Intellectual Output 1

Rationalisation Phase

Deliverable: IO1/A1

BCT4SMEs

10.05.2021

Authored by: ASSERTED KNOWLEDGE

Project Number: 2020-1-UK01-KA202-078895

Co-funded by the Erasmus+ Programme of the European Union

REVISION HISTORY

Version	Date	Author	Description	Action	Pages
1	24/2/2021	AKNOW	Template Creation	C	8
2	10/5/2021	AKNOW	Comparison Analysis	C	40

(*) Action: C = Creation, I = Insert, U = Update, R = Replace, D = Delete

REFERENCED DOCUMENTS

ID	Reference		Title
1	2020-1-UK01-KA202-078895		BCT4SMEs Proposal
2			

APPLICABLE DOCUMENTS

ID	Reference		Title
1			
2			

Executive Summary

Small businesses confront several problems in the business economy. Many of them face barriers in entering trade markets, while others can confront difficulties in several sectors, such as transactions, data storage, cash flow, and security. Blockchain technology can offer a solution to these challenges, as it can have a wide range of applications in many fields, such as IoT, monetary exchange (bitcoin), storage, etc.

BCT4SMEs aims to support SMEs managers and owners in integrating blockchain technology and benefit from the advantages it comes with.

This document represents the deliverable of the activity IO1.A1 that refers to a National research aiming to identify the financial and security problems that SMEs confront frequently.

The present document contains information regarding:

- The security and financial issues that SMEs face in partner's countries;
- Information about the successful application of blockchain technology in the EU;
- Conclusions on the gap between the desired situation and the present situation.

Table of Contents

1. Methodology

During the rationalization phase, partners conducted a research to identify the current financial and security state of SMEs in their countries (UK, Netherlands, Spain, Greece, Cyprus, and Poland) and documented their findings in a National report. The current report comprise a comparison analysis of the National reports produced by the partners. The report is divided in two parts. The first part is the identification of the current problems in terms of finances and security that SMEs face, while the second part refers to the winning practices from SMEs that use blockchain technology to address the issues that have proved as the most challenging for them.

The scope of the research is to identify and compare the problems and identify the solutions that can address this situation. The next activity is the validation phase in which partners will communicate with a range of SMEs to assure that the problems identified in this phase are the most important problems for them.

2. National phase

2.1 Financial Challenges for SMEs

CYPRUS

The desk research in Cyprus focus on the main financial challenges that SMEs confront and their consequences (European Investment Bank, 2017). It presents: (i) Information on the macroeconomic market environment in Cyprus and (ii) The lessons learnt from past experiences with financial instruments (FIs) in Cyprus.

SMEs are the backbone of the Cypriot economy, since they produce nearly 75% of the value added of the non-financial business sectors, which is 17% higher than the then EU average (European Investment Bank, 2017). At the same time Cypriot SMEs generate 83% of jobs in the non-financial sectors, in contrast to approximately 66% which is the EU average (ibid). As a result, promoting growth and investment among SMEs is a top EU policy priority, which requires that financial challenges are tackled.

As defined in the Small Business Act for Europe (SBA) Factsheet report for Cyprus in 2019 (European Commission 2011a), Cyprus' SBA performance is mixed. State aid & public procurement and internationalisation are now both above the EU average. In particular, State aid & public procurement improved substantially compared to year before that this was below the EU average last year. Secondly, the Entrepreneurship, 'responsive administration' and skills & innovation are in line with the EU average. Finally, 'Second chance' and 'single market´ are below the EU average. In fact, Cyprus is among the EU's weakest performers for SMEs' access to finance (ibid).

The main European Investment Fund (EIF) SME Access to Finance Index (ESAF) results for 2018 are presented in Figure 1 (Kraemer-Eis et al., 2019). The leaders in this updated version of the ESAF is now Sweden, with Germany and Finland in the second and third place, respectively. Greece is ranked last in the ESAF ranking for the sixth consecutive year in a row, preceded by Cyprus and Romania.

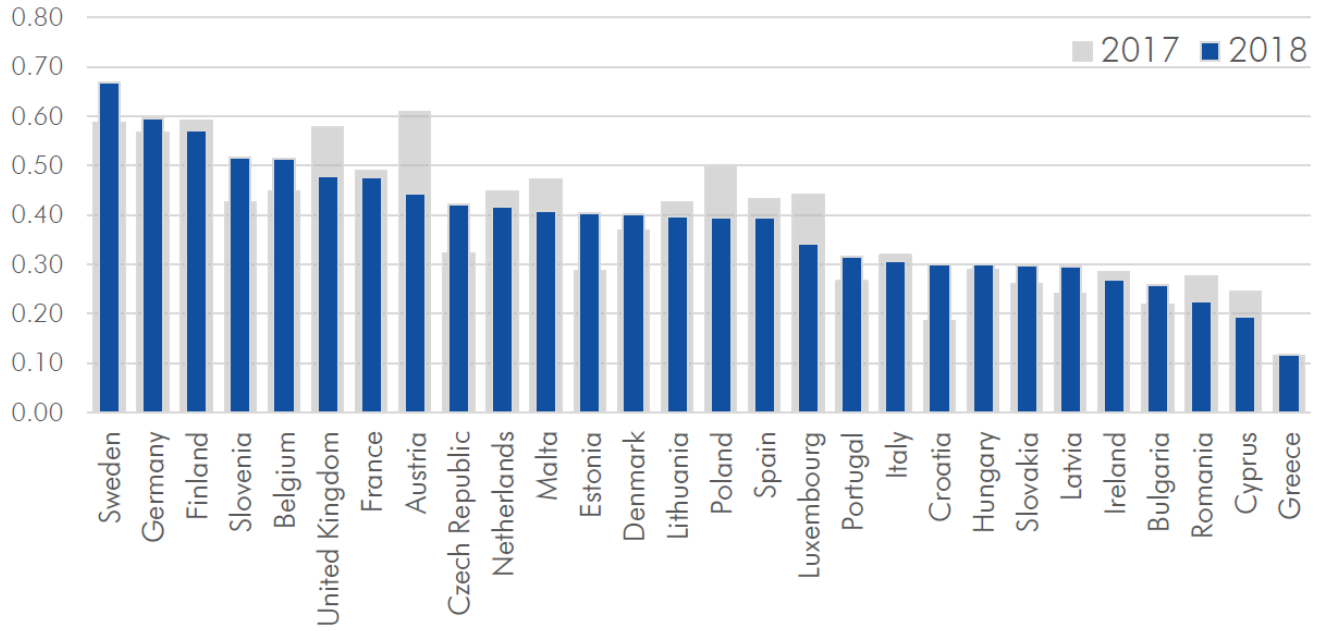


Figure 1: The EIF SME Access to Finance Index: country comparison and evolution over time – Source: Torfs (2019)

The primary challenge faced by Cypriot SMEs is generally the lack of access to financing. In order for SMEs to grow and/or drive innovation they need to be able to have access to finance. Especially in Cyprus, following the financial crisis, financial intermediaries have been limited by creditworthiness constrains, and by the need to apply strict risk management standards, making it difficult for SMEs to qualify for access to finance. Therefore, they are overly dependent on bank lending, while alternative financing options such as Venture Capital (VC), Business Angels (BA) and crowd funding are limited. This significantly hampers their capability to invest and grow. According to a European Commission's survey, 25% of Cypriot SMEs cited difficulties in access to finance as their most important concern, the highest across EU (European Commission, 2016). As such, the introduction of FIs could be a good means to develop businesses in Cyprus.

