Eleven Paths

Cyber security for small and medium-sized companies

Keys to "new normality"

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

01

Executive Overview

The long and slow process of digitisation in small and medium-sized companies is a debate that has been going on for years. However, due to changes in consumption habits and production processes resulting from the health emergency of the COVID-19, this process was accelerated considerably in a short time.

Digitisation has gone from being a good opportunity for growth to being the lifeline. This has had the direct consequence that more progress has been made in recent months than in recent years worldwide.

Without going any further, in this segment, e-commerce in Argentina has grown by a 35% interannually in 2020, according to a report by the consultancy firm Focus Market.

In this digital framework, **the urgency for SMEs to have a cyber security strategy that makes this digitalisation viable takes on greater relevance.** Furthermore, companies belonging to this segment have already had a pending subject with cyber security for some time, as a large percentage of those that suffer a cyber-attack do not recover. Therefore, as in all major crisis, we must see the current situation of uncertainty as a historic opportunity for significant reforms in this business segment, which will help make their **businesses more sustainable and competitive.**

In this document, we will explain the current situation of cyber security in these companies based on its definition, the state of its digitalization, the consequences that the pandemic has had and will have this year, the ElevenPaths proposal and the benefits that this proposal brings to clients.

02

Context small and medium-sized companies

A. What is an SME? SMEs in figures

But… what is an SME? This is the question that is never absent from any conversation about companies in this segment and there is really no single answer to it. In other words, the answer depends directly on the geographical context in which it takes place. Each country or geographical area has the power to define what an SME is in its region. The definition could be given by those companies that are well below a certain number of employees, below a certain volume of turnover, or by a combination of both parameters.

For example, the number of employees of an SME within Latin America is similar, a maximum of 200 employees; which is not the same as the number of employees in the European Union, which is around 250 employees. And both are far from the US SMEs which are around 500 employees. In addition, in all countries there is an internal sub-segmentation of this type of company. An example would be, self-employed, soho, small and medium.

While in Latin America the definition is given by one of the two parameters, in Spain it is the combination of both that defines them.

What is clearly unanimous is the economic importance of the companies in this segment, as they are the backbone of the business network in all countries. They represent a high percentage in terms of volume and contribution to GDP.

In both Europe and Latin America, these companies represent 99% of the business network and at world level it is no less than 90% in any case. The contribution to GDP is 56% in Europe and 25% in Latin America.

Although companies in this segment are the most vulnerable in times of economic uncertainty, their good health is essential because they are the engine of the economy.

B. Digital Maturity

Digital maturity is the term that explains the level of adoption of technologies that has been achieved by a company within the existing possibilities. That is to say, what point in the process of digital transformation they find themselves at.

Therefore, we could say that **the digital maturity of a company tells us how much technology does for the progress of that company.** The final objective of this journey through the digital transformation will be to obtain the maximum benefit from the new technologies for the company's performance.

Depending on their degree of evolution towards digitisation, the solutions they need to improve their maturity and, consequently, the risks to which they are exposed, will vary.

Achieving this objective is not something that will happen overnight, but rather the companies following the path of progress gradually. What is more, it is not a path with a clear goal, since the digital environment is an ever-living environment in which updates are a constant.

It can be said that the digital transformation has two major dimensions: the internal and the external.

The external dimension

It refers to how the company presents itself to its clients and how it relates to them.
For this approach to be correct, it must be understood that these clients (existing and potential) are already digital, and therefore it will be necessary to adapt to this situation if we do not want to make a mistake.

This is where companies have been able to make the most progress, due to the direct impact that this relationship with the client has on their income. Therefore, if the client is already digital, it is essential to have that digital visibility as well and to be in the same environments as them.

Nowadays, the first action that any consumer carries out when he or she is evaluating the purchase of a product or service, is the online search for existing options. Knowing that this is the real situation of consumers, **companies must expose themselves in the most visible and efficient possible way on this digital platform.**

This does not mean that they all have to be able to sell online, but it does mean that they have perfectly understood all the existing solutions and have subsequently chosen and implemented the most beneficial of the possible solutions.

The internal dimension

It refers to everything that is transparent to the client. In other words, the internal processes and the way the company works.

By internal processes we mean many **tasks of a repetitive and mechanical nature.**
The digitalisation of these processes implies the use of all those tools that make these tasks more efficient and reliable.

