dedicated personal assistance in order to increase customer confidence.

The last business model's area mentioned by literature take into consideration "firm resources", the main assets of startups correspond to patents, technologies and human capital. Given the IT risks arising, companies are tending to put barriers and restrictions on the use of technologies and licenses by employees, in order to keep them secret. As stated by Deloitte, this behaviour will obviously lead to higher costs for the business, according to Samsung "Organizations pro-BYOD policies save an average of 17% per year on their bill communications". Secondly, these barriers will slow down the systems, creating administrative burden and harming company's flexibility. Third, employees, having IT restrictions, will tend to find ways to overcome the problem, creating greater risks for the company. Among the company's resources there is also the human knowledge, according to the system theory, companies will increase their investment in Cyber awareness training their employees and in order to reduce costs and duplication of efforts, therefore the various areas of the business will be in constant communication through a feedback-based system.

CHAPTER 3

METHODOLOGY

3.1 The case study approach

The purpose of this thesis is to investigate how the small firm's business model changes in consequence of the advent of Cyber risks. The first two chapters concern an analysis of the existing literature about Business model and Cyber security but, since the previous literature is limited in providing answers which are relevant for my research question, I focused on the inductive theory building using embedded multiple cases.

Originally, concepts were generated taking into account only the previous writings, but this involved testability problems, for this reason using the case studies approach, the theory is more reliable, in this way I am able to test the principles at the time in which I create it, according to Glaser and Strauss(1967) the close connection with reality makes possible to generate a valid and relevant theory, in fact the basic principle of the research method that I used has a scientific foundation, "in line with Kuhn, in normal science, theory is developed through incremental empirical testing and extension".

The case study as a research method has been developed to overcome the limitations deriving from the quantitative approach in the understanding of the company behaviour, in particular researchers using this method have the possibility to adopt a holistic system that allows to go deeper with the analysis. Yin defines the case study research method "as an empirical inquiry that investigates a contemporary phenomenon within its real life context; when the boundaries between the phenomenon and the context are not clearly evident; and in which multiple sources of evidence are used".

In my exploration, the existing literature is exploited with the aim of giving greater strength on what emerged in case studies, furthermore it will allow me, in case of disagreement with what has been discovered, to look critically at the results obtained.

Despite all the advantages, I evaluated also the complications related to the Eisenhardt model: first of all the complexity of the theory generated, due to the large amount of details present in the case studies, moreover the fact that not being used quantitative data

there is the risk of failing to identify the most important findings; but as we will see in the paragraph “data analysis”, using the within-case analysis I am able to eliminate these two negative effects.

3.2 Cases selection

A fundamental aspect of this methodology is the selection of the representative sample of the population, in fact, through this it is possible to make the research applicable to all the small businesses.

Due to the variety of the firms, I had the possibility to choose a random sample, but in this way, I would not have taken in consideration some important variables for my research. Jason Seawright and John Guerring led two Monte Carlo experiments, “in the first experiment, a computer generates five hundred random samples, each consisting of one thousand cases. In the second experiment, the computer generates five hundred random samples, each consisting of only five cases”, the investigation clearly highlights the impartiality of the sample, making it unrepresentative of the population. This is perfectly in line with what was declared by Pettigrew(1988) who argues that given the extreme unpredictability of situations, it is preferable to choose polar types of sample in order to create a “transparently observable” theory.

In order to respond more specifically to the research question, the first factor taken into consideration to design the sample was to isolate the research only to small companies. On one hand if the specificity consents to have greater focus on the research objective, on the other hand the generality allows to create a valid theory, in fact, taking into account as further variables the date of establishment of the company, the turnover and the technology adoption level I am able to search for a recurring pattern that applies to all the small firms.

Using these variables, I want to cover all the categories of small companies in my research with the aim of creating a system that can be applied on a general scale.

Being confidential information, the firms interviewed asked me to don’t show their name, so I will call them Y,J and K

Y is a Russian company founded three years ago, it operates in the field of Cyber security proposing facial recognition systems based on neural network, these services are aimed at firms interested in both security systems and customer behaviour understanding. The team consists of 50 people and the main customers are not only private companies but also public ones. Choosing Y, I want to represent all the technological startup with the highest turnover and with the greatest cyber defence capacity due to both the technological factor and the economic factor.

The second company I interviewed is J, it is a 4 person architectural firm whose turnover doesn't exceed 200 000 euros per year. J was created 20 years ago and it is characterized by low technological adoption, in fact, its core business concerns construction engineering works for companies such as ENI, ACEA and Italgas.

J falls into the second category of differentiation, indeed, it embodies all those firms that present weak cyber defence capabilities due to the low technological level and the scarce resources possessed.

The third company examined, which I will call K, has been created six months ago from a university research, the team is made up of seven people and it offers IT consulting services for small firms. K presents high technological adoption, while the turnover until today is almost zero still being in an initial phase of customer acquisition. The newly established startup is representative of the third classification of small companies, for which we mean all those companies that, despite having an high technological level, may have difficulty in defending themselves from cyber threats due to the limited resources possessed.

3.3 Data collection

Data collection is the process of gathering information from relevant sources in order to find answers for the research question. For this section, I decided to use the interview, in this way I have the opportunity to investigate issues in a depth way obtaining a high response rate. Companies were contacted via email, they were both specified my research question and asked the possibility to do a telephone/in person interview. I carried out a

40-minute face to face interview in which participants were asked to answer to 17 questions. The interviewed figures all belonged to the firm's top management, this allowed me to reduce the possibility of errors deriving from the lack of knowledge. Both closed and open questions were used in order to collect more data, in fact giving the possibility to answer in an open way offers me the occasion to grasp details that I had not foreseen. The first demands were aimed at gaining confidence with the interviewees, indeed they were asked about the company's business model and the type of activities carried out; subsequently they were requested more detailed evidences about the confidential information processed, the defence tools used and the previously received Cyber attacks. In order to measure the propensity to change the business model were asked to the firms about both the investments in cyber defence and the customer's trust in the purchases on the proprietary channels. Considering the scarcity of resources in small companies, I wanted to verify if they had adopted other tools to deal with Cyber threats, so finally I asked them about forms of cooperation with other companies and about the team composition.

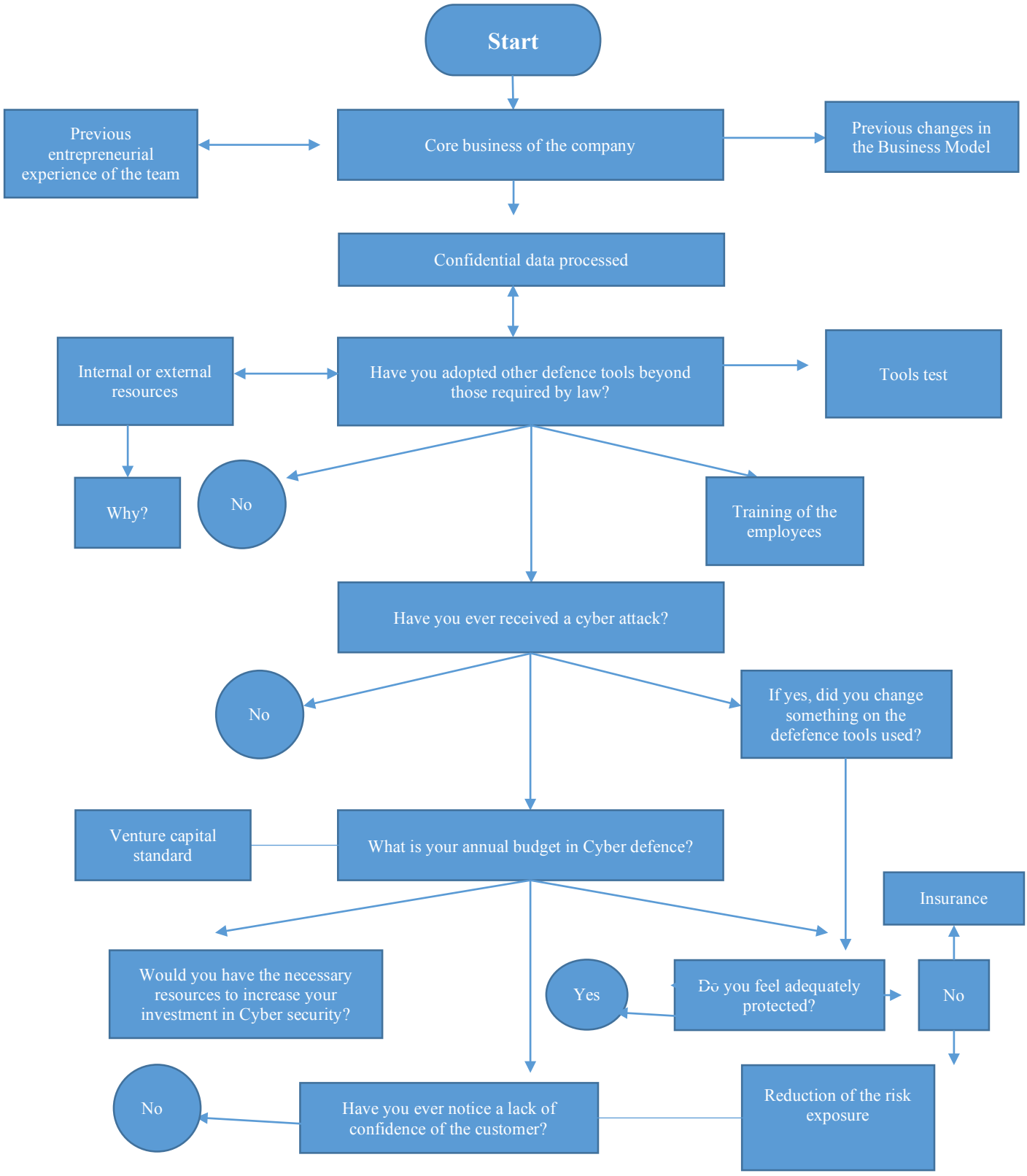
Interview Questions
1) What is the business model of your company?
2) What kind of confidential data do you process?
3) Have you adopted other defence tools beyond those required by law? Which one?
4) Have you ever received a cyber attack? After the attack did you change something in the defence tools used?
5) Are the security systems in your possession tested on a periodic basis? If so, how often?
6) For the cyber defence tools have you developed internal resources or do you rely on third parties?
7) What is your annual spending on Cyber security? Would you have the necessary resources to increase your investment in Cyber security? Do you think you are adequately defended?
8) Have you ever notice a lack of confidence of the customer in making payments on your website or in giving you confidential information?
9) Would you be willing to change sales channels(sell on third party platforms rather than on your on) to reduce risk exposure?
10) Do you require cyber security standards for partners(such as suppliers and allied companies) which hold your data?
11) Do you adopt forms of cooperation with other companies regarding cyber risk prevention?
12) Have your employees received training on the risks related to cyber attacks and how to prevent them?
13) Have investors ever asked you for any cyber security standard to adopt?
14) Do you already have or plan to have insurance from cyber risks?