On the other hand, Cyprus performs above the EU average in State aid & public procurement (European Commission, 2019a). It has the EU's highest score for the proportion of bids coming from SMEs. This score is one of the highest percentages of awards won by an SME. Despite a drop, in 2019, of approximately 7 percentage points in the share of the total value of public contracts awarded to SMEs, it is still above the EU average (ibid). Still a problem that remains in terms of State aid & public procurement is the long time required to receive the actual payments.

Despite the fact that the Cypriot government, since 2008, has defined and put in place some actions and specific measures to financially support SMEs, still access to finance and particularly investments is a continuous and key obstacle for start-ups and SMEs (European Commission, 2019a). In specific, the Ministry of Finance introduced several tax incentives to encourage individuals to invest either directly or via investment funds in innovative start-ups and SMEs (European Commission, 2019b). This was performed in order to counter the drop in public financial support. Moreover, in other actions, the Ministry of Energy, Commerce and Industry also introduced measures to extend finance and investments for specific target groups (e.g. young people and women). Another relevant measure was adopted, namely the Alternative Investment Funds Law that aims to introduce: (i) the Reserved Alternative Investment Fund (RAIF); (ii) limited partnerships with legal personality as an alternative investment fund vehicle; and (iii) arrangements for establishing a variable capital company to increase

the versatility of limited companies as a corporate vehicle for open-ended funds (European Commission 2019a).

Duruflé, Hellmann and Wilson (2017) identify the main elements of a strategy to help Europe catch up to the US in terms of scale-up funding: creation of larger venture funds and a venture debt market, reinvigoration of tech IPOs, improved markets for secondary shares and avoiding selling companies too early (Duruflé, Hellmann, & Wilson, 2017).

The entire European economy is negatively affected by late payment. To protect European businesses, particularly SMEs, against late payment, the EU adopted Directive 2011/7/EU on combating late payment in commercial transactions in February 2011. Each year across Europe thousands of small and medium-sized enterprises (SMEs) go bankrupt waiting for their invoices to be paid. Jobs are lost and entrepreneurship is stifled. Late payment causes administrative and financial burdens, which are particularly acute when businesses and customers are in different EU countries. Cross-border trade is inevitably impacted.

On the face of it, late payments to businesses in Cyprus have fallen significantly in the post-bail-in period, with fewer than half of all respondents affected (ACCA, 2014). It is almost certain that this trend reflects the reduction in trade credit, as opposed to an improvement in credit conditions. If this interpretation is true, then it suggests that a substantial number of businesses in Cyprus have reverted to working mostly on a cash basis, post-bail-in.

Although things have improved since then, still the amount of time it takes to get paid by customers and the share of bad debt loss (i.e. the number of receivables that have to be written off because of not being paid) is among the highest in the EU (European Commission, 2019a). According to a 2016 Commission report on the implementation of the Late Payment Directive (European Commission 2011), Cyprus ranked last for payments in business to business (B2B) transactions with an average payment period of 85 days (business to public (B2P) 84 days) (Commission Staff Working Document, 2016).

In addition, the average delay in payments from public authorities continues to be a significant challenge for SMEs in Cyprus. The length of delay continues to be among the longest in the EU (European Commission, 2019a).

For Europe's valued SMEs, any disruption to cash flow can mean the difference between solvency and bankruptcy (European Commission, 2011b) . The economic crisis presented numerous difficulties, but for SMEs the challenges presented by late payment have grown disproportionately as credit lines and bank loans become less available. In many countries, the loan financing gap appears to have increased (see Figure 2). In Ireland, Austria and Germany (north-eastern quadrant), banks tightened the supply of credit to SMEs while facing increased loan demand (Kraemer-Eis et al, 2017) . Furthermore, banks in Cyprus, Greece, Malta, Latvia, Slovakia Luxembourg and Italy kept credit standards constant but reported an increase in loan demand. In Belgium, Slovenia and Spain, loan demand reportedly stayed constant, but credit standards were tightened (considerably so in Belgium) (ibid). All these cases imply an increase in the financing gap, from the (supply) perspective of bank. In overall, Cyprus faces serious challenges in terms of access to finance, including other credit lines and bank loans, investment funds and heavy delays in terms of payments, which all contribute to the cash flow management issue.

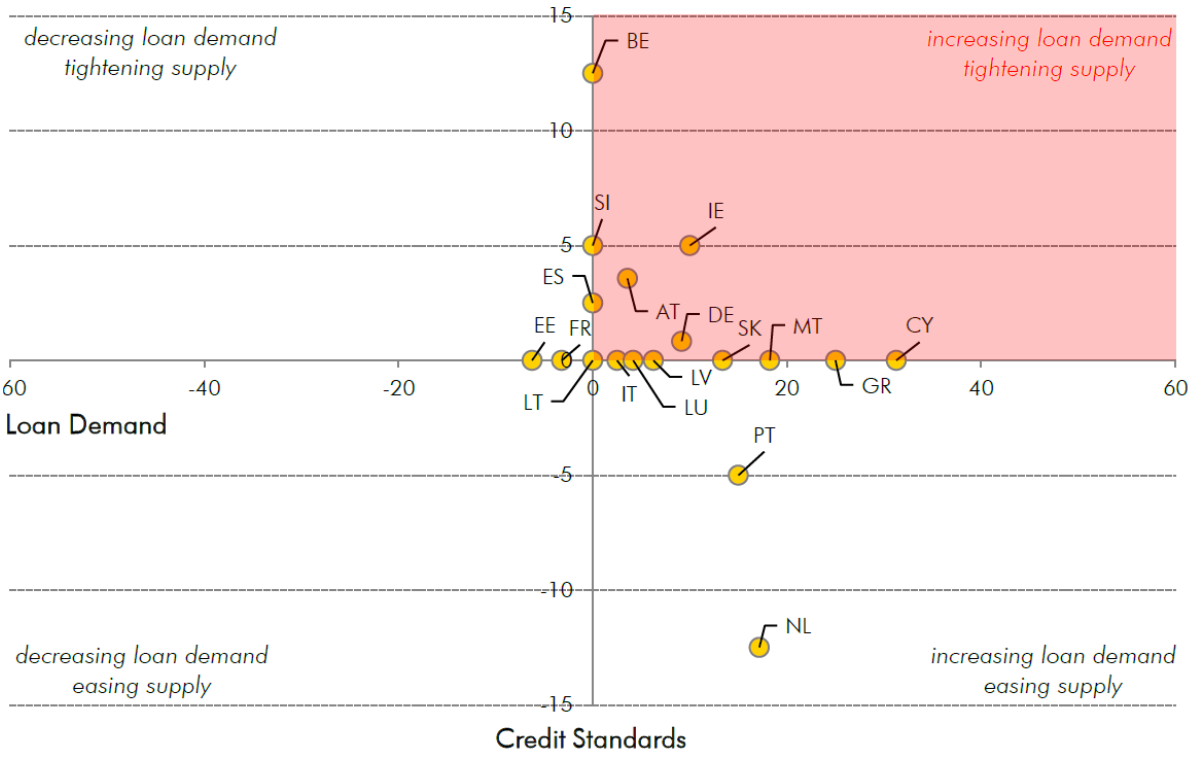


Figure 2: The SME financing gap from a supply perspective (HY1/2019) – Source: Authors, based on ECB Bank Lending Survey (ECB, 2019c)