It is common for companies in this segment to carry out a large number of tasks manually, with the subsequent economic cost, and with an increased probability of error. The inclusion of mature tools in the market that allow the automation of processes, such as CRM for all the company's data management, is a clear saving of effort. The digitalisation of these processes increases productivity and efficiency. The inclusion of technologies such as the Cloud and its collaborative tools, Big Data which helps to improve business decision making based on data or IoT technologies and their support functions for logistics, can also be productivity enhancers in many companies.

Regarding the way of working, it goes beyond the adoption of new technologies. A change in the way of working is a change of habit and this can take time so that the assimilation is correct.

Within these new ways of working, the use of **agile methodologies** must be taken into account. The main objective of this type of methodology is to have client satisfaction as a priority and, therefore, the company must have the capacity to respond quickly to any situation and adapt rapidly to changing environments.

However, the biggest change in corporate culture in recent times has been the way we relate to colleagues, clients and suppliers. We have gone from the traditional face-to-face way to establish relationships entirely online through videoconferences, telephone...etc. **A change that has been boosted by the arrival of COVID-19 and which has shown that those who have been able to adapt best are those who were most advanced in their digitalisation.**

The importance of the sustainability of SMEs for the economy means that governments must support them through financing. But this aid will only be temporary and the businesses that they are trying to continue in the market and those that wish to grow will necessarily be digital. Technology is more accessible than ever and the new companies that have emerged in recent months are already digital natives.

Finally, this is not the time to cut back on digital transformation, but rather to prepare for a sustainable and uncertain future.

According to a study carried out by Sage, 48% of SMEs will invest in digitalisation as part of their business strategy to adapt to the new situation.

C. COVID-19 - The "new normality" for small and medium-sized companies

On the 12th of March the WHO declared the COVID-19 as a global pandemic and as a consequence a few days later in some countries such as Spain a home lockdown was established in order to avoid the total collapse of the health system.

According to the survey on SMEs and the digitalisation of work in Spain carried out by Fiverr, **51% of the companies surveyed consider that they have not been prepared for this crisis** and among the main reasons are not being sufficiently prepared for teleworking (47%) and not having the necessary technology to deal with the situation (39%). With these data, the existing digitalisation deficiencies are quite clear.

This historic event took everyone by surprise, and at that very moment **the digital resilience of SMEs was challenged.** This meant that there were some - the fewest - that were more prepared to adapt to this new scenario, while others found themselves in a situation for which they did not have enough support.

This new context forced, overnight, a rethinking of the business model to curb the negative impact of the lockdown and to be able to survive. A solution had to be found to be able to maintain business continuity without the physical existence of the business. This business continuity meant that employees could continue to carry out their functions from home (managing orders, answering the phone, etc.) so that clients could keep on contracting these products or services through digital channels, such as social networks or websites.

> The online presence of the SME was not limited to having an e-commerce through which to purchase products but went beyond that and opened up new avenues of business for those sectors with a strong on-site tradition.

For instance, the restaurants that could not open in a face-to-face way and that knew how to transform quickly, turning to offer their meals through home food service platforms.