15) What is your annual growth rate in terms of turnover? Has your business model changed from the creation of the company to today?
16) How many people are your team made up of? What is the education level of the top management?
17) What are your company's priorities over the next twelve months?

3.4 Data analysis

Qualitative research implies the ability to interpret the information collected, in doing so the researcher first of all has to distinguish between general cases and particular cases, the latter has little relevance because it do not lead to create a theory generally valid.
The analysis of the data is a fundamental step for the methodological system that I have chosen, through the interviews conducted, I manage to obtain a huge quantity and variety of information; Pettigrew said "death by data asphyxiation", in fact it is really important to order all the facts acquired. The within-case analysis is a fundamental tool used to group the information obtained, in fact I have treated each case as a single entity, marking the findings for the variables I wanted to analyse, this allowed me to gain even more confidence with individual case studies. Having explored the individual cases, in a second step with the cross case analysis, the objective is to find a recurring pattern, so I selected different sizes for each case and then comparing the single size of a case with that of other cases I have observed intergroup similarities and differences; according with Eisenhardt "the key to good cross-case comparison is counteracting these tendencies by looking at the data in many divergent ways". The comparisons allowed me to analyse the discoveries with greater depth by testing them on the other case studies in order to create a more accurate and reliable theory.
At this point, basic concepts and relationships among the variables have begun to emerge, so with the delineation of the constructs I try to verify the fit between discoveries and case studies. Thus the underlying logic is replication, for which I mean the fact of treating cases as experiments that confirm or disconfirm the theory, those that confirm add validity to the construct created while the cases which disconfirm the new discoveries give the opportunity to redefine the theory.

Through the literature investigated in the first two chapters, I am then able to carry out a further verification, analysing if the emerging theory is in agreement or in disagreement with what was said by the previous theoreticians. This methodological aspect, in line with Eisenhardt, is important for two reasons: first it permits to offer greater validity to the new theory created, second it consents to put into discussion what emerged, offering the opportunity to refine the concepts developed.



(Self elaboration: flow chart for the design of the survey)

CHAPTER 4

EMPIRICAL FINDINGS

4.1 Case study: company K

K is a Russian company created two years ago, today it has over 50 employees located in the main office in Moscow and New York, where is located the marketing team. The startup's core business consists in the sale of a facial recognition software based on the neural network that is provided to customers in the form of SDK (software development kit). Thanks to this technology many needs can be met: face detection, verification, identification, and detection of age, gender and emotions.

The speed of information processing is incredible, in fact the images taken by the camera in half a second are compared to a database containing billions of faces for the identification of the framed subject. VK, the most important Russian social network, allowing to use its own APIs, gives K the possibility to process all the pictures on the website by making VK an enormous database available to K.

The fields of application of this technology are several, the service can be requested by public bodies with the aim of identifying criminals, but also by private companies to observe the behaviour of customers during the purchase phase, such as a supermarket that in order to increase its profitability is interested in understanding the customer behaviour.

K is the most important facial recognition firm in the World with a turnover of more than 15 million euros per year and a growth rate of 350%: this certainly allows it to have sufficient resources to adequately manage with cyber threats. The company's security system is based on two fundamental elements: using and requesting only the strictly necessary informations and constantly investing in Cyber security systems.

Regarding the first aspect, according to what was stated by the business development manager interviewed, clients which get in touch with K are asked to indicate only their email, although not being able to purchase products on the website of K, they don't register their credit card information. The payment system implemented by the Russian

company, in order to ease the size and the criticality of the information held, is based on the classic bank transfer made to K's account.

The confidential information analysed up to now is that external to the company, therefore related to third parties with whom the Russian company interfaces; as regard confidential information internal to the firm, such as the code relating to the owner's algorithm and the information about its financial statement, after being encrypted, are sent to Amazon Web servers in Germany ensuring maximum security. The second factor in guaranteeing success in the battle against Cyber criminals is the constant investment in Cyber security: the company declares that the main tool is the employees training, in fact every single dependent within the firm receives a full instruction on the measures to be adopted to prevent IT risks; in addition, for the internal communications is used Telegram, which is considered one of the safest platforms in the world.

Regarding the figure of the Cyber security officer, companies usually have two possibilities: to recruit external specialists or to use internal company figures. K declares to utilise this second option in line with what the interviewed explains: *"internal offices have higher costs in the short term, but we believe that in the long term this can bring significant benefits to our corporate credibility"*.

Most of the startup employees have an engineering degree, this allows K to be more inclined to technology in adopting protection approaches. The top management members before creating K have led previous business experiences, this benefits their problem solving skills. The Russian firm points out that the conformity with current legislation is essential not only to avoid legal risks but also to ensure more reliability to its customers: K declares that has adopted both the GDPR and the PSD2 regulations.

According to what was declared, the company has never received Cyber attacks and this is due to both the high technological capabilities of the firm and the economic resources used for the Cyber security: in fact, 15% of the profit is spent on IT protection.

Regarding the relationships with external parties, on the client side K requires, for the continuation of the business relationship, strict privacy standards to be respected when customers use its Software Development Kit. On the other hand, with regard to suppliers, K has just closed a contract with a company that deals with the production of surveillance cameras: this has been requested to respect the privacy standards related to product information developed for K.

4.2 Case study: company J

J is an architectural firm based in Rome with twenty years of experience in housing renovations. Since the late 90s it started to receive assignments from the most important Italian corporations for the design and construction supervision for road works and public services, remediation of works made of asbestos, static tests and fire prevention activities in many regions of Italy. The company also deals with consulting for technical regulations (UNI, CEI, UNEL, ISO).

The small architectural firm operates only in Rome, presenting a zero internationalization degree. Until 2001, J had more than 8 employees and an annual turnover of 800,000 euros, but today, as a result of the crisis, the number of dependents has dropped to 4 and the annual turnover has fallen to 300,000 euros.

In carrying out its core business, the firm interfaces both with private individuals and public companies. Regarding the first category, the confidential information treated are few: they only consist in the name, surname and email address of the person requesting the work; indeed, there is not an internal payment system on the website, compensations are made by bank transfer, this obviously guarantees greater protection for J because no data related to credit cards is in their possession.

On the other hand, regarding the works carried out for public companies, J deals with the positioning of public service pipelines such as telephone cables, sewers and water pipes. These information, in the hands of someone with bad intentions could paralyze the critical infrastructure of the city. I asked the head of the company if he was aware of the relevant regulations*: "Up to now I'm only conscious of the directive related to the GDPR. The main problem is that we are not exhaustively informed from the State and our firm has not technological skills, so it is very difficult for us to understand how to operate in order to be protected from IT risks; furthermore not having enough economic resources, it is impossible for us to hire internal figures within the company that deal with this kind of problems".*

In June 2016, the company claims to have received a cyber attack that, entering in the network infrastructure, blocked the access to all the data placed inside computers, paralyzing J's activity for over 2 weeks. The hackers, have asked for a redemption of 300

euros to unlock the access to information, but thinking of incurring in major damages, the head of the firm decided to do not pay them. The data have not been recovered and this has led to a loss of over 20 000 euros, equal to half of J's annual profits.

After the attack, the firm was unable to meet the established deadlines because the data loss forced employees to do all the procedures that were done before the attack for a second time. In this occasion also the damage of the company image was significant, in fact, J had to re-contact all the customers to request the lost information again. Cyber criminals attacked the network using phishing techniques, and these probably lead one of the employees to open an email with an attached link, which initiated the theft of information.

After the incident, more precautions have been taken, bringing to the company an annual cost of 1500 euros in order to install new antiviruses and to adopt systems for storing and copying data; today all this information are contained in a cloud in Germany. While these activities provide J with the possibility, in case of future attacks, to always have a second copy of data within the cloud, on the other hand it does not appear that J have been taken measures to avoid the theft of sensitive information by hackers.

The head of the company told me that after receiving the attack, he asked to other firms operating in the same sector about the protection systems they adopted, but without many results: many of them did not know neither what was meant precisely for “IT risks”.

The employees still do not have training in terms of Cyber security, the main reasons for this choice are two: the lack of encoded resources, and secondly the fact that 90% of the dependents are not graduates and this certainly limits their technology skills. Top management has had no previous business experience, this certainly discourages change, in fact the head of the company declares that they would not be willing to change sales or commercial channels to reduce risk as they consider themselves protected enough.

The priorities declared by the company in the next twelve months consist in the investment in marketing activities to look for other business opportunities.

4.3 Case study: company Y

Y is a company based in Rome created six months ago during a university research. The mission of the startup is to innovate in the field of CPU processors proposing a hardware accelerator able to process more information in less time and consuming less energy than standard CPU processors. The advantages of the product are not just these, in fact the cost of realization is much lower than the solutions put on the market until today. The universality of the application field is another feature of the CPU born from this startup: particular utility is found in the aerospace sector and in the green economy, due to the energy savings guaranteed by the processor. Companies that interface with Y are small and medium-sized enterprises that offer IT, telematics and telecommunication services.
In carrying out its operations, the newly established firm comes into contact with the confidential information of companies for which it advises, including network architectures and access keys for the development of software applications. To protect this data, the technological tools mainly used are: the configuration of firewalls, which allow to protect points of interconnection between two networks; the use of antivirus and the introduction of complex passwords in order to be protected against brute force attacks. Furthermore, every week is made a meeting regarding the IT security of the firm.
The team of Y is made up of 7 engineers, 3 of them with previous entrepreneurial experiences. The technological capabilities obviously help the company in training its employees on the behavior to be adopted to prevent the Cyber threats, in fact according to the interviewed, Y does not need external consultants in the field of Cyber security as each individual member of the team has the basic notions to avoid losses resulting from cyber attacks, furthermore the small startup has not sufficiently resources to hire a Cyber security officer. Precisely because each member has been trained, the economic investment in Cyber Defense is very low, about 1000 euros per year.
Regarding the other confidential information of the client companies, such as discussions of contracts and reserved agreements, Y, in order to avoid electronic interference, has decided to do everything physically, then visiting the company on the spot: the sale of Y's services takes place only through meetings.

The firm claims that it has never received damages from cyber attacks, but every day it detects attempts to access the servers through brut forcing. Brut forcing is an algorithm that consists in testing all the possible passwords as long as the correct one is not found: it is a slow and expensive attack tool and for this reason, as mentioned previously, among the main defense tools used there is the use of complex passwords often created through automatic generators.

Despite this, the company does not underestimate this type of tool, in fact the brute force attack suffered by GitHub, a software platform used by developers to share their software projects, has been compromised 21 million user accounts, putting the target company in an unpleasant position.