GREECE

Most of the Greek enterprises (99.9%) are SMEs, and most of them are micro-enterprises. The financial crisis in 2010 and the sovereign debt crisis had a profound impact on the Greek economy. During the following years SMEs had many issues in loans lending while, in the 2017 the SME lending slightly increased, following a 7-year period of consistent decline. For many years, credit to all businesses was falling, but in 2016, SME loans' stock increased to EUR 48.1 billion, but again declined to EUR 44.7 billion in 2017 and EUR 41 billion in 2018 (OECD, n.d).

In fact, Greece is one of the weakest performers in the EU in access to finance. Venture capital is not available in Greece, while the funding for new and growing firms in Greece is one of the lowest in the EU. Surveyed experts have estimated the availability of equity funding for new and growing firms in Greece to be one of the lowest in the EU. Greece is also among the worst performers in three indicators measured by SBA: share of rejected or unacceptable loans to SMEs, the willingness of banks to provide a loan, and access to public financial support (SBA Fact Sheet- Greece, 2019).

One problem the Greek companies (start-ups and developing ones) face is the bureaucracy. As a result, a great number of businesses who manage to overcome the initial difficulties and started their activities do not survive more than two years. This is also a result of the very limited support offered by the public sector and the related chambers of commerce, trade associations and similar institutions.

As a consequence, at the initial development stages, SMEs have to depend on funds coming mostly from the owners, their families, friends, and sometimes from venture capitalists. In the later development stages, SMEs are primarily funded from their own funds coming from surpluses or other

means of external capital, while at a later stage, they have access to bank loans and other groups of companies from the SME sector. External acquisition of capital by SMEs is the factor that allows them to finance investments aiming to further development and growth. The main sources of these external sources of capital for the SMEs are non-banking sources, such as trade credit, lease, factoring, franchising, etc., and bank loans which could be short-term and/or long-term (Katsioloudes & Jabeen, 2014).

Another problem that the Greek SMEs face is the limited cash flows. According to a research conducted by the Piraeus Bank, most Greek SMEs operated with limited liquidity in 2018 due to the economic crisis. In fact, the companies that have adequate cash flows in terms of liquidity, efficiency and solvency and are ranked in the highest rating ("a") of ERS, is only the 7.9% of the companies (mononews, n.d).

Furthermore, a survey from the European Central Bank, revealed that access to finances is the main concern for SMEs in Greece, while is the only European country which is affected to a great extend from this problem. When asked whether "access to finance" was as a problem in their current situation, as SMEs in Greece continued to perceive it as a very important problem during the years. A relevant problem for Greek SMEs, as already mentioned, is the need for bank loans. In particular, in Greece, the availability of bank loans has tightened further during the last years, as 38% of SMEs identified the presence of increasing difficulties in accessing bank credit for SMEs, but also for large enterprises. At the same time, SMEs in Greece reported negative expectations regarding the availability of internal funds while expect further challenges in bank loans, bank overdrafts and trade credit. Another important problem of the banking sector in Greece is the size of the Non-Performing Loans, which also hinders the availability of bank finance to SMEs.

In addition to this, SMEs in Greece have noticed a negative perception of banks' willingness to lend (-30%, down from -22%) and access to public financial support (-51%, down from -36%) during the last years. Also, many SMEs mentioned fear of rejection as a factor discouraging applications for a bank loan, while 9% of SMEs reported that their loan applications were still pending (European Central Bank, 2015).

Nevertheless, many Member States are trying to provide alternative solutions for available finances to SMEs, beyond the banking system and diversify the types of finance available to SMEs. Alternative solutions comprise factoring or crowd-lending, which have recently shown strong growth rates in some Member States. In Greece alternative markets like crowd-lending are not yet established and, thus these types of financing do not exist or are poor.

In the country, there is a single digital portal to inform public audience on available financial instruments. The portal was created by the Directorate for the Support of SMEs of the General Secretariat of Industry & SMEs of the Hellenic Ministry for Economy & Development. The portal gives information and guides SMEs to accredited organisations that provide financial instruments and opportunities (European Commission, 2020).

We can conclude that the main problems that SMEs in Greece have are access to finances in all their development stages. In particular, bank loans are really hard to be accredited to the companies, while another critical issue that many times comes as a result of this situation is the limited liquidity.

UK

SMEs are of huge importance to the Scottish and UK economies, representing about 99% of the business population. And although in many ways, the UK has a reputation as being a hospitable environment for SMEs, with studies suggesting that it is relatively favourable toward SMEs in terms of issues such as tax simplification, regulatory burden, and taxation overall, there are a number of financial challenges for SMEs in Scotland and the UK more broadly. Some of these are perennial and general challenges that any SME anywhere might expect to sometimes encounter, others are more ephemeral challenges, specific to this time and this country. Whatever the source of the challenges, however, they are challenges, and will impact SMEs either way.

Starting with the more particular challenges, Brexit has until very recently been the highest on the agenda. The UK's leaving of the European Union and the resultant customs and regulatory barriers that have since been erected is one of the defining economic changes of the era, and as such for many SMEs, it is a defining challenge. Almost 40% of SMEs in the UK claimed in one survey that they felt they would be worse off as a result of Brexit, with only around 10% predicting that the opposite would be true. Indeed, in the short few months since Brexit has begun in earnest, the consequences for certain industries – most notably the Scottish fishing industry – have been severe. The delays and confusion caused by new border checks and the inevitable bureaucracy that accompanies them has been terrible news for supply chains, and in particular for those products that are perishable.

The other main issue is a more widespread one, if hopefully now in its closing phase. That is of course the COVID pandemic, which has forced the closure of many SMEs during repeated lockdowns and considerably reduced foot traffic and income even when they were allowed to open. Given the nature of this, in many ways the difficulty is most concentrated on retail businesses, but the impact has been enormously broad across the economy. On this challenge, it remains to be seen the full extent of the difficulties that SMEs will face, whether there will be a strong economic rebound immediately following vaccination or whether customers will take a longer time to return to their pre-pandemic spending habits. That being said, however, reduced footfall is not a COVID-specific problem, but rather part of an ongoing trend in which SMEs with physical shop locations have been losing out at the expense of online businesses. The COVID pandemic, as mentioned, has certainly accelerated this, but it again remains to be soon whether or not changes in consumer habits will continue after the pandemic's end.