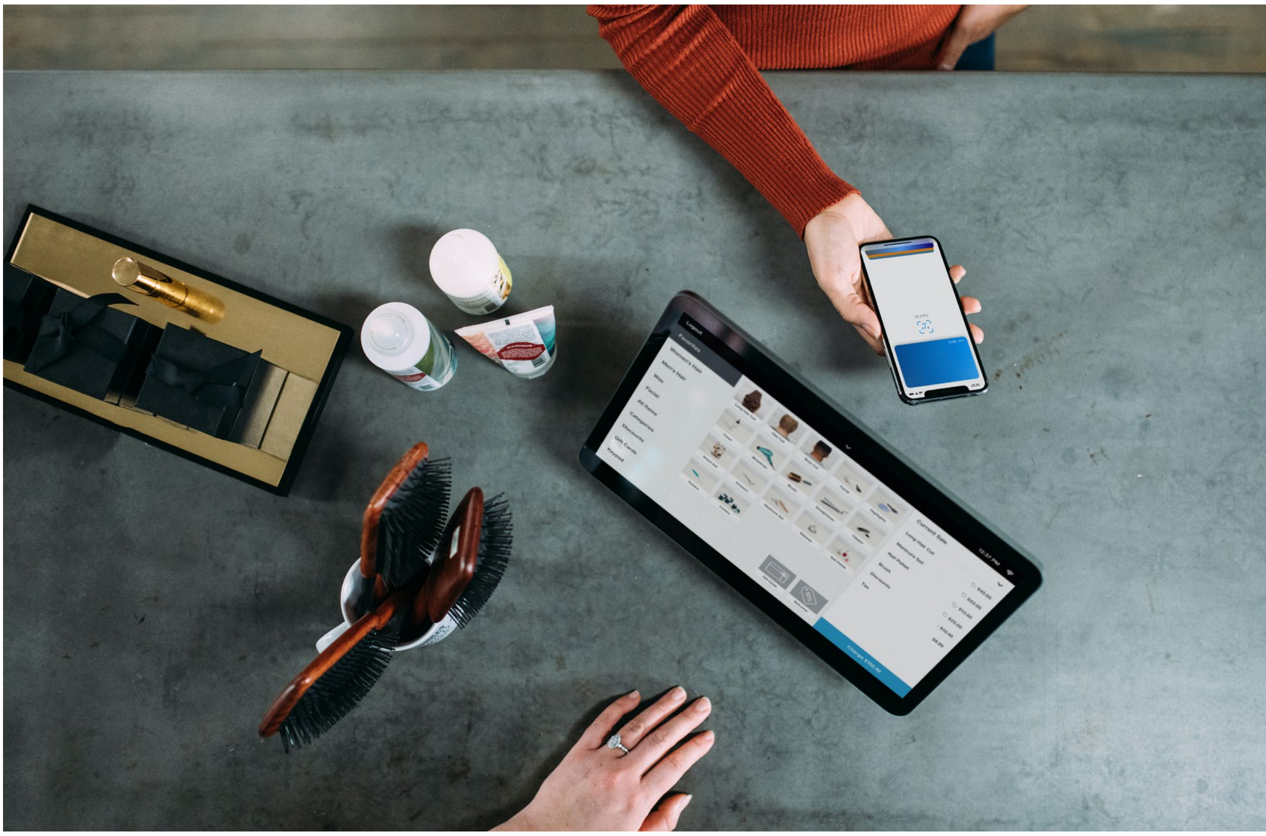
From the initial stages, as the situation evolved, and in the present day, it is possible to observe an evolution of business needs in terms of technology.

Starting with an initial rush to be able to work remotely in March, which increased interest in communication tools, improved connectivity, virtual desktops, firewalls and network monitoring tools. Following with the attention to infrastructure improvements in April, and security for remote workers in June, to the creation of online shops for retail businesses after the summer focused on relevant dates of mass consumption such as Black Friday or Christmas.

And it's not over here. According to Gartner, small and medium-sized companies will adapt their IT infrastructures so that employees can work from home throughout 2021.

Unlike the usual recommendations for a gradual adoption of technology, companies have been forced to jump over any barriers they may have on the road to digitisation in an abrupt way.

As a consequence of all this digitalisation that companies have had to carry out, they have been exposed to a greater risk of becoming victims of a cyber-attack, increasing the success rate of these criminals. All of this highlights the urgent need to make progress in cyber security so that digitisation is possible.



03

Main information security risks in small and medium-sized companies

A. Lack of awareness

Having a clear picture of the digital situation of SMEs, one can have a better understanding of the main risks they must face.

The greatest risk faced by SMEs concerning cyber security is the lack of awareness of this issue. Until recently, not everyone was aware of the importance of digitisation and was therefore unaware of the associated security component.

Many companies in this segment believe that they cannot be targets of cyber-attacks and are unaware of the dire consequences of suffering one despite being the main focus of attacks.

SMEs have the same needs in terms of information security as large companies, but with severe limitations in terms of budget, knowledge and qualified personnel. For all these reasons, SMEs are an easy target for cybercriminals.

> In Spain, according to the National Cryptology Center, during the first three weeks of March this year attacks on small businesses and the self-employed grew by up to 70%.

Therefore, this awareness must reach all employees of the company since knowing how to act at a given time is everyone's task.

B. Phishing and Malware

Some of the attacks that SMEs receive are all types of bugs (bots, trojans, adware, etc.), information leaks, internal and external threats, denial of service attacks, password attacks, etc. Next, we are going to look in depth at two of the most common ones and their consequences.