According to the interviewed software developer: *"although we do not have many economic resources to invest in IT defense systems, we consider ourselves adequately protected, the experience and skills of our team members allow us to have a strong consideration of the risks deriving from the sector and therefore, this give us the possibility to make statements in a non-superficial way. We think that our technological skills can compensate for the limited investment budget in cyber defense".*

Y specifies that, while not adopting specific forms of cooperation and interaction with other companies in terms of cyber security, living in a university, the situations of confrontation with professors, students and other entrepreneurial realities are many.

Having closed only a 60,000 euro round of financing at the time, the young Roman startup has the priority over the next 12 months of acquiring new customers to increase its cash flow.

The figures within the firm now claim to possess the necessary defense tools to ensure the security of information, but do not exclude that increasing their business volume could grow the risks arising from the Cyber space and therefore to maintain a system of adequate security may need other resources.

CHAPTER 5
ANALYSIS

5.1 Propensity to change the business model

For the selection of the companies interviewed, I focused primarily on the definition of small firm, considering it as an organization with a limited number of assets. Therefore, assuming the presence of scarce resources, I have taken into account three extreme cases in order to cover the entire existing population: high level of technology – mildly scarce resources, high level of technology –scarce resources and finally low level of technology – highly scarce resources. The combination high level of technology – abundant resources was not selected because abundant resources presuppose the fact of being a large company, while the research conducted is aimed at small companies.

Firm	Technological level	Financial resources
Y	High level	Scarcity
J	Low level	High level of scaricity
K	High level	Low level of scarcity

(Self elaboration:typology of companies interviewed)

The purpose of this first phase of analysis is to understand if startups really have the prerequisites and the needs to change their business model following the advent of the Cyber threats; the potential options are: death, static and change. In order to determine this phenomenon I submitted a series of questions directed to the firms and using the cross-case-analysis I want to find the answer that is common for the various organizations. The initial module of enquiries submitted is: *"What is your annual spending on Cyber security? Would you have the necessary resources to increase your investment in Cyber security? Do you think you are adequately defended?*
Company J claims that the annual capital spending made in Cyber defence is 1500 euros and given its share of profits, it would not be able to increase the investment. The head of the small firm declares to be adequately protected from IT risks, but this gives me

many doubts in fact: none of its employees have ever received a training about the Cyber defence prevention, nor the instrument used are regularly tested. In support of the hypothesis of low risk awareness, J reports that there should be a state initiative in addressing small companies for the Cyber security measures because they do not have the technological knowledge to do it.

From J, I deduce that the resources invested are not sufficient to ensure adequate protection, it is demonstrated by the attack received in 2016. From the contradiction of the firm regarding the self confidence about its Cyber defence methods and the need for a government intervention, it is possible to assume a low consideration of the risks related to the Cyber space. In addition, given the inadequate economic and technological resources, I can conclude that it would not be possible for J to increase its investment in Cyber defence.

On the other side, company Y invests annually in IT security 900 euros; the software developer interviewed lists among the main priorities of the next twelve months the customer acquisition, in fact, the assets that Y currently has, will not be sufficient to guarantee an adequate protection for the future. The interviewee says: “increasing our business volume could enhance the risks arising from the Cyber space and therefore, in order to maintain a secure infrastructure we need more resources”.

In the case of Y, there is a strong awareness about the menaces of the Cyber space due to the firm technological know how, moreover, the necessity of more economic resources to operate guaranteeing an adequate protection system, makes me assume also in this occasion a current impossibility to intensificate the investment in Cyber defence. The Russian firm K seems to deviate from the statements of the two companies previously interviewed, it claims that investing 15% of its profits in Cyber security makes it safe.

Moreover, also from the technological side, K is able to counter the Cyber threats, in fact, having a team composed principally by engineers, it holds the know how required by the external environment. But K is an exception for three motivations: it is at the limit between a small and a medium company having a turnover exceeding 15 million euro, it invests over 500 000 euros per year in Cyber defence and to conclude, working in the Cyber security sector, it possesses skills that are completely unknown to small companies not operating in the same field.

From this first module of questions analyzed, I can affirm for the small companies a high propensity to change their business model, indeed, both J and Y believe to do not have the adequate technological and economic resources to defend themselves while K with its huge investments and know how in Cyber security, shows me that in order to be adequately protected, the resources and the technological skills required are not within the reach of a small company.

I want to give more strength to the theory that I am going to create, for this reason, I have put another section of questions for the companies interviewed that allow me to measure the drivers behind the transformation of the business model: *How many people are your team made up of? What is the education level of the top management? How many people on your team have already other entrepreneurial experiences?*

The members of a team can favour or discharge the change, according to the theorists previously mentioned in the literary part, the entrepreneurial activity, more present among components of small firm's team, plays a fundamental role in stimulating the organizational learning and the selection of internal resources; this process increases the startup knowledge and the development of substantive capabilities, which, in turn, through the development of dynamic capabilities, increase the firm's performance, influencing positively the propensity to change the business model.

Both Y and J have a small number of team members and for this reason, in line with the literature section, it would be easier for these two firms to change their business model. The absence of the necessary assets for an acceptable protection, allow me to exclude the chance to remain static, therefore, only two hypotheses would remain available: death and change. Excluding death, as possible option remains only the change.

K instead, with its 50 employees, shows to be less prone to change because it already has resources and know how to fight the Cyber criminals, so it will be more inclined to adopt a static behaviour. Moreover, in this case, even if desired, due to the greater presence of immobilized assets, it would be less prone to change its own business model. Also in this occasion, as in the previous one, K is more static while J and Y are favourable to change their business model giving more force to the theory developed by me.

In line with Helfat both the level of education of team members and the previous entrepreneurial experiences are two factors that influence the dynamic capabilities that in turn drive the change of the business model. The dynamic capabilities increase

proportionally with the level of instruction of the startup partners. The interventions that I have actually led, disconfirm Helfat's idea, indeed, on one hand for company J, despite the average level of education is low (high school diploma), the only way to overcome the Cyber threats is the business model's transformation.

On the other hand, in the case of the company K, given the high level of skills within the company, from the interviews emerges that a change of the business model is not required to survive at the Cyber threats, therefore also in this case I can disconfirm Helfat's theory. The behaviour of Y is in the middle between J and K, in fact the small firm actually is adequately protected from IT risks thanks to the technological skills of its team and therefore seems, from this point of view, less favourable to the change its business model. According to what emerged, the level of education does not represent a driver for the change of the business model, indeed, it is possible to observe that as the level of education increases, also the company's propensity to keep its business model unchanged increases.

In line with the threat rigidity theory, in risky situations, managers tend to apply existing routines; in contrast, according to the prospect theory, managers, in situations of risk tend to adopt solutions that involve more hazard. This kind behaviour is more visible in companies that have less to lose according to Bowman, for this reason startups would be more prone to change.

Notwithstanding what is highlighted in the threat rigidity theory through the interviews conducted, we can observe that none of the companies interviewed presents significant Cyber security routines to justify what emerges in the model. From the investigation conducted, I am able to demonstrate the proximity of small companies's behavior to what is expressed by the prospect theory, so in situations of high risk, startups are inclined to adopt a risk taking actions. During the interviews I asked about the main priority that the three companies have over the next twelve months, no response directly quotes the Cyber security, this shows that firms, despite being aware of the level of risk, do not have sufficient resources to devote for the resolution of the problem, then, when placed in front of risky situations, they tend to dedicate resources on other tasks.

For a greater support about this thesis, I asked to the three companies if they are willing to take out insurance form Cyber risks, none of them responded positively to me, thus demonstrating their propensity to risk. In line with the findings emerged from the research

conducted, the selected sample disconfirms the threat rigidity theory while it is in line with the prospect theory, thus showing a considerable propensity to change its business model.

5.2 strategic operations framework

Doz & Kosonen in order to highlight the concept of business renewal, have built a framework which conceptualized strategic agility as the "thoughtful and purposive interplay on the part of top management" between three meta capabilities: the strategic sensitivity, leadership unity and resource fluidity.

Using this model for the startups I interviewed, I have the opportunity to get a further demonstration of the inclination of small companies to change their business models.

The investigation consists in observing whether the three elements mentioned by the two theorists are applicable to the companies interviewed, therefore, in this research, taking in consideration the components highlighted by Doz & Kosonen one by one and apply them to all three companies, I am able to observe the firm behaviour in front of Cyber threats.

The first element taken into consideration is the strategic sensitivity, which may depend on various factors related to the surrounding environment that allow the company to seize the opportunities. It is possible to find this peculiarity certainly in the company Y which, finding itself within a research center, is more inclined to change being influenced by the contact with the academic environment: in fact within the university environments there is a high rate of innovation and the spread of knowledge turns out to be the norm, allowing the startup to be updated about what happens in the external environment.

Regarding the company K, we can see a different propensity to seize the external opportunities, in fact Russia presents itself as one of the countries with the highest Cyber crime rate and this surely pushes the Russian companies to be more informed about tools

against hackers. In this way we can consider Russia as a cluster of Cyber security, following some demonstrative theoretical evidences: *"Russia is in the seventh place for Cyber crime rate" (Symantec), "Some of the top spam sending countries include China, Brazil, United States and Russia (Project Honey Pot, 2016)", "The number of internet-connected computers that are infected with at least one botnet is estimated to be at 14% (Kindsight, 2012)", "Among the top known countries to host bootnets include India, Vietnam, China and Russia (Spamhaus,2016)", "Among some of the top sources of phishing attacks include China, Russia, Ukraine, the United States and Brazil (APWG, 2014)".*

On the other hand, J shows the element of strategic sensitivity in a different way, in fact, when I asked about the prospects in the next twelve months, the answer I received was the following: *"We want to make an investment in marketing to seize new opportunities of profitability, perhaps starting to apply our knowledge also in other business sectors".*

Having verified the first element for all three companies, I analyse the second element of the model, the "Leadership unity": this kind of behaviour can be observed most frequently in small companies, which, given the small number of workers within them, are less burocratic than large companies.

This type of element is more suitable for J and Y, which fall perfectly within the category of small firms, in fact having low fixed costs, they are able to make quick decisions in order to change their core business. Company K, considered at the limit between small and medium – sized business, would present more difficulties given the larger amount of fixed costs, despite this, by what the interviewee said, they would be small enough to foster changes.

The last element analysed by the two theorists is "Resource fluidity", which is the ability to transform the structure of internal resources in order to implement changes. Always using the cross case analysis I will observe the presence of this element in the three selected sample companies. In order to measure this peculiarity, I rely on the history of the individual companies.

Company J perfectly shows in the 90s a change in the structure of internal resources passing from purely architectural works based on interior design to engineering works for large companies. Given the lack of immobilized costs, J was able to allocate part of the

budget available for the recruitment of engineering figures and for the purchase of softwares that made it possible to exploit the opportunity presented.