Related to this is one of the key more perennial financial challenges faced by SMEs. Technology, although a hugely important source of opportunity for SMEs, can in some cases also be a burden if they are not properly equipped. Surveys and studies of this suggest that one of the biggest worries SMEs have, and especially around technology, is the cost of introducing it. This is demonstrated, for example, by one study suggesting that over 40% SMEs believe a cashless society would be bad for their business. Ostensibly, there are many ways in which SMEs could considerably benefit from such a cashless society, but it is most likely their lack of infrastructure and preparation to handle such a society that intimidates them. This infrastructure can be costly, and as such presents a financial challenge.

A further relevant point is the changing nature of banking for small businesses. Banking is crucial for SMEs and having sufficient access to the funding and investment they can facilitate is hugely important. The challenge here is that banking is in many ways becoming harder for SMEs, with branch closures being increasingly common and online banking more mainstream. While in some ways this is easier, reports suggest that this also denies SMEs the more traditional relationships with staff at their local bank and some of the flexibility that often accompanies this. This challenge is especially egregious for

those SMEs not quite large enough to have their own finance department, as the loss of friendly advice and expertise from a local bank branch is amplified.

Part of the knock-on effect of this is cashflow problems. As basic as it sounds, this is a very common problem that businesses face: more money going out than coming in. The consequences of this can be disastrous, including late payment of employees or other debts, or even inability to accept work, but it is something that 57% of UK small business owners report having faced. It is also important to note that one of the effects of cashflow problems, combined with access to finance issues in banking as mentioned above, is that the share of exports coming from SMEs in the UK has been declining notably in recent years. With these challenges, cashflow and exports, it is difficult to ascertain the precise nature of which industries or sectors are having the most sever issues with cashflow in the UK.

NETHERLANDS

The country is facing the deepest recession in 100 years, despite the coronavirus support packages. This recent crisis has affected most the SMEs around the HORECA, the trade, the transport equipment, the production of the culture, recreation sports, and the tourist industries (NL Times, 2020a), but enterprises in other industries (construction, food manufacturing) have not yet seen the full impact of it. An economy that is highly dependent on exports of goods and services has been highly vulnerable to drops in demand from abroad (NL Times 2020b).

It is true that the country's economy is undoubtedly in a better condition than other EU countries', as a result of the smart (partial) lockdown and the high level of digitisation which helped absorb the first blows of the pandemic, nevertheless the damage is done.

Small and medium-sized enterprises in the Netherlands are generally considered to be the engine of the Dutch job industry, as it is the case in Europe. In this sense, Dutch SMEs do considerably contribute to the national macro-economy. 443,842 enterprises were recorded as SMEs in Netherlands, according to 2020 data (STATISTA data, 2020).

Annual surveys by Euler Hermes and Bibby have recorded that SMEs in the Netherlands face several struggles with **capital inflow** (FACTRIS 2020) as a result of managing late or unpaid invoices, as well as with the limited financing by banks, the most considerable external source of financial support for SMEs: Dutch SMEs are obtaining bank loans less often than SMEs elsewhere in the eurozone (European prespective, n.d)

Access to finance was recorded to be the most important issue for 6% of Dutch SMEs, slightly lower than the EU average (at 7%).

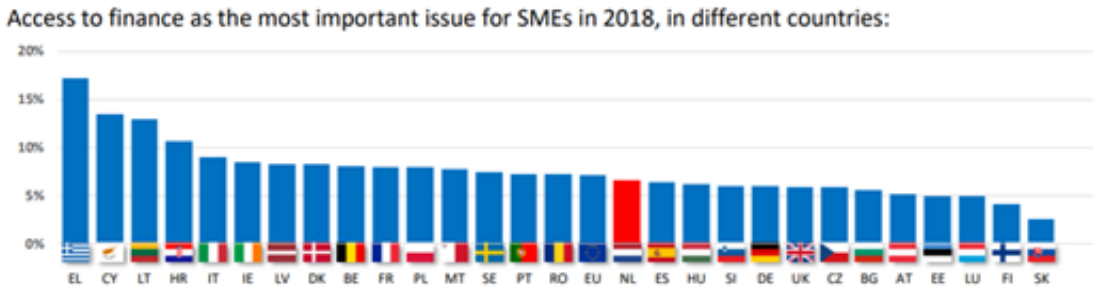
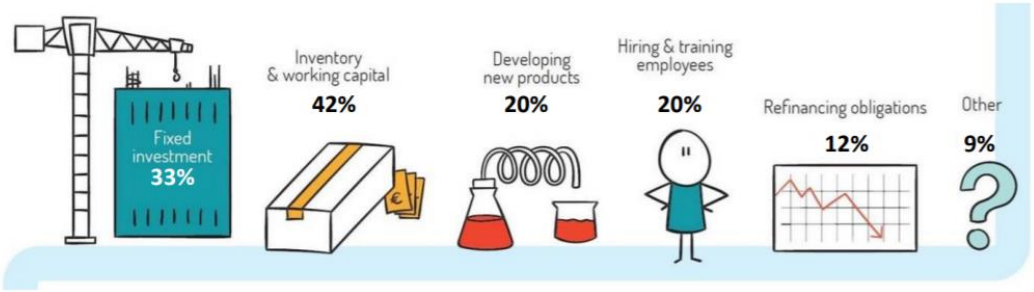


Figure 3: Access to finance as the most important issue for SMEs in 2018, in different countries

In the same report with EC data from 2018 (European Commission 2018), it was stated that bank loans remain the relevant form of external financing for 42% of Dutch SMEs (compared to 47% at EU level). Some loan applications were rejected (3%), and of those successfully through 11% received less than they applied for, while a considerable amount of them did not even apply, out of fear of rejection.

The following image offers information on the sectors which the Dutch SMEs use the financing for:



Blockchain promises to solve this problem with 'smart contracts' which are self-executed, coded agreements that deliver guaranteed outcomes, under certain conditions, which will make transaction processes faster, simpler and efficient.

POLAND

In Poland, SMEs constitute the vast majority of enterprises (99.8%), of which more than 2 million are micro-enterprises (employing fewer than 10 workers). Thus, employment rests to a large extent on their shoulders (they are responsible for 68.7% of all people employed in enterprises). The dominant sector of SME in Poland is services (52%) trade (23.5%), industry (13.3%) and construction (10.3%). The significance of SMEs for the economy is enormous. However, this sector is facing its own problems. The financial challenges will be presented here (PARP, 2020).

The launch or ongoing operation of enterprises in an industry is, of course, linked to the raising of funds and their allocation. The primary objective of enterprises is naturally to maximise market value. In order to make it easier for SMEs to make a profit, there must be an attractive legal background and transparency and opportunities to raise capital.

Problems of a financial nature can usually be linked to external financing. The main problem is limited access to sources of finance. Both bank loans for SMEs and external investment in them are associated with high risk (Rymarczyk J. 2019).