Phishing

It consists of impersonating a legitimate sender in order to obtain information through different channels such as SMS, telephone or e-mail. This last one is the most common due to the high volume of emails that are handled on a daily basis. Since phishing is one of the most common attacks, it is also the best known and, therefore, cybercriminals have increased their creativity in their methods to achieve their objective.

There are an increasing number of methods and they are more sophisticated: Pharming, Spear Phishing, Clickjacking, Phishing Spray and Pray are just some of them.

For instance, a small company receives an email impersonating a public organization that manages financial assistance to SMEs due to the pandemic, it and requests certain bank details in order to pay for this assistance. If the company does not detect this impersonation and provides its banking information, it may be giving all its financial savings to cybercriminals with the consequent economic bankruptcy that would mean the disappearance of the company.

Malware

Any type of malicious software that can infect computers and cause various types of damage. Malware can reach the company through different channels: through the Internet connection, email, security breaches, applications and public WIFI networks. In addition, there are different types of malware: worms, trojans, Spyware, Exploits and ransomware, which is the most relevant in recent times.

According to Kaspersky, **71% of ransomware attacks target SMEs.**

For example, while a user is browsing and downloads a file, without knowing that it is ransomware, a message appears on the screen informing him/her that he/she must pay a ransom if he/she wants to be able to recover the information from his/her computer.

This situation can lead to a worsening of the brand image towards its clients by the company in case it can recover the information and its disappearance if it finally cannot recover it.

C. Teleworking

If the risk of these attacks was already high, teleworking has increased it exponentially. In fact, **teleworking has become the main entry vector for business security.** The start and subsequent use of teleworking means that company information expands at different points, that employees sometimes work with personal equipment without security measures or with professional equipment that does not have these updated measures. Remote access and video calls are not always sufficiently secure, but their use is frequent.

In other words, companies that had some security measures already implemented in the company lost them by allowing their employees to work from home. For example, those that had already taken measures to control attacks such as phishing or malware within the corporate network, had to look for an alternative in the domestic environment.

While trying to adapt domestic cyber security measures to corporate ones, cybercriminals are profiting from this situation since the typology of attacks is the same, but with a clear decrease in security controls.

The impact of cyber-attacks is enormous in terms of both economic and reputational losses. This is why small and medium-sized companies will increase their security budget despite the difficult economic situation they are going through.

04

ElevenPaths' proposal

A. Peace of Mind

The current context of small and medium sized companies, between health emergency and economic emergency, where getting through is more difficult than ever, does not have to be at odds with the need to care for and protect their business which, as we have seen, is increasingly becoming more digital.

For all these reasons, we believe that it is important to focus the cyber security offer on this segment, towards the Peace of Mind of the client.

In other words, a solution that allows the company to focus on its own business because ElevenPaths takes care of its security. Moreover, they don't want to delegate only security without any guarantee, but they want to delegate that part of their internal tasks to the best suppliers in the market.

B. Managed security service

ElevenPaths proposes a cyber security solution based on the security management of its clients. In other words, by contracting this security solution, the SME is contracting a "solver" for its security needs.

With this, **ElevenPaths becomes the security manager of the companies in this segment**.

What is this solution like for the clients to reach their Peace of Mind?

These are some of its characteristics:

Managed:
The SME does not care about security and delegates it completely to ElevenPaths.

Supported:
Assistance is given both in security incidents/doubts and in the digitalisation process.

Simple:
Intuitive security services and better client experience.

In order to achieve these benefits of the solution, ElevenPaths provides its SMEs with the following capabilities:

Personalised service:
specific support for small businesses, speaking their exact same language and with high quality delivery.

End-to-end service:
companies are provided with a complete service covering the entire service life cycle. It is not just a resale.

Compatibility with the IT ecosystem:
the commercial security offer is compatible with other commercial offers from other IT areas (Cloud, Big Data, IoT...).

Trust in the operator: only an operator can guarantee security in communications by default. That is to say, from the first minute that communications are contracted, they are already secured without the need to contract additional security services, due to the network security deployments carried out previously.

Capillarity:
the large number of channels (face-to-face, online, telephone, etc.) through which we can reach them.

C. SME Security Centre

Due to the relevance of security management within this value proposal, there is a support centre for SMEs. This centre is a **group of experts who support the company at all times and who, through their knowledge of security and specialising in speaking the very same language as these clients, make security simple for them.**

This comprehensive service ranges from the first steps in protecting the company (with recommendations for the most appropriate solution), to regular reporting, deployment support, maintenance of security systems and resolution of threats and security incidents. All this with 24/7 availability every day of the year.