The company Y exhibit the characteristic of "Resource fluidity" in a different way, being a newly established company, but in my opinion it is very significant. This firm, was born from a university research, so the resources invested previously were destined solely for the research: Y enlarged the team, taking on students and dislocating part of its resources in the business side for the acquisition of loans, finally thanks to the asset allocation turned into a company that provides consulting services to companies.

Even for K, it is possible to observe a similar behaviour, initially the business model and the services offered were different, in fact previously, the product presented consisted of a website in which users, uploading a photo of a person, could trace the name on the social networks. Today, increasing the investment and expanding the team, K has been able to change the service offered to interface with companies.

At the end of this paragraph, I can say that taking into consideration the Doz & Kosonen framework and applying the three elements to all the three companies, I am able to prove the existence of strategic agility within the small companies, and therefore, this shows a further demonstration of the propensity to change the business model in small companies.

Firm	**Behaviors expressed during the interviews**	**Strategic agility framework**
Y	-The annual investment in Cyber defence is 900 €. -Insufficient resources for an adequate protection.	*Strategic sensitivity*: University environment. *Leadership unity*: Quick decisions due to low fixed costs. *Resource fluidity*: From a research to a consulting firm.
J	-The annual investment in Cyber defence is 1500 €. -Attack received in 2016. -Request for a government intervention.	*Strategic sensitivity*: New opportunities of profitability. *Leadership unity*: Quick decisions due to low fixed costs. *Resource fluidity*: From interior design to engineering projects.
K	-Small/middle company. -The annual investment in Cyber defence is 500.000 €. -K operates in the Cyber security sector	*Strategic sensitivity*: High Cyber crime rate in Russia. *Leadership unity*: Small enough to foster changes. *Resource fluidity*: From B2C to B2B.

(Self-elaboration:findings about the propensity to change the business model)

5.3 External forces behind the adaptation process

Thanks to the existing theory and the interviews conducted, through the cross case analysis, I have come to demonstrate the tendency of startups to change their business model with the advent of the risks related to the Cyber space. In this section my aim is to determine whether the transformation is due to an innovation of the business model or an adaptation linked to the external factor. When we talk about business model innovation, we mean the process wanted by the company that leads to make changes in the way in which the company interacts in its internal and external relations: it represents a shift in the way an organization make deals in order to promote a better performance.

Speaking about the business model adaptation we mean the phenomenon that aims, through learning and continuous research, to adapt to environmental circumstances.

First of all, I analysed the business model innovation, which according to the definition preconceived by the theoreticians, implies and leads to a significant improvement of the company performance, therefore, more than a solution of a problem, it implies a generation of surplus, so it is considered only in "positive terms". From the interviews conducted, none of the companies told me about "a decision desired by the company" aimed at increasing its performance, but in dealing with the Cyber threats they always talk about solving a problem in order to limit potential future damages. Therefore, the main factors that differ from assuming an innovation of the business model are: no existence of the internal factor and absence of a perspective to improve the company performance.

Regarding the business model adaptation, to verify this phenomenon, I consider a driver that the theoricians judge fundamental: the effectuation. With the effectuation, we assume that startups are not able to plan the adaptation process and then they plan step by step. Through the interviews I can say that this behaviour is suitable for the each of the three companies Y, J and K.

For J, the planning incapacity is shown to me in several aspects: first of which, the absence of a technological know-how that would allow to analyse the problem and then choose the appropriate tools to defend its business. Secondly, the company's request for an explicit support of the State, confirms an incapability to establish a path to pursue the

war against Cyber crime. On the other hand, as regards the characteristic of the step by step improvement indicated in the effectuation theory, I find a behaviour that corresponds with what was applied in 2016 when, after the attack received, J introduces new defence measures, leading a firm learning in the use of defence tools.

In the case of Y, despite the technological know-how possessed, in support of the hypothesis of inability to plan, the software developer interviewed, told me that he is not able to estimate the resources and the tools that will be required when their customers will increase, indeed, Y until now has the defence tools that allow it to operate safely, but for the future investments they will use a step by step approach. Also in the case of K, although to a lesser extent, can be found a similar behaviour to that of J and Y: with the transition of the offer of service from companies to individuals, the protection instruments have changed following a step by step approach, with a shift due to the adjustment of the business model with the transition from individuals to companies.

With K, considering it at the limit between small and medium firm, the planning process emerges through the regular meetings on its defence strategies. The main drivers of the business model adaptation are the scarcity of economic and technological resources and the regulatory forces.

I conclude this section through a question specifically asked in the questionnaire: *"Have you adopted other defence tools beyond those required by law? Which one?"*

This question allows me to measure the adjustment of the three companies to the regulatory forces, in particular considering the recent legislation on GDPR, which applies to all the firms that process personal data of European citizens.

It is possible to observe that for the company J, the regulation has had a good impact on its policy in terms of personal data, in fact J aims to collect the minor number of data as possible in order to do not fall in the sanctioning mechanism of the legislation. The directive regulates the objectives to be achieved but does not mention the tools to be used in order to accomplish the ordinance, leaving wide discretion to the firms.

The same behavior is observable for Y, which being aware of the risks related to the Cyber space, declares that the treatment of confidential information of companies takes place only through meetings in physical locations, in order to avoid the risk of being in possession of confidential information without have adequate resources to protect them. In fact GDPR's goals are aimed at reducing the risk exposure by pushing to collect only

strictly necessary data. Regarding company K, despite having seen that the resources and technologies in its possession are higher than the standard for small companies, guaranteeing a proper cyber defense, the information processed are limited to the minimum in order to reduce exposure to risk. The GDPR regulations deals with objectives to be achieved, but give wide discretion for the tools that can be used, in fact one of the main goal of the directive is to encourage small firms to collect as few data as possible. To demonstrate this, when K releases its software to client companies, every image taken by surveillance images remain outside the Russian company, which by choice decides to keep out of possessing them.

Comparing the sample of selected companies, with what has been said in the existing theory, I agree with the theoricians of the effectuation theory. Probably, this would be enough to confirm the process of adaptation of the business model, but in order to be more sure, through the interviews conducted, I verified that the drivers of the selected companies were external, in this way I am able to say that the element at the base of the business model change is the external factor, ie the Cyber risks.

Firms	Effectuation theory	External drivers
Y	-Inability to estimate resources/tools required. -Investment directly correlated with the customer acquisition.	-Treatment of confidential information during face to face meetings.
J	-Government intervention in order to establish a path. -New defence measures after the attack.	-minor number of confidential information as possible.
K	-Regular meetings. -Step by step investments in Cyber defence.	-Every image taken by surveillance camera remain outside the Russian company.

(Self elaboration:findings about the business model adaptation perspective)

5.4 A new design for the business model

In the previous paragraphs I have observed how startups, following the advent of Cyber risks, are faced with a double choice: to change their business model or to keep it static. After seeing that, given the absence of alternatives, the "natural selection" forced the small firms to change it, I wondered what is the driver that push the business model's transformation. Then, through the research conducted, I have seen that the business model adaptation is at the center of the variation. In this section I will see how, under a practical profile, the business model of companies will change. As stated by Teece, business models represent the logic by which firms create and deliver value to customers.

During the interviews, I asked specific questions aimed at measuring the responses of the business model in the following areas: key partners, channels, unique value proposition and cost structure.

I begin with the observation of the business model area that has to do with the "key partners", with which I consider all the actors outside the firm, such as suppliers and distributors, that contribute to create value. In order to understand the startup's behaviours I asked to the startups: *"Do you adopt forms of cooperation with other companies regarding cyber risk prevention?"*

Contrary to what is said in the system theory, none of the firms interviewed adopt forms of cooperation in order to deal with Cyber threats, indeed, they tend to keep their confidential information secret.

This happens for two main reasons: first of all, companies prefer to do not show their own vulnerabilities, second they want to keep hidden, from the public, any cyber attacks in order to preserve the trust of their customer. Company J for example, after the attack, simply had a discussion with other firms regarding their security tools but without giving information about its experiences with respect to the cyber attacks received, this, according to the interviewee, could have endangered their business relationships with other enterprises. On the other hand Y and K, being IT consultancy firms, in order to preserve their core business, cannot question their defense capabilities in public, so they also tend to do not divulge information with "Key partners", excluding possible forms of cooperation.

All the companies inverviewed, declare that for the choice of a partner, the defense capabilities of him are a key factor to consider. Until few years ago, the variables taken into consideration for establish business relationships with other companies were costs and quality of the service, today a third factor is added, the Cyber defense practices. According to what has been observed, I can say that the theory developed by me differs profoundly from the one highlighted by the system theory advocates, in fact, facing Cyber risks, first companies would tend to require more safety standards to their partners, secondly, the relationship has a propensity to exclude any form of cooperation on Cyber defence practices, especially with competitors who could exploit the difficult situation of the company in question to discredit it in front of its customers.

Another key point for which startups are inclined to exclude the instrument of cooperation, is their image in front of the customers, in fact according to the firms interviewed make aware the "Key partners" of their defense tools, could create problems with their own customers because they certainly trust the company in question but it is not said that they also trust external partners. From this first analysis, I can establish that relationships with partners will tend to become increasingly closed and selective.

The second factor considered in order to observe how the business model changes is the firm's channels, with which I consider the tools used by the corporation to reach its market segment. In order to measure what happens in this area, I asked the following question:

"Would you be willing to change supply and sales channels (sell on third party platforms rather than on your on) to reduce risk exposure?"

From the previous literature emerges that the Channels area, is that which allows to measure the customer trust and his main fears, thus companies in order to survive have to change in line with the customer demand. Regarding company Y, the software developer interviewed said that, when firms request advice from them, in order to reduce the risk exposure, they try to limit the exchange of information online. On Y website, it is not possible to make payments and there is not an area where customers can enter their information, indeed, the data sharing occur only during the offline meetings. The interviewee declares that in this way the information is protected and subsequently the client feels more secure in sharing his data. A Similar behaviour is seen in company J, in fact on its website there is no possibility to enter confidential data or to make payments.