At the first stage, therefore, their financing often takes place mainly using own resources, thanks to financial support from family and friends. Recently, crowdfunding services have become more and more popular. In a nutshell, they consist in raising money from fundraising platforms such as Kickstarter, Experiment or Polish platforms such as Wspieram.to or PolakPotrafi. Croundfunging itself is often associated mainly with start-up activity. Apart from that, there are also methods such as using business angels or venture capital funds.

The first problem faced by Polish SMEs (although this is common problem in big part of Europe) is obtaining funds for setting up and starting a business.

Only 27% of SME companies use external finance, which reflects a reluctance and fear of getting into debt. Unfortunately, innovation is expensive. SMEs are encouraged to use external financing, for example through de minimis guarantees (guarantees to secure the repayment of a working capital or investment loan) offered by BKG (Wierciszewski M, 2021).

Another problem that afflicts Polish SMEs is the lack of timely payments from contractors. It is estimated that almost half of Polish companies are affected by this problem (in pre-pandemic reality). It causes serious problems with financial liquidity, which affect the functioning of the company and its development opportunities (Witkowski R, 2020). The problem of financial liquidity and causing so-called vicious circle of payment backlogs (is also reinforced by the Covid-19 pandemic. Currently (in pandemic reality), the problem with financial liquidity is reported by 7/10 SMEs.

The problem of overdue payments causes a snowball effect. The BIG InfoMonitor research states that micro companies' entrepreneurs, forced by the situation, will not be able to pay their own contractors (due to lack of financial liquidity). The pandemic itself is also a huge (probably the biggest at the moment) financial crisis for the SME sector in Poland. It has frozen the operations of many businesses, necessitated a wage freeze for employees or even caused businesses to collapse (Wiadomości Handlowe, 2020).

Funding from the EU, the European Investment Bank or public money has been a solution to some of the financial problems associated with, for example, paying for the necessary research or implementing innovation for some SMEs. However, this is a drop in the ocean of needs.

SPAIN

The closure to the public of non-essential businesses due to the pandemic has been particularly hard on SMEs whose business revolves around the physical presence of their customers.

The problem is that beyond the occasional closures, customers' consumer habits have changed, perhaps structurally. Consumers who have never shopped online before have now lost their fear, have become used to this way of purchasing goods and services, and will most likely continue to do so in the future.

In this context, e-commerce can be an alternative for many SMEs to expand their business and attract new customers.

From bars and restaurants that have so far not considered home delivery to companies that offer services that can be delivered over the Internet, such as training or consultancy, there is now an opportunity for growth through e-commerce.

Consequences: Another alternative for expanding the customer portfolio is exporting. In Spain, international activity has traditionally been concentrated in large companies, while SMEs have found it much more difficult to go abroad. Now, with COVID-19, exporting to new markets could be an opportunity for them.

The fear of not knowing where to start is one of the main obstacles that SMEs argue against going abroad, which can be overcome with specialized advice. In this sense, tools such as the "Self-diagnosis for access to new markets" can be used, which the Directorate General for Industry and Small and Medium-sized Enterprises offers on its website.

Spanish companies, which are characterized by being very small (94 per cent of them have an average of less than 10 employees), may have serious difficulties to continue in the market if they do not consider joining forces with other companies.

To compete with guarantees in this complex economic scenario requires companies of a larger average size.Alliances, mergers, or acquisitions may be different options to achieve this. This is not an easy challenge, as it involves even cultural changes. For this reason, many Spanish entrepreneurs prefer to act independently, even if this means facing greater difficulties.

In an environment in which the standstills in activity since last spring have led to an imbalance in the cash flows of many companies, from which they are still trying to recover, it will be essential to continue to guarantee an adequate level of liquidity to develop activity.

Although the extension of the maturity and grace periods of the loans guaranteed by the Official Credit Institute (ICO) has provided companies with a lifeline, it will be necessary to continue to focus on reducing costs and adjusting short-term assets and liabilities in order to adapt the flow of receipts and payments this year. It will be particularly important to manage customer collections, trying to prevent late payment figures from soaring.

The role that companies play in this area is essential. The business models of the future cannot look the other way and have to put the environment at the center of business decisions. The majority of SMEs are beginning to understand terms such as 'circular economy', 'recycled materials' or 'energy efficiency' and some are already applying these concepts in their business models.

In the coming year, many SMEs will continue to rely on this way of working, which will start to gain traction among small businesses and become part of the everyday life of SMEs.

A significant proportion of entrepreneurship in Spain is concentrated in sectors which are more vulnerable to the credit crunch. Part of SMEs' access to credit depends on the development of more entrepreneurship in other sectors in addition to these.

The real estate and construction sectors are particularly vulnerable, firstly, because they are businesses that often require long term investments, often with few projects in the pipeline on which they are overly dependent and a significant need for liquidity, as they have to make regular payments and their collections tend to be concentrated.

Moreover, these are sectors that are not only dependent on their own credit, but also on that of their clients. Vulnerability therefore increases very sharply in times of crisis or when there is simply a certain likelihood of a slowdown in the sector. This issue is most relevant_construction and real estate sectors.

Getting credit requires confidence. To achieve this, the first thing we need to know is what our situation is and how it could change. And then we must be able to convey that we are aware of the risks and that we have the capacity to respond.

Some responses are executed once the risk has materialised. For others, it is important to act beforehand. Clear examples of this are, for example, taking out insurance or hedging transactions to hedge against risks such as interest rate, currency, etc.

Unfortunately, a not insignificant number of SMEs, instead of facing up to risks and managing them properly, systematically avoid them. Precisely in the financial sphere, many do not properly analyse debt alternatives. They reject them because they see a risk in them and often miss out on options for financing investments that are essential for their survival.

It is common that many SMEs, at the beginning, only consider exporting or importing. From that moment on, possible future scenarios have to be considered. Attention should be paid, for example, to the possibility of opening branches, looking for partners, financing in the target country, contracting, making all kinds of investments, etc.

Lending to a company that is lagging behind digitally carries high risks. If, in addition, it does not plan to implement actions to overcome it, it can be even more complicated.

And this is not only a strictly digital problem, but an organisational problem in the broadest sense. In general, a lack of digital culture is an indication that an SME is not very flexible and adaptable to the circumstances of the environment. They tend to be businesses that suffer greatly from adverse internal or external circumstances, which does not make it easy for them to borrow funds.

Moreover, the difficulty is compounded by the fact that there may be a competitiveness problem. Many of the investments that can improve productivity and costs cannot be afforded under conditions of digital lag.

Financing involves the future of business, which inevitably involves technology. And it is in the goods or services we launch on the market where providers of third-party financing and any other third party have the best reference of how our company relates to technology.

Even in the most traditional products, there are options for technological upgrades. We can show that we are up to date in distribution, in the way we serve the public, in after-sales services, and so on.

This is the part that shows something that is not seen and that matters a lot to third-party finance providers: the organisation's relationship with technology. That is, having products that are up to date is a sign that the workforce is up to date, which greatly improves our prospects of generating cash flows in the future with which we can pay back what we borrow.