It also includes advice on regulatory compliance with the latest international security standards.

D. Training and technology

This proposal is therefore mainly based on management, beyond the underlying technology. The constant and rapid evolution of technology forces companies to delegate technical tasks to suppliers who are continuously updated and have sufficient experience in the sector to take over security decisions for them.

At ElevenPaths, the catalogue of information security services is extensive and is carried out in collaboration with the leading suppliers in the security market and some of our own developments

It ranges from the most common solutions for companies (regardless of their sector or degree of digitalisation) such as Antivirus and Antirsansomware, secure navigation, headquarters security, secure remote access and Clean Mail; to some more advanced ones such as Web Application Firewall, CASB, Digital Signature, GDPR compliance solutions, cyber security or even specific training in security matters to raise awareness among company employees.

Cyber security education for employees in any company is essential to ensure that they are knowledgeable about cyber security and aware of best practices in this area. This will make the company more prepared in case of a cyber-attack and less likely to receive them.

E. Benefits for the clients

Some of the benefits of this solution for clients would be:

- **Quality of delivery:** of the cyber security services in general, and of the connectivity in particular, since only one operator can provide the secure communications from the beginning.
- **Single invoice:** with the reduction in the management of suppliers. Unified connectivity and security, but other IT services such as Cloud, Big Data, IoT could also be joined...
- **Monthly:** periodic cost without the need for initial investment, making it more accessible to companies at any time.
- **Supporting the company in all its digital growth.** This cyber security solution grows hand in hand with the digitalisation of the company. Managing cyber security at all times.

05

Conclusions

The new reality in which SMEs find themselves after the pandemic, which happened this same year, has already marked a before and after in their level of cyber security awareness as a result of the digitalisation that they have undertaken in a disruptive way on some occasions.

Cybersecurity has become a fundamental pillar of the business strategy of companies in this segment and now is the time to implement this new strategy as effectively as possible.

ElevenPaths has created a clear and understandable security solution to help in the difficult task of bringing security closer to small and medium-sized companies, with an offer adapted to the protection needs of the company and taking care of the administration and maintenance of the company.

This is a comprehensive security solution. From the awareness of your needs, to the implementation of the solution and the resolution of incidents, together with the most specialised support for your needs.

From ElevenPaths, as part of the Telefónica group, and now integrated in the new Telefónica Cybersecurity Tech, they have years of experience in addressing the problems of SMEs with different types of solutions deployed in more than 11 countries. As well as agreements with the best manufacturers in the market, own developments made to measure for the companies in this segment, an offer integrated with the rest of the areas involved in the digitalization as Cloud or Big Data and the confidence that offers to be the secure operator, since it is the best positioned to be able to give security on the communications that it also offers.

Trust ElevenPaths as your travel partner in this new stage called to be the new digital revolution for small and medium-sized companies.

About ElevenPaths

ElevenPaths is Telefónica's cybersecurity company, part of the Telefónica Tech holding, which brings together the digital businesses with the greatest growth potential in the company

In a world in which cyberthreats are inevitable, as intelligent managed security services suppliers, we focus on preventing, detecting, responding and diminishing the possible attacks faced by companies. We guarantee the cyberresilience of our customers through 24/7 support entirely managed from eleven i-SOCs around the world with global operational capacity.

We believe in challenging the current state of security, a characteristic that must always be present in technology. We are constantly rethinking the relationship between security and people with the aim of creating innovative products capable of transforming the concept of security. In this way, we manage to stay one step ahead of our attackers, whose presence is increasing in our digital lives.

We work to guarantee a safer digital environment through strategic alliances that allow us to improve the security of our clients. Besides constant collaborations with leading organisations and entities such as the European Commission, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Industrial Cybersecurity Centre (CCI) y APWG.

More information

elevenpaths.com | **@ElevenPaths** | **blog.elevenpaths**

This document is intended solely to support its reader in the use of the product or service described herein. The reader is committed and obliged to use the information contained herein for personal use and not for any other.
ElevenPaths shall not be liable for any loss or damage arising from the use of the information contained herein or for any errors or omissions in the document or for the misuse of the service or product. The use of the product or service described herein shall be governed by the terms and conditions accepted by the user of this document for its use.

ElevenPaths

Telefónica CYBER SECURITY COMPANY