In the case of company K, the exchange of confidential information is made during the agreements table and, in any case no sensitive data is recorded on K website.
According to what was declared by the business development manager in Europe, their website is only a way to show their products.
Analyzing the answers received, it is possible to notice a change in the supply and sales channels of the firms, the main purposes are: limit the exposure to risk and give to the customer a perception of reliability, indeed, websites are always aimed at collecting less information about the customers. Furthermore, there is a tendency to move from direct sales channels, therefore owned by the company, to indirect channels in order to have greater security for both the company and the customer.
The next area of the business model that I decided to analyze is the "value proposition", which represents the combination of products and services that give value to the customer, thus it represents the reason why customers choose the product of a company rather than that of another one. Until few years ago, companies in defining their value proposition, were focalized on the price and the quality of the product offered, today in accordance with what emerges from the interviews that I did, another element assumes a fundamental importance, the IT security. In order to measure this tendency I asked the following question:
"Have you ever notice a lack of confidence of the customer in making payments on your website or in giving you confidential information?"
The head of the company J says*: "to date we have not had lack of confidence of the client, just because the confidential information we hold are almost nil. Despite not having a business that would require to have relevant information about the customer, we try to give security by managing the smallest possible number of data ".* This statement shows the special attention that J dedicates to the perception of security that the client has about the company. J underlines how the Cyber Defense should become a key factor in the offer of its products, falling within its value proposition. From another point of view, interviewing Y, it emerges that, despite having just entered the market, the small firm has not yet had phenomena concerning the lack of customer confidence. The software developer says*: "we are aware that for our customers, the safety in processing their confidential information is fundamental, for this reason the exchange of our data takes place physically in meeting tables ".*

In this case the client's trust derives from the treatment of their own information offline, this in fact has become a standard practice within the company, becoming a service that contributes to create the value proposition of Y. Regarding K, there are three elements aimed to increase the customer trust: the first comes from the fact that K is a company that operates in the field of information security, the second is that no payment is performed on their proprietary platform and to conclude, it is given the possibility to the customer to test the software before the purchase, this usually according to what the interviewee says, has among the main purposes, the explanation of the Cyber defence mechanisms of K in order to guarantee maximum reliability towards the customer. According to what emerged from these interviews, I can say that, the cyber defense practices or the perception of their existence by the customer are fundamental elements of the value proposition of companies that can strongly influence the motivation to purchase.

The next area of the business analyzed model is how the cost structure of small companies changes with the advent of Cyber threats. For this purpose, I asked the interviewed firms, the following question: *"For the Cyber Defense tools have you developed internal resources or do you rely on third parties? "*.

Surely, as seen previously, the budget constraint of small firms leads to not being able to exceed a certain investment quota for Cyber defense tools, and this is precisely the reason that drives small companies to change their business model in order to adapt to the surrounding environment. Despite this, I still wanted to observe the changes in the cost structure, supported by the companies for the Cyber Defense. In my opinion, apparently, costs seem irrelevant but in reality there are many hidden costs. In this section first of all I want to make it clear that in case of successful cyber attack, the costs for the startup would become so high as to bring it disappear, this represents the highest cost to sustain for companies and it represents a hidden expense that many times it is not mentioned.

Taking this factor into account, we will analyze the costs that companies support to prevent attacks.

During the interview the head of company J tells me: *"surely with the introduction of the tools of prevention (only the Antivirus) from cyber attacks our cost structure has increased and if we had the opportunity we should invest more, in fact today our investment only covers the software side, but it does not include the technological skills*

we need. " According to what was said by J, with the resources invested it is not possible to have within the team figures specialized in Cyber Defense, in fact only when it is extremely necessary, the company uses external advice. Having an internal resource (the Cyber security officer) in the long run would be certainly more convenient, but for now it is not within the economic reach of J. From this first analysis apparently it would seem that the cost structure does not increase significantly, because there are not financial possibilities for this, so reconnecting with what was said before, this would represent the fundamental reason that would lead startups to change their business model. On the other side doing an analysis of the hidden costs borne by the company, we can observe that, they are much wider than what was declared by J, in fact following the attack received in 2016 the company has lost about 20 000 euros, equal to 40% of its own profit, furthermore, it has suffered costs in terms of credibility that could have led it to lose customers, but for the moment we will only evaluate this possibility without proceeding with a concrete estimate. From a first analysis we observe that for company J the cost structure would tend to increase considerably, taking into consideration even the hidden costs.

Also in the case of Y, the amount invested at the moment is low and therefore apparently almost irrelevant for the cost structure of the company, but unlike J, the young startup is entirely composed of engineers and therefore has a high know-how in technology.

As previously stated by the software developer interviewed, with the increase in turnover, Y will need to increase significantly its investment in Cyber Defense, thus the costs that the company support will increase, but even in this case until now the startup is not able to increase its investment in Cyber Defense, so the cost structure apparently has remained unchanged. Doing a more in-depth analysis I can see that the situation is actually different. In fact, taking into consideration the time that the engineers within the team must devote to the IT security, the company's Cyber defense cost increases exponentially.

Regarding K, the investment dedicated to Cyber security is equal to 15% of its income, thus exceeding € 500,000 per year; in this case are used mainly the internal resources but sometimes K asks for external consultancy. For K the costs structure is transparent and it is very far from the economic possibilities of small companies.

In conclusion it is possible to observe that with the advent of the Cyber threats the costs sustained by the small companies tend to increase considerably. With the research carried

out in this paragraph I am able to demonstrate the change of the business model in the following areas: key partners, unique value proposition, cost structure and sales channels.

Firm	Key partners	Channels	Value proposition	Cost structure
Y	-Impossibility to question the defence capabilities. -Partner defence capabilities. -Customer trust.	-Minimizing the exchange of information online. -Impossibility to pay online.	-Cyber defence as a Key requirement. -Cyber security is a standard practice in our value proposition.	-Future increase in the cost structure. -Time dedicated by the employees on Cyber defence practices.
J	-Partner defence capabilities. -Customer trust about Key partners.	-Impossibility to insert confidential information in the website.	-Relevant information about the customer not required -Special attention to the customer perception about Cyber security	-Impossibility to have an internal Cyber security officer. -20.000 € damage after the attack. -Lost of credibility.
K	-Impossibility to question the defence capabilities. -Partner defence capabilities. -Customer trust.	-No sensitive data collected on the website. -Face to face agreements.	-Core business based on information security. -The customer test the software before the purchase.	-500.000 € yearly investment. -Internal resources to deal with Cyber tools.

(Self elaboration: findings about "A new design for the business model")

CONCLUSIONS

In the first part of the thesis I studied the dynamics related to the Cyber space, narrowing the research on the interaction between Cyber security and small companies, then, observing the methods of attack used by hackers and the related company's defence tools, I have been able to observe the resources required by startup to curb the threats deriving from the Cyber criminality.

In order to deal with this first part, I have investigated about the existing regulations and the fears of customers in making online purchases going to observe which tools are used by companies to ensure greater security to clients interested in purchasing the services offered. In the second part of the thesis, I conducted a research on the dynamics related to the business model of the small firms, deepening business model innovation, business model adaptation and the related drivers that push companies to adopt one type instead of the other. During the investigation, I was able to explore the predisposition of companies to transform their internal structure; in doing so the concept of dynamic capabilities was fundamental.

The topic was never addressed, what prompted me to do it was the interest to make a contribution to an area unexplored until now, with the hope to be helpful both for future research and for startups in dealing with the risks associated with the Cyber space. In this paper, no defense tools are posed, but analyzing what happens for the small firms interviewed, finding a recurring pattern, this writing can be a starting point to find solutions that are within the reach of a reality with limited economic - technological resources.

One of the factors that pushed me to deal with this issue was the interest in understanding how it is possible to apply an approach on the evolution of species in Darwinian terms to startups. In particular, I refer to the observation of the dynamism of the business model following the external dangers, in this case the Cyber threats.

The final purpose of the analysis is to observe how the business model of small companies changes with the advent of Cyber risks; in doing this, I asked a series of questions to the firms interviewed, then following a step by step approach, I started the discussion by looking at whether the Cyber space actually represented a real risk for companies; this

allowed me to move on to the second question: *are the resources available to a small company sufficient to guarantee an adequate Cyber defense?*

In the second chapter, observing the dynamics of the business model, I focused on the observation of the variables that influence the propensity to change the internal structure of the company. This served me to understand what are the possible ways in which a startup can escape from the risks related to the Cyber space. At this point I began to understand the drivers that push firms to change their business model, choosing between business model innovation and business model adaptation. The understanding of the drivers, ultimately allowed me to respond to the final question, ie *how business model areas tend to change in front of IT risks?*

Given the lack of literature concerning my research question, I decided to use the Eisenhardt method, so I relied on a qualitative approach, specifically creating 3 case studies.

In line with Glaser and Straus (1967) in the case studies methodology, the close connection with reality makes possible to generate a valid and relevant theory, similarly Kuhn said that “in normal science, theory is developed through incremental empirical testing and extension”.

The possibility of adopting a holistic approach allowed me to go deeper with the research, noting things I would not have noticed otherwise. In fact, the data collection method that I used were the interviews, I proposed to the participants a face to face interview composed of 17 questions for the duration of 40 minutes, moreover in order to collect more data I asked both open questions, which offer me the occasion to gasp details that I had not foreseen, and closed questions.

For the selection of the sample, I focused on small companies, so I took 3 extreme cases to cover the entire population; this is perfectly in line with what was declared by Pettigrew (1988) who argues that given the extreme unpredictability of situations, it is preferable to choose polar types of samples in order to create a "transparently observable" theory.

Each of the firms surveyed was in one of the following categories: high level of technology - mildly scarce resources, high level of technology - scarce resources and finally low level of technology - highly scarce resources. The combination high level of technology - abundant resources was not selected because it assumed the fact of being a large company. Given the large amount of data that I found, for the analysis phase, firstly

I used the within case analysis, so I grouped the information treating them case by case. Secondly, using cross case analysis, I compared the data obtained from one of the companies with the others to see if they were in match, with the aim of finding a recurring pattern applicable to all the small companies.

Through the literature investigated in the first two chapters, I am then able to carry out a further verification, analysing if the emerging theory is in agreement or in disagreement with what was said by the previous theoreticians. This methodological aspect, in line with Eisenhardt, is important for two reasons: first it permits to offer greater validity to the new theory created, second it consents to put into discussion what emerged, offering the opportunity to refine the concepts developed.

The first step of this thesis was to understand if the Cyber risks could undermine the health of small companies. According to what has been discovered, it is possible to claim that the damages that a startup can suffer belong to two areas. The first area concerns the performance of companies in terms of profitability which is driven primarily by sales. According to (Coulter, 2002), when people bought online, they were in a highly uncertain environment because they could not verify the identity of the vendor or even evaluate the quality of the product purchased. With the advent of Cyber risks, another factor has been added: the protection of the personal data; think about, if after buying on Ebay with your credit card you discover that Ebay's information have been stolen by a group of hackers. From this case, it is possible to understand how is crucial for startups to give the customer a perception of security during the purchase time, in line with Chellappa and Pavlon "To attract and retain e-payment users, it is vital to enhance consumers' perceptions of security trust and e-payment transactions".

According to the Gartner Group study, 95% of online customers are concerned about the privacy and security when they make online payments.