We must have sufficient training to deal with the corresponding type of activity. In an ever-changing world, it is not easy to keep up with everything. What does give a lot of confidence to anyone who can lend us money is that we make an effort to provide quality continuous training for the managers of the company and for the whole staff. The same applies to consultancy. It is undergoing a process of specialisation. The consultant is becoming a kind of business partner who helps to fill gaps and seize opportunities.

Indebtedness requires payments to be made in the future and creditors are doubly interested in cash management. Firstly, because it is necessary to generate the expectation that, at all times, there will be sufficient liquidity to meet payments. Secondly, because excess cash is a drag on the profitability and viability of many small businesses.

It is very important to maintain a balance that allows us to generate credibility. On the one hand, we have to show that we know how to make good forecasts and keep control of cash flows. This implies not only having as good an idea as possible of the expected values of receipts and payments, but also of the possible risks that may affect them at any given moment and correctly monitoring their evolution.

It is also very important to improve the knowledge of many small entrepreneurs in two aspects. The first is related to the sources of short-term financing available to them. The second is the use of solutions that allow them to manage their cash flow in a way that is appropriate for their business.

2.2 Security Challenges for SMEs

CYPRUS

Commonly larger enterprises have more digital capabilities and are more concerned with their security, while SMEs tend to be less digitally intensive, have less ICT capabilities and smaller to no IT teams. Therefore, depending also on specific factors, such as the nature of their business, their sector of activity and/or immaturity to apply appropriate digital security practices, SMEs have a higher probability of suffering an incident (Financial Tribune Daily and Contributors, 2017). Furthermore, although digital transformation is essential and required given the vulnerabilities that the COVID pandemic revealed, still it increases SMEs exposure to digital security risks and likelihood to be victims of cybercrime. In fact, it makes SMEs more exposed to digital security incidents and making them more reliant on digital technology (ibid). The Internet of Things increases digital connectivity, the number of vulnerabilities to exploit and the potential frequency or probability of attacks, while other technologies such as cloud computing further increase the exposure due to the use of cloud services and data storage in the cloud. Cyprus has a cybersecurity strategy in place since 2012 (European Union Agency for Cybersecurity, 2012), while the Digital Security Authority has proposed a new cybersecurity strategy, which is pending final approval from the Ministry of Communication and the Council of Ministers (European Commission, 2018).

Cybercrime is considered a huge threat to states' economies. Therefore, it is critical to raise awareness, to have a good level of collaboration with relevant stakeholders but most importantly have the right tools that can shield business and the economy in general. In an effort to address the above issue the conference titled "How S@fe is Your Business?" was organized in Cyprus back in 2017, by the by the Cyprus Chamber of Commerce and Industry and the Cyprus Neuroscience and Technology Institute (Financial Tribune Daily and Contributors, 2017). It was addressed, among others, by Luigi Rebuffi, secretary general of European Cybersecurity Organization and George Michaelides, commissioner of Electronic Communications and Postal Regulation of Cyprus (Financial Tribune Daily and Contributors, 2017). It is estimated that 43% of cyberattacks target SMEs. Cybercrime costs are projected to reach €2 trillion ($2.15 trillion) by 2019 whereas 19% of business in the EU admitted that they have been attacked. Some 68% of funds are lost because of a cyber-attack and these funds were declared unrecoverable. In 2015 there were 38% more security incidents detected than in 2014 while only 38% of global organizations claim they are prepared to handle a sophisticated cyberattack.

Digitalization has made the protection of trade secrets increasingly difficult. The revolution in data codification, storage and exchange (i.e., cloud computing, emails, USB drives) are prime drivers of a rise in trade secret infringements (OECD, 2019a). Increasing value given to intellectual property (and de facto its misappropriation), staff mobility and changing work culture and relationships (e.g., temporary contracts, outplacement, teleworking) or the fragmentation of global value chains (with more foreign parties involved within more diverse legal frameworks and uneven enforcement conditions) also contribute to increase exposure and risk of disclosure (Almeling, 2012).

A trade secret is a valuable piece of information for an enterprise that is treated as confidential and that gives that enterprise a competitive advantage. Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) harmonises the definition of trade secrets in accordance with existing internationally binding standards (European Commission, 2019a). With much delay, in 2021, Cyprus has transposed the directive for the protection of undisclosed Know-how and business information (trade secrets) against infringements.

Data are increasingly generated along business operations, e.g. production and delivery (process data), and compiled at various stages of business transactions (user, consumer and supplier data) (OECD, 2019a). User, consumer and supplier data are crucial for developing market knowledge, improving customization and shaping new products and business models. In addition, the COVID-19 crisis has made more businesses reliant on digital technology than before, giving an opportunity for malicious actors to intensify attacks, e.g. phishing then fraud, taking advantage of sudden and massive surge in teleworking arrangements and online transactions. The typical criminal is primarily interested in obtaining credentials and personal data (Verizon, 2020). After those two categories, medical, internal or payment data are roughly the same in terms of interest.

SMEs make up 99% of the European businesses and while 77% of SMEs have a website only 17% are selling online (European Commission, 2020b). At the same time, 41% of Europeans are concerned about the security of online payments (Eurobarometer Europeans' attitudes towards cyber security – January 2020). Moreover, Web sales was the dominant mode of conducting e-sales in all EU Member States in 2019. The percentage of enterprises receiving electronic orders only over websites or apps ranged with Cyprus being only at 12% (below the EU average – 15%), ranked 24th and well beyond leaders such as Denmark (24%) (ibid). Consequently, websites or apps are increasingly offered by enterprises or third parties for various purposes. By contrast, in 2019, the percentage of enterprises that used only EDI-type messages for their sales ranged from 1 % of enterprises in Bulgaria, Romania, Luxembourg, Cyprus and Poland to 8 % in Czechia and 9 % in Sweden (ibid). Although Cyprus, is not one of the leading EU countries in terms of web transactions and payments, especially from SMEs, still the COVID pandemic and the need and strategy of digital transformation of the EU and its Cyprus steps to adopt it have contributed to an increase in SMEs interested to enhance their e-commerce capabilities, while over the last years scams and frauds in online transactions and payments are increasing in volume and frequency also for Cyprus. This can be attributed to the strive for digital transformation.

Due to its flexibility and scalability, cloud computing reduces the costs of technology upgrading by exempting firms of upfront investments in hardware and regular expenses on maintenance, IT team and certification, turning ICT management model into a model based on software acquisition (codes) and digital (hyper)connectivity (OECD, 2019b). Data on business use of ICT across OECD and EU countries highlights the close relationship between digital vulnerability, and hyper-connectivity and codification. As firms tend to increasingly purchase cloud computing services or their employees to use computer with Internet access, they are more likely to experience ICT related security incidents. In fact, the increasing connectivity of data-intensive activities adds layers of complexity, volatility and dependence on existing infrastructures and processes (OECD, 2017). Cloud computing is resulting in increased migration of sensitive data to external parties to the enterprise in question, which means that security and protection of that data are technically managed by an external party.