The evidence of this is found in the interviews conducted, especially for companies K and Y, which claim that their customers rely primarily on the reliability in dealing with confidential information. From the analysis of this first area it is possible to find the direct proportionality between sales and Cyber defense systems. The second area investigated regards the damages that a startup can suffer as a result of a Cyber attacks: first of all the loss of electronic data, indeed, inside the infected computer there could be confidential

information of the company, such as lists of suppliers and customer or in case of hi-tech startups proprietary algorithms, whose spill could put at risk its business.

In the case of the company J, following the attack suffered in 2016, the loss of data has led to a loss of over € 20,000. Moreover, according to a study by Deloitte, the visible costs associated with data breaches represent only 5% of the total costs, in fact for 95% there are represent by hidden costs.

Also Y says that every day it detects attempts to access the servers through brut forcing; until now it has managed to defend itself adequately thanks to its team of engineers, but it argues that increasing its business, Y will have to increase its investment in Cyber Defense, in fact among hidden costs there is also the lost of reputation because customers, following an attack can decide to switch to a competitor because they fell more secure.

After verifying, therefore, that the Cyber space is one of the main risks for startups, I wanted to evaluate how it is possible for them to be adequately protected. In the questionnaire I asked the following question to the three companies:

"What is your annual spending on Cyber security? Would you have the necessary resources to increase your investment in Cyber security? Do you think you are adequately defended?".

Regarding company J, the technical factor is the main criticality, ie the absence and the impossibility of investing in technological resources that could direct the company to have a sufficient protection system. Y instead claims to have the technological resources, having a team composed entirely of engineers, but the economic resources available do not allow to increase the investment. Company K, is the only one to feel adequately protected, but K is an exception for three motivations: it is at the limit between a small and a medium company having a turnover exceeding 15 million euro, it invests over 500 000 euros per year in Cyber defence and to conclude, working in the Cyber security sector, it possesses skills that are completely unknown to small companies not operating in the same field.

From this evidence emerges, in accord with the literature seen in chapter 2, that small companies are not able to adequately defend themselves against the risks related to the Cyber space.

At this point of the thesis, applying the theory of evolution of Darwin species to startups I set the goal to observe how small companies try to survive through the change of the business model.

A small firm seems to have two alternatives: die or change.

In this part of the analysis the purpose is to observe the propensity to change the business model, in doing so I decided to submit to the companies interviewed a series of questions to measure their dynamic capabilities. According to the existing theory, the dynamic capabilities are the main factors that drive the change of the business model and these mainly reside, as specified by Helfat, in the level of education of the top management and in the previous entrepreneurial experiences.

Analyzing the sample of startups interviewed, I disconfirm what was said by Helfat, in fact the company most likely to change is J, namely the one with a lower average level of education. On the other hand, in the case of the company K, given the high level of skills within the company, from the interviews emerges that the change of the business model is not required to survive at the Cyber threats. The next question posed to companies concerns priorities over the next 12 months, none of the companies interviewed mentions the Cyber threats, this shows that despite the risk awareness the small firms do not have enough resources to solve the issue, then, when placed in front of risky situations, they tend to dedicate their assets on other tasks. This evidence goes against what was said in the threat rigidity theory, while it confirms the prospect theory, in fact, in situation of risk startups tend to adopt solution that involve more hazard.

In order to more vigorously measure the propensity to the business renewal, I applied the strategic agility framework of Doz & Kosonen defined as "Thoughtful and purposive interplay on the part of the top management" between three meta-capabilities: the strategic sensitivity, leadership, unity and resource fluidity.

After having verified for all three companies the alignment with the three proposed elements, I was able to give greater proof to the high propensity of small firms to change the business model.

Proceeding with the analysis, I set myself the goal of understanding which drivers are at the center of the changing process, then I analyze the dynamics of the business model innovation and the business model adaptation.

In verifying, which of the two models to apply, I incur in the effectuation theory which claims that the adaptation process can not be planned and therefore is done step by step. Through the questions put to the sample of companies, doing cross case analysis, it is possible to find this type of behavior for all three firms, in fact in the occasion of J the inability to plan, which is a main feature of the business model innovation, is shown in several aspects: first of which, the absence of a technological know-how that would allow to analyze the problem and then choose the appropriate tools to defend its business. The software developer of Y declares that he is not able to estimate the resources and the tools that will be required when their customers will increase.

Also in the case of K, although to a lesser extent, can be found a similar behaviour to that of J and Y: with the transition of the offer of service from companies to individuals, the protection instruments have changed following a step by step approach, with a shift due to the adjustment of the business model with the transition from individuals to companies. These aspects, allow me to establish that the drivers of the changing process lead to the business model adaptation, but to give more strength to the theory, knowing that the adaptation process is due to external factors, I asked the interviewed startups about their relationship with regulations. For all three companies, it appears that the transformations adopted are largely due to a process of adaptation to the existing regulations, confirming that the process follows the dynamics of the business model adaptation.

The final research question of the thesis is to understand how the business model tends to change, so I will proceed to analyze each of the following areas: Key partners, Channels, Unique value proposition and Cost structure.

In order to understand how the relationship with Key partners tends to change I asked the the companies if they adopt forms of cooperation with other firms regarding Cyber risk prevention and if they require to their own partners cyber defense standards to keep their confidential information protected. What emerges from the interviews conducted is that the relationship with external parties tends to be increasingly closed for two main reasons: the startups prefer to do not show their own vulnerabilities, second they want to keep hidden, from the public, any cyber attacks in order to preserve the trust of their customer. On the other hand all the companies inverviewed, declare that for the choice of a partner, the defense capabilities of him are a key factor to consider.

From this point of view the theory developed by me differs profoundly from what was said by the proponents of the system theory, which argue that firms in front of the Cyber risks would tend to open up more towards the external environment.

For the sales channels area, it emerges from the interviews that the tendency is to request less and less information on sales channels, preferring, when possible, an offline relationship with the customer. In the most extreme cases, a firm can decide to sell its products / services on third-party sales channels considered to be more secure.

Proceeding with the analysis of the third area of the business model, then the unique value proposition, startups declare that until few years ago the main factors to consider were the price and the quality of the service offered. Today, given the extreme attention placed by the customer on the security of their data, I can say that, the cyber defense practices or the perception of their existence by the customer, are fundamental elements of the value proposition of the firms that can strongly influence the motivation to purchase.

To conclude, the final area of the business model that I have analyzed is the cost structure. According to a superficial view, from the interviews conducted it would seem that costs don't increase considerably, but in reality it is not so because the hidden costs are enormous. J states that following the attack, it lost 20,000 euros, about half of its annual profit.

On the other hand Y, despite never having suffered losses following a Cyber attack, declares that taking into consideration the time that the engineers within the team must devote to the IT security, the startup's Cyber defense cost increases exponentially.

Regarding K, the investment dedicated to Cyber security is equal to 15% of its income, thus exceeding € 500,000 per year; in this case are used mainly the internal resources but sometimes K asks for external consultancy. For K the costs structure is transparent and it is very far from the economic possibilities of small companies. So from this analysis it turns out that the structure of hidden costs incurred by the companies, following the cyber threats, increases considerably.

References

Amin Z., (2017). *A practical road map for assessing Cyber risk*. Journal of risk research.

Antonio Teti, (2016). *Cyber security e investimenti, quali scenari?* Rivista italiana di intelligence.

Atkinson J., (2002). *Four steps to analyse data from a case study method.* ACIS 2002 Proceedings.

Autio E., Sapienza H., Almeda J., (2000*). Effects of age at entry, knowledge intensity, and imitability on international growth.* The academy of management journal, Vol. 43, No.5.

Baldwinn R., Montanari L., (2015). *Consapevolezza della minaccia e capacità difensiva della pubblica amministrazione.* Cyber security report 2015.

Baldoni R., De Nicola R., Prinetto P., (2018). *Il futuro della Cyber security in italia: ambiti progettuali e strategici.* CINI: laboratorio nazionale di Cyber security.

Boston Consulting Group, (2009). *Business model innovation, when the game gets though, change the game.*

Bowman J. S., (1994). *At least, an alternative to performance appraisal: total quality management.* Public administration review, Vol. 54, No.2, pp. 129-136.

Chattopadhyay P., William H., Huber G., (2001). *Organizational actions in response to threats and opportunities.* Accademy of management journal, Vol. 44.

Chellappa R., Pavlou P., (2002). *Perceived information security, financial liability and consumer trust in electronic commerce transactions*. Logistic information Management.

Chukwudi A. E., Udoka E., Ikerionwu C., (2017). *Game theory basics and its application in Cyber security.* Sciences Publishing Group.

Cowan D., (2015). *Security for startups: the affordable ten step plan survival in Cyber space.* Bessemer Venture Partners.

Creedon M.R., (2011). *Space and Cyber Shared Challenges, Shared Opportunities.* Strategic Studies Quarterly, Vol6, No.1, pp. 3-8

Culnan M., Armstrong P., (1999*). Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation*. Organization Science.

Das S., (2018). *Social Cyber security: reshaping security through an empirical understanding of human behaviour*. Usenix Association.

Deloitte, (2017). *Cyber risk in consumer business*.

Deloitte, (2016). *Business impacts of Cyber attacks.*

Dopfer et al., (2017). *Adapt and strive: how ventures under resources contraints create value through business model adaptation.* John Wiley & Sons Ltd.

Edwards B. et al., (2017). *Strategic aspects of Cyber attack, attribution and blame*. National Accademy of Science.

Eisenhardt M. *Building theories from case study research.* Accademy of management review.

Eisenhardt M., Martin J.A., (2010). *Cross business unit collaborations in multi business organizations.* The Accademy of Management Journal.

Eisenhardt M., (2016). *What drives business model adaptation? The impact of opportunities, threats and strategic orientation.* ScienceDirect Journal.

Eisenhardt M., Martin J.A., (2000). *Dynamic capabilities: what are they?* Strategic management journal, Vol. 21, No. 10/11, pp. 1105-1121

Flàvian C., (2006). *Customer trust, perceived security and privacy policy: three basic elements of loyalty to a web site.* Industrial Management and Data Systems.

Foss J.N., Lien L., Saebi T., (2017). *What drives business model adaptation? The impact of opportunities, threats and strategic orientation.* Science direct Journal.

Foss J. N., Lyngsie J., Zahra S., (2013). *The role of esternal knowledge sources and organizational design in the process of opportunity exploiation.* Strategic Management Journal.

Foss J. N., Saebi T., (2016). *Fifteen years of research on business model innovation: How far have we come, and where should we go?* Journal of Management, Vol. 43, No. 1.

Gartner Group. (2001). *On-line fraud prevention white paper for the E-Commerce fraud prevention network*. August 26, 2013, from http://www.gartner.com

Gerring J., Seawright J., (2008). *Case selection techniques in case study research.* Political Research Quarterly, University of Utah.

Griffith A., Harvey G., (2006). *Social exchange in supply chain relationship: the resulting benefits of procedural and distributive justice*. Journal of operation management.

ISACA, (2009). *An introduction to the business model for information security.*

Janet & Mark L. Goldenson Center for Actuarial Research, (2016). *Cyber risk for small and medium-sized enterprises.*

Johnson S., (2016). *Managing risk and information security*. Malcom W. Harkins.

Joyce A., Raymond L., (2016). *The triple layered business model canvas: a tool to design more sustainable business models.* Journal of Cleater prudction, Volume 135, pages 1474 - 1486

Kahneman D., Tvesky A., (1979). *Prospect theory: an analysis of decision under risk.* ECONOMETRICA, Volume 47.

Kimberly A. W., Farris P.W., (2017). *The impact of Cyber attacks on brand image*. Journal of Advertising Research.

Kosonen M., Doz L. Y., (2010). *A leadership agenda for accelerating business model renewal.*

Lance Strate, (2009). *The varieties of Cyber space: problems in definition and delimitation.* Western Journal of Communication.

O' Connor H., Madge C., (2005). *Mothers in the making? Exploring liminality in Cyber/Space.* Article in transactions of the Institute of British Geographers.

Osiyevskyy O., Dewald J., (2015). *Explorative versus exploitative business model change: the cognitive antecedents of firm level responses to disruptive innovation.* Strategic Entrepreneurship Journal.

Osawa J, (2018). *The reversion of Cyber space to the world of classical realism*. Japan SPOTLIGHT.

Phils Zinkewicz, (2017). *Cyber space, the miraculous, vulnerable world.*

Piotr Dela, (2016*). Cyber space as the environment affected by organized crime activity.* Connections, Vol. 15, No.3, pp. 55-64.

Powell W. et al., (1996). *Interorganizational collaboration and locus of innovation: networks of learning in biotechnology*. Administrative science quarterly.

Pwc, (2017). *Consumer Intelligence Series: Protect.me.*

Roy S. et al. *A survey of game theory as applied to network security*. University of Memphis.

Salim H., Madnink S., (2016). *Cyber safety: A systems theory approach to managing Cyber security risks*. Massachussets Institute of Technology, Cyber security interdisciplinary laboratory.

Shaker A., Zahra, (2016). *Entrepreneurship and dynamic capabilities: a review model and agenda.* Journal of Management Studies, Volume 43.

Shukla S., (2017). *Game theory for security investments in Cyber and supply chain networks.* University of Massachussets Amherst.

Skopik F., (2017). *Collaborative Cyber threat intelligence*. CRC Press, cap. 4.1.

SuttonBank, (2016). *Cyber security for small and medium size business.*

Teece D.J., (2018). *Profiting from innovation in the digital economy: enabling technologies, standards, and licensing models in the wireless world*. ScienceDirect.

Teece D.J., (2017). *Business models and dynamic capabilities*. Journal homepage: http://www.elsevier.com/locate/lrp

Teece D.J., (2010). *Business models, business strategy and innovation*. Journal homepage: http://www.elsevier.com/locate/lrp

Velmurugan S., (2009). *Security and trust in e-business: problems and prospects. International Journal of Electronic Business Management*, Vol. 7, No.3, pp. 151-158

Wang Tao et al., (2010). *An empirical study of customers' perceptions of security and trust in e-payment.* Electronic Commerce Research and Applications, Volume 9.

Woszczynsky Amy B., Green A., (2017). *Learning outcomes for Cyber defense competitions.* Journal of information systems education, Vol. 28.

Zainal Z., (2007). *Case study as a research method.* Jurnal Kemanusiaan bil.9.

Zott C., Amit R., (2007). *Business model design and the performance for entrepreneurial firms.* Organization Science, Vol. 18, No. 2, pp. 181-199.

Zott C., Amit R., (2010). *Business model design: an activity system perspective.* Journal homepage: http://www.elsevier.com/locate/lrp

SUMMARY

The Cyber Space represents the conceptual place where people interact telematically exchanging informations, it could be considered as a complex network that today groups and manages individual's life; just consider when we send an email to another person, the correspondence passes from a computer to another through the Cyber Space.

Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data".

The economic losses related to Cyber crime amount to $345 billion each year, on average large companies suffer 100 attacks per year and around 1/3 of them is successful despite the Cyber Security spending is $70 billion per year; these numbers don't seem to stop, in fact, with the advent of IoT(Internet of things), by 2020 online devices are projected to outnumber human users by a ratio of six to one, creating a huge opportunity for cyber criminals to manipulate connected appliances.

Today, online sales lead to companies a large percentage of profits, over the years in fact, many firms have started to hire designers and computer engineers with the aim of creating an online infrastructure as high-performing as possible.

With the advent of IT risks, costs for these small companies seem to increase, indeed, the customer's security in making the purchase is a determinant factor for the success of the sales department, for this reason startups are dedicating more and more attention to customer perception during the payment process.

According to the Gartner Group study, 95% of online customers are concerned about the privacy and security when they make online payments. This data shows how important it is for online businesses to ensure adequate security in order to survive.

Companies can receive different kinds of attacks, partly for this reason it is difficult to defend themselves; "malware" is the main tool used by Cyber criminals to steal resources from firms, it includes different category of software that behave like vehicles to access, control and compromise the information contained inside a computer. In order to operate,

malwares need to be installed, thus attackers can use different methods to reach their goal such as bring the user to click on a link or open an attachment, this strategy considers that in order to induce someone to open a link, trust is necessary, so hackers usually send an email that appears to be from someone that the user trust.

The incumbency of these threats can cause firms an innumerable variety of damages, first of all the loss of electronic data, indeed, inside the infected computer there could be confidential information of the company, such as lists of suppliers and customer or, in case of hi-tech startups proprietary algorithms, whose spill could put at risk their business. The lost of reputation is the main collateral effect of IT risks, indeed, Cyber attacks can seriously damage the health of startups because customers can decide to switch to a competitor because they feel more secure.

Traditional policies don't cover any more companies from the risks related to the Cyber Space, in fact the concept of property is changed: while until the period before the advent of internet, firm's asset revolved around infrastructures, desks and other movable and real estate assets, with the advent of E-business the main resources held by firms are information and software, for this reasons traditional protection tools no longer have an effect.

With regard to hardware devices, computer protection is possible through the periodic change of access passwords, the removal of unnecessary software and the exclusion of superfluous admin accounts. Regarding the human resources, given that most attacks derive from human error, it is crucial to educate the employees and remove former dependent's authorizations.

On the other side, information's exchange among companies gives the possibility to reduce security expenses, having the opportunity to be aware of a weapon or a mode of attack from those who suffered it, gives the possibility to prepare an efficient defensive strategy. This methodology seems to be in line with small firms business model for two reasons, the first one is the cost factor, the second is the locations in which startups operate, usually co-working places where information sharing is favoured. One of the main aspects for companies to start cooperating is the mutual trust, since data about internal security systems is often disclosed. However, information sharing needs to be structured and coordinated and for this purpose standardization bodies, including NIST, ITU-T and ISO (2012) have established national cyber security centers.

In line with Adams and Sasse, insufficient awareness of security issues directs small firms to adopt inefficient protection models.

On the other hand, regulatory interventions can result in friction for startups, forcing them to use resources for activities not directly correlated to their core business; on the other hand could be very useful for small businesses, which due to the lack of resources to defend themselves, they need a state mediation.

On 25 May 2018 the GDPR legislation came into force with the aim of standardizing the policy of personal data within the various European Union countries. The objective is to regulate not only information's management but also the conservation, the confidentiality and the cancellation if requested by the interested party. The legislation speaks about objectives to be achieved but leaves wide discretion to companies as regards the tools to be used. Companies are required to have an expert in the field of data protection, the data protection officer (DPO). Being aware of the fact that make 100% data secure is really hard, especially if we are talking about small companies, GDPR's goals are aimed to reduce the risk exposure pushing firms to collect only strictly necessary data, using them only for specific purposes and deleting them when they are no longer useful. Failure to comply with the law brings sanctions of up to 20 million euro or up to 4% of the turnover of the previous year.

In Italy the national plan for cyber protection aims to update the DPCM Gentiloni by easing the methods for responding to cyber crisis in order to streamline the decision making process. In order to strengthen the defence mechanism, the Computer Emergency Response Team(CERT), the structure that deal with prevention and assistance on the risks deriving from the Cyber space, is unified. The main features of this model are the certification of ICT tools, the cooperation between public and private sectors and the creation of academic programs directed to innovate existing defence systems.

In order to understand how startup's business model changes in front of Cyber threats first of all I need to identify the concept of business model, for which, in line with Amitt e Zott, it is the unit of analysis that captures the value creation potential deriving from the design of transactions between the company and all the other outsiders such as partners, suppliers and customers. As stated by Teece, business models represent the logic by

which firms creates and delivers value to customers, according to this view, the value captured by companies is the essence of the business model.

Today the greatest percentage of enterprises operate in the "E-business", for which I mean the online business, therefore the business that is done through the Cyber Space. The growth of E-business was without precedent, the greatest share of companies that 10 years ago operated offline today have an online store, in fact by 2002, 93% of U.S. firms have some fraction of their business on Internet.

There are two central theories that allow me to measure the degree of propensity to adopt disruptive business model solutions in order to take into account all of the possible firm's behaviour.

On one hand the threat-rigidity theory argues that risks lead managers to apply existing routines while opportunities stimulate risk taking actions. In these occasions, the past behaviour tends to influence the decisions of the company, which will coincide with solutions already used and internalized by the firm. The better fit with this theory is find in large companies, which being equipped with both past experiences and resources are less disposed to change their business model in front of IT risks. On the other hand the prospect theory supports the opposite, in fact in this case, in risky situations managers tend to make resolutions that involve more hazard.

In order to determine this phenomenon, I submitted a series of questions directed to the firms and using the cross-case-analysis I want to find the answer that is common for the various organizations. The initial module of enquiries submitted is*: "What is your annual spending on Cyber security? Would you have the necessary resources to increase your investment in Cyber security? Do you think you are adequately defended?*

Company J claims that the annual capital spending made in Cyber defence is 1500 euros and given its share of profits, it would not be able to increase the investment. The head of the small firm declares to be adequately protected from IT risks, but this gives me many doubts in fact: none of its employees have ever received a training about the Cyber defence prevention, nor the instrument used are regularly tested. In support of the hypothesis of low risk awareness, J reports that there should be a state initiative in addressing small companies for the Cyber security measures because they do not have the technological knowledge to do it.

From J, I deduce that the resources invested are not sufficient to ensure adequate protection, it is demonstrated by the attack received in 2016. From the contradiction of the firm regarding the self confidence about its Cyber defence methods and the need for a government intervention, it is possible to assume a low consideration of the risks related to the Cyber space. In addition, given the inadequate economic and technological resources, I can conclude that it would not be possible for J to increase its investment in Cyber defence.