The leading sectors in terms of ICT spending in Cyprus are the financial sector, followed by the ICT and the public sectors (European Commission, 2020b). In terms of digital technology integration, even though Cypriot SMEs engage in the use of social media and e-commerce activities, they are less inclined to take up new technologies such as Cloud Computing, partly due to concerns about security and the ownership and availability of data (ibid), as attested in the DESI 2018 Cyprus report. However, recently as defined in DESI 2020, digital transformation (DX) projects appear to be gaining momentum among Cypriot enterprises, even though they are still at an early development stage, which is evident from the growth of cloud adoption from 12% (DESI 2018) to 18% (DESI 2020) and big data technologies from 3% (DESI 2018) to 12% (DESI 2020) and big data technologies. As a result of the increased adoption of cloud computing and big data technologies, SMEs in Cyprus and the government (new cybersecurity strategy to be approved in 2021) have a vital need for these technologies to offer security

in their use, which is defined as the preservation of the principles of confidentiality, integrity and availability of information during its transmission, processing and storage (European Union Agency for Cybersecurity, 2021).

GREECE

Because of the COVID-19 pandemic, European Small and Medium-sized Enterprises face many issues including abrupt shift to remote work and cybersecurity challenges. The most common issues that companies face regarding to cybersecurity are (Seaton, 2020):

- Lack of awareness about the cybersecurity risks
- False sense of security, and wrong security policies
- Lack of knowledge and understanding
- Lack of staff training
- Lack of allocated budget

According to PwC's 2017 Global State of Information Security Survey, at least 80% of companies in Europe have experienced at minimum one cybersecurity incident, while the number of security issues across all sectors worldwide increased by 38% in 2015, in comparison with the previous year. Also, in 2017 recorded two major ransomware attacks in businesses across Europe. In Spain, telecommunications, in Germany, train systems and in the UK, public health systems were all affected. As a consequence, all 28 Member States have developed cybersecurity strategies, with Greece being the most recent and the last state to adopt a national strategy. Although all Member States have a cybersecurity strategy, there are many differences among them (Kertysova, et al., 2018).

However, in Greece there is no comprehensive legal framework on Cyber Security. In the Criminal Code the following cybercrimes are included: computer fraud (art. 386a) violation of secrecy of computer programs or data (art. 370B), unauthorized use of software, (art. 370c para. 1) unauthorized data access (art. 370c paras. 2 & 3), child pornography (art. 348a), grooming (art. 337). Although, Greece signed the Cybercrime Convention, its legislation does mention legal sanctions in case of attacks against information systems. Some other relevant laws are the following:

-Data Protection Act (Law 2472/1997, art. 10 para. 3), which provides for the obligation of the data controller to take technical and organizational measures for the protection of personal data.
-Law 3471/2006 (Article 12) transposing Directive 2002/58, while provides for the obligation of telecom providers to take technical and organizational measures to ensure the security of its services and of the public electronic communications network.
-Law on electronic communications (Act No 4070/2012) which provides rules for the security and integrity of electronic communication networks and services (Christodoulaki, et al., 2015).

Pylones Hellas, which is a provider of IT solutions for medium and large companies, with a presence of more than 22 years in Greece, created and conducted a research on cloud computing security, in collaboration with the Department of Digital Systems of the University of Piraeus. More than 350 IT professionals and executives participated in the research. 67.06% of the total participants are in a key

position in the IT sector, with 27.84% stating that they are in the IT security sector professionally, while 13.47% are in the IT Networking sector and 25.75% of the participants are employed in other IT sectors.

According to the survey results, 37.54% of the participants have already faced a cyber-threat or cyber security breach without serious problems. However, 10.81% stated that they had serious consequences from cyber-attacks. The most common threats are breach of accounts, services and data, phishing attacks, malware (viruses, worms, Trojans, ransomware) which are all in the same level of concern for IT professionals.

48.20% of respondents believe that the biggest problem when it comes to protection against cyber-attacks is the ignorance of the risk of cyber-attacks. In addition to this 29.38% of the respondents believe that, it is not possible to properly address the threats due to lack of resources or infrastructure. They conclude that the primary measure to be taken is education (IT security awareness training) about these type of threats, and larger investments in Network & Firewall protection and Cloud security.

Also, the cloud services are being used by many companies, especially in the COVID-19 era. In particular, 82% of the respondents stated that they use a cloud service in their company such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). However, 50% believes that the cloud security provided by the provider is not sufficient. The biggest concern regarding the use of cloud services seems to be the lack of skills to understand the impact on security by 51.80%. While a significant percentage of 52.91% declare as the biggest challenge of cloud security the detection and response to security incidents that comes as a result of lack of visibility in the cloud and ignorance of cloud security (Naftemporiki, 2020).

Some European Countries have explored the topic of governmental clouds, connected to the adoption of security frameworks (Gov Cloud adopters). The Greek Gov Cloud is comprised of Okeanos18 and ViMa, which are Cloud services provided by the Greek Research and Technology Network S.A. (GRNET) and they are mostly used to the national academic and research Okeanos is a Cloud service with customers in the academic and research community, and thus is mostly used by Higher education Institutes. ViMa aims to provide shared computing and network resources to the educational and academic community, with production-level quality. In order to be able to ensure high availability, both Okeanos and ViMa are hosted on multiple computing clusters distributed in several data centres in Greece. The Gov Cloud network infrastructure ensures seamless connection to the telecommunications backbone (and Internet), at very high speeds. Okeanos and ViMa are based on open source software (ENISA, 2015).

In conclusion, the most common threat in terms of security is cyber security, and the attacks aiming to steal personal data, services and accounts, while could security is also arises some concerns and issues. While some European countries are Gov Clould adopters, the cloud services are mostly used for national and academic research, meaning that companies still have to figure out how to solve their issues on their own.

UK

Although the nature of security has certainly changed in recent decades, there is no question that security itself is still an issue that SMEs face. Indeed, in some ways, the number of security issues that

SMEs have to worry about has multiplied as the advent of the digital age opens new vulnerabilities in the everyday operations and transactions of business.

First among these is cybersecurity. Cybersecurity is a term that covers a very broad range of threats and issues, many of which are a danger to SMEs. Such a threat may take the form of a straightforward email scam, in which a business is coerced or deceived into making payments into a fraudster's account; or ransomware, a form of malware that steals data and extorts the business in question for money in order to get the data back or prevent it being published, where it is sensitive information. Whatever form these threats take, there is evidence to suggest that cybercrime of this nature is rising, and that it is more often targeted at larger businesses than smaller ones.

Furthermore, and on a related note, it is inevitably smaller businesses that are more likely to lack the resources, expertise, or awareness to properly protect themselves against these threats. The nature of such cyber threats is that someone who is unaware of or unfamiliar with them is considerably more likely to be vulnerable to them. Not to mention, as discussed in the previous section on finance, that businesses do not always have the capital to invest in more up-to-date and secure infrastructure.