On the other side, company Y invests annually in IT security 900 euros; the software developer interviewed lists among the main priorities of the next twelve months the customer acquisition, in fact, the assets that Y currently has, will not be sufficient to guarantee an adequate protection for the future. The interviewee says: “increasing our business volume could enhance the risks arising from the Cyber space and therefore, in order to maintain a secure infrastructure we need more resources”.

In the case of Y, there is a strong awareness about the menaces of the Cyber space due to the firm technological know how, moreover, the necessity of more economic resources to operate guaranteeing an adequate protection system, makes me assume also in this occasion a current impossibility to intensificate the investment in Cyber defence. The Russian firm K seems to deviate from the statements of the two companies previously interviewed, it claims that investing 15% of its profits in Cyber security makes it safe.

Moreover, also from the technological side, K is able to counter the Cyber threats, in fact, having a team composed principally by engineers, it holds the know how required by the external environment. But K is an exception for three motivations: it is at the limit between a small and a medium company having a turnover exceeding 15 million euro, it invests over 500 000 euros per year in Cyber defence and to conclude, working in the Cyber security sector, it possesses skills that are completely unknown to small companies not operating in the same field.

From this first module of questions analyzed, I can affirm for the small companies a high propensity to change their business model, indeed, both J and Y believe to do not have the adequate technological and economic resources to defend themselves while K with its huge investments and know how in Cyber security, shows me that in order to be adequately protected, the resources and the technological skills required are not within the reach of a small company.

Doz & Kosonen in order to highlight the concept of business renewal, have built a framework which conceptualized strategic agility as the "thoughtful and purposive interplay on the part of top management" between three meta capabilities: the strategic sensitivity, leadership unity and resource fluidity.

Using this model for the startups I interviewed, I have the opportunity to get a further demonstration of the inclination of small companies to change their business models.

The investigation consists in observing whether the three elements mentioned by the two theorists are applicable to the companies interviewed, therefore, in this research, taking in consideration the components highlighted by Doz & Kosonen one by one and apply them to all three companies, I am able to observe the firm behaviour in front of Cyber threats.

I can say that taking into consideration the Doz & Kosonen framework and applying the three elements to all the three companies, I am able to prove the existence of strategic agility within the small companies, and therefore, this shows a further demonstration of the propensity to change the business model in small companies.

The changes in the business model is not only driven by the management's decision to innovate it, but also from its adaptation to external factors like Cyber threats.

For business model adaptation I mean the process by which startups change their business model aligning it with the external factor. Rapid learning and the capability to adapt to market changes are the basis of the business model adaptation, which in accordance with Saebi, consists in the continuous research, selection and improvement based on the surrounding environment.

The main drivers behind the business model adaptation are the external stakeholders, regulatory forces and technologies; furthermore the more drastic is the threat and more likely companies are inclined to business model adaptation. The transition from one model to another implies a temporary decline in performance for companies, also because often they have to change market segment, value proposition and value chain; business model adaptation is a "risk taking behaviour" since it often involves changing routinely patterns of action often with an uncertain outcome. Especially startups, have "little to lose" and then reconnect to the prospect theory, in front of a threat they will have a more risk-taking behaviour and then respond with the business model adaptation (T. Saebi et al.). Regarding the business model adaptation, to verify this phenomenon, I consider a

driver that the theoricians judge fundamental: the effectuation. With the effectuation, we assume that startups are not able to plan the adaptation process and then they plan step by step. Through the interviews I can say that this behaviour is suitable for the each of the three companies Y, J and K.

For J, the planning incapacity is shown to me in several aspects: first of which, the absence of a technological know-how that would allow to analyse the problem and then choose the appropriate tools to defend its business. Secondly, the company's request for an explicit support of the State, confirms an incapability to establish a path to pursue the war against Cyber crime. On the other hand, as regards the characteristic of the step by step improvement indicated in the effectuation theory, I find a behaviour that corresponds with what was applied in 2016 when, after the attack received, J introduces new defence measures, leading a firm learning in the use of defence tools.

In the case of Y, despite the technological know-how possessed, in support of the hypothesis of inability to plan, the software developer interviewed, told me that he is not able to estimate the resources and the tools that will be required when their customers will increase, indeed, Y until now has the defence tools that allow it to operate safely, but for the future investments they will use a step by step approach. Also in the case of K, although to a lesser extent, can be found a similar behaviour to that of J and Y: with the transition of the offer of service from companies to individuals, the protection instruments have changed following a step by step approach, with a shift due to the adjustment of the business model with the transition from individuals to companies.

With K, considering it at the limit between small and medium firm, the planning process emerges through the regular meetings on its defence strategies. The main drivers of the business model adaptation are the scarcity of economic and technological resources and the regulatory forces.

I conclude this section through a question specifically asked in the questionnaire: *"Have you adopted other defence tools beyond those required by law? Which one?"*

This question allows me to measure the adjustment of the three companies to the regulatory forces, in particular considering the recent legislation on GDPR, which applies to all the firms that process personal data of European citizens.

It is possible to observe that for the company J, the regulation has had a good impact on its policy in terms of personal data, in fact J aims to collect the minor number of data as

possible in order to do not fall in the sanctioning mechanism of the legislation. The directive regulates the objectives to be achieved but does not mention the tools to be used in order to accomplish the ordinance, leaving wide discretion to the firms.

The same behavior is observable for Y, which being aware of the risks related to the Cyber space, declares that the treatment of confidential information of companies takes place only through meetings in physical locations, in order to avoid the risk of being in possession of confidential information without have adequate resources to protect them. In fact GDPR's goals are aimed at reducing the risk exposure by pushing to collect only strictly necessary data. Regarding company K, despite having seen that the resources and technologies in its possession are higher than the standard for small companies, guaranteeing a proper cyber defense, the information processed are limited to the minimum in order to reduce exposure to risk. The GDPR regulations deals with objectives to be achieved, but give wide discretion for the tools that can be used, in fact one of the main goal of the directive is to encourage small firms to collect as few data as possible. To demonstrate this, when K releases its software to client companies, every image taken by surveillance images remain outside the Russian company, which by choice decides to keep out of possessing them.

Comparing the sample of selected companies, with what has been said in the existing theory, I agree with the theoricians of the effectuation theory. Probably, this would be enough to confirm the process of adaptation of the business model, but in order to be more sure, through the interviews conducted, I verified that the drivers of the selected companies were external, in this way I am able to say that the element at the base of the business model change is the external factor, ie the Cyber risks.

During the interviews, I asked specific questions aimed at measuring the responses of the business model in the following areas: key partners, channels, unique value proposition and cost structure.

I begin with the observation of the business model area that has to do with the "key partners", with which I consider all the actors outside the firm, such as suppliers and distributors, that contribute to create value.

Contrary to what is said in the system theory, none of the firms interviewed adopt forms of cooperation in order to deal with Cyber threats, indeed, they tend to keep their confidential information secret. This happens for two main reasons: first of all, companies

prefer to do not show their own vulnerabilities, second they want to keep hidden, from the public, any cyber attacks in order to preserve the trust of their customer. All the companies inverviewed, declare that for the choice of a partner, the defense capabilities of him are a key factor to consider.

According to what has been observed, I can say that the theory developed by me differs profoundly from the one highlighted by the system theory advocates, in fact, facing Cyber risks, first companies would tend to require more safety standards to their partners, secondly, the relationship has a propensity to exclude any form of cooperation on Cyber defence practices, especially with competitors who could exploit the difficult situation of the company in question to discredit it in front of its customers.

From this first analysis, I can establish that relationships with partners will tend to become increasingly closed and selective.

The second factor considered in order to observe how the business model changes, is the firm's channels, with which I consider the tools used by the corporation to reach its market segment. Analyzing the answers received, it is possible to notice a change in the supply and sales channels of the firms, the main purposes are: limit the exposure to risk and give to the customer a perception of reliability, indeed, websites are always aimed at collecting less information about the customers. Furthermore, there is a tendency to move from direct sales channels, therefore owned by the company, to indirect channels in order to have greater security for both the company and the customer.

The next area of the business model that I decided to analyze is the "value proposition", which represents the combination of products and services that give value to the customer, thus it represents the reason why customers choose the product of a company rather than that of another one. Until few years ago, companies in defining their value proposition, were focalized on the price and the quality of the product offered, today in accordance with what emerges from the interviews that I did, another element assumes a fundamental importance, the IT security.

According to what emerged from the interviews, I can say that, the cyber defense practices or the perception of their existence by the customer are fundamental elements of the value proposition of companies that can strongly influence the motivation to purchase.

The next area of the business model analysed is how the cost structure of small companies changes with the advent of Cyber threats. Surely, as seen previously, the budget constraint of small firms leads to not being able to exceed a certain investment quota for Cyber defense tools, and this is precisely the reason that drives small companies to change their business model in order to adapt to the surrounding environment. Despite this, I still wanted to observe the changes in the cost structure, supported by the companies for the Cyber Defense. According to what was said by J, with the resources invested it is not possible to have within the team figures specialized in Cyber Defense, in fact only when it is extremely necessary, the company uses external advice. Having an internal resource (the Cyber security officer) in the long run would be certainly more convenient, but for now it is not within the economic reach of J. From this first analysis apparently it would seem that the cost structure does not increase significantly, because there are not financial possibilities for this, so reconnecting with what was said before, this would represent the fundamental reason that would lead startups to change their business model. On the other side doing an analysis of the hidden costs borne by the company, we can observe that, they are much wider than what was declared by J, in fact following the attack received in 2016 the company has lost about 20 000 euros, equal to 40% of its own profit, furthermore, it has suffered costs in terms of credibility that could have led it to lose customers, but for the moment we will only evaluate this possibility without proceeding with a concrete estimate. From a first analysis we observe that for company J the cost structure would tend to increase considerably, taking into consideration even the hidden costs.

Also in the case of Y, the amount invested at the moment is low and therefore apparently almost irrelevant for the cost structure of the company, but unlike J, the young startup is entirely composed of engineers and therefore has a high know-how in technology.

As previously stated by the software developer interviewed, with the increase in turnover, Y will need to increase significantly its investment in Cyber Defense, thus the costs that the company support will increase, but even in this case until now the startup is not able to increase its investment in Cyber Defense, so the cost structure apparently has remained unchanged. Doing a more in-depth analysis I can see that the situation is actually different. In fact, taking into consideration the time that the engineers within the team must devote to the IT security, the company's Cyber defense cost increases exponentially.

Regarding K, the investment dedicated to Cyber security is equal to 15% of its income, thus exceeding € 500,000 per year; in this case are used mainly the internal resources but sometimes K asks for external consultancy. For K the costs structure is transparent and it is very far from the economic possibilities of small companies.
In conclusion it is possible to observe that with the advent of the Cyber threats the costs sustained by the small companies tend to increase considerably.