Part of what makes businesses vulnerable in some of the ways described above is the nature of how data is managed and stored today. Whereas in years gone by, it might have been common for a physical file to be kept, or for perhaps a digital file on a single device, nowadays it is extremely common to have data stored or backed up on a digital cloud. There are various different applications and services that allow businesses to store data online, in a space that they can access from any device anywhere, making this both a convenient solution and a potential vulnerability. Especially given the ongoing pandemic, it is not inconceivable that an employee or SME owner might decide to use their data cloud storage to work more frequently from home or elsewhere rather than their office. The devices they use in those environments, however, might not necessarily be as secure as those in the office.

On a different note, but similarly affected by the COVID pandemic, is the security of payment. Although again technological advancements has made this in many ways more convenient and has dramatically expanded the potential for growth, it has also, as before, introduced vulnerabilities. The rise of digital payments rather than cash or cheque has been accelerated by lockdowns in the UK, which can more easily be exploited by those with malicious intent. Indeed, the impersonality of online payment was exploited to the tune of over £2 million last year.

NETHERLANDS

Despite the high digitization od Dutch SMEs, the sector has a lot to do in terms of cyber security. A recent EU restriction on the area of General Data Protection Regulation (GDPR), which came into force in 2018, found over the 80% of Dutch SMEs falling short of GDPR compliance.

Research by Capgemini and insurance company Interpolis has shown that many entrepreneurs in the country score well in the areas of physical security, access to the corporate network and security of the website, but they lack vision and policy in the organisation of business processes (ComputerWeekly.com, 2018)

This is due to the fact that cyber security is often neglected or under-estimated among SMEs, until an incident occurs. As the pandemic has pushed towards teleworking and online businesses, both the cases and the level of cybercrime is deteriorating, which has made the call for action more vital than ever.

The last 15 years the EU Agency for Cybersecurity has been assisting SMEs to integrate cybersecurity into their digital environments by publishing a number of reports and information packs, as well as guidelines on security risks, as well as tips to help towards cybersecurity crimes (ENISA, 2019). In addition, a workshop on challenges and recommendations for SMEs was held by ENISA online in November 2020.

Initiatives at EU level (the Connecting Europe Facility - CEF and the Horizon 2020 – H2020 programmes) have been supporting cybersecurity projects and capability developments, as well as act as a catalyst to attract further funding from the private sector and other public sector actors. Pilot projects such as CONCORDIA, ECHO, SPARTA and CyberSec4Europe aim to address the cybersecurity skill gap in EU and to deliver innovative solutions. Next to these EU initiatives, national ones for the Netherlands include (FinTech Magazine, 2020):

Implementing the National Cyber Security Research Agenda III (NCSRA III) in order to pursue the development of cybersecurity research aimed at the development and commercialisation of innovative solutions

- Encouraging open-source encryption by making additional resources available for this within the framework of NCSRA III
- Establishing a Cyber Security Research Agency

Blockchain technologies offer security in transactions thanks to the decentralization of applications which does not let room for manipulation of transactions. Blockchain can also help SMEs build smarter and more secure supply chains, which ensures real-time tracking all along the trade line.

POLAND

The biggest challenge facing SMEs in Poland (and probably the world) became the Covid-19 pandemic. The economic downturn and changes in business management (unexpected downturns, high volatility, lack of liquidity) affected the work of a huge proportion of companies in Poland. Thus, security for many SMEs in Poland has simply taken the form of a form of surviving. The slowdown and downturn also affect the acquisition of finance and willingness to invest.

Many companies are looking for digital solutions that allow their businesses to continue working. Some companies where this has been possible have decided to move to a remote working mode.

Working in a digital environment is inextricably linked to cyber security, and it is cited as one of the biggest threats that SMEs face. Losses resulting from cyberattacks worldwide are estimated at $600 billion (Allianz Risk Barometer, 2019).

As far as cyber-attacks are concerned, they are mainly directed not strictly at the digital architecture of companies, but at their employees. An important statistic here is that (globally) 95% of cybersecurity breaches are due to human error (cybintsolutions.com/cyber-security-facts-stats/). Among the types of cyberattacks, phishing (79%), Advanced Persistent Threat (77%), ransomware (77%), DDOS attacks (75%) and Bring Your Own Device (74%) are still the most common (CyberDefence24, 2018).

The solution to this problem lies in the continuous education of employees and business owners in the SME sector. To do this in Poland, public institutions organise, for example, courses such as:

- *Cyberbezpieczeństwo w MŚP* (Cyber security in SMEs) organised by PARP (Polish Agency for Enterprise Development). A course for employees and employers who want to take care of their company's cyber security. More information on: https://akademia.parp.gov.pl/course/view.php?id=63

There are also guides being developed (at government level) for SME entrepreneurs on how to take care of cyber security. Examples include:

- *Poradnik dla małych i średnich przedsiębiorstw* (*Guide for small and medium-sized enterprises*) created by the Cyber Security Working Group of the Ministry of Digitalisation in Poland. More information on: https://www.gov.pl/attachment/6dfcd10b-9124-416f-8d09-2f7bb8de0221

You can also get grants to support cyber security in your business through contests such as:

- CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość (CyberSecIdent - Cyber Security and eIdentity) organised by NCBR (National Centre for Research and Development).

Another example that SMEs currently face in terms of security is the topic of personal data protection and storage.

An even bigger challenge for SMEs when it comes to cyber security is brought by the new fourth industrial revolution. The report "Smart Industry Poland 2019", states that 31.6% of industrial SMEs in Poland have already implemented innovations based on Industry 4.0, and another 38.3% will introduce Industry 4.0 technologies in the next 3 years (BiznesTuba, 2020).

These technologies, while revolutionary, are not without risks when it comes to their implementation and use. The dangers include IoT devices (vulnerable to cyber-attacks) or the risks associated with the use of cloud computing or cloud-based solutions. So it seems that Polish entrepreneurs seem to give these solutions a lot of credence.

According to the latest data, 52% of Polish companies use (or plan to use) cloud computing. They use it, among others, for data archiving and creating backup copies. Additionally, almost half of companies (48%) declare that they trust their cloud computing solutions provider. (Pasławski K, 2020)

With the GDPR policy entering law, SME companies also have new responsibilities. They need to do more work to communicate to customers how they are using their data. Still, one of the most significant risks lurking for SMEs is when customers' personal data is stolen.

Often, the main problem that SMEs have is also outdated cyber security tools and a lack of qualified staff.

Companies believe that a lack of adequate IT staff can be replaced by using cloud computing technology, where data is secured by professional providers (as many as 68% of medium-sized companies move data to the cloud to increase security). However, at the same time, as many as 92% of medium-sized companies worldwide have a director responsible for security (CISCO, 2018).

Moving operations to the cloud (while this practice is legitimate from a security or workforce reduction point of view) is certainly a trend, but there is no denying that organisations must not think they are

getting rid of security responsibilities so easily. Businesses should understand the dynamics and ways in which cloud mechanisms work.

SPAIN

Precisely, the arrival in e-commerce of many companies with no previous experience can be the perfect breeding ground for cybercriminals to act against their interests. Bad practices are also increasing with the enhancing of online business performance since the pandemic emerged.

In particular, SMEs have to deal with email spoofing to protect themselves. Through this practice, someone can, for example, impersonates a bank with which the company works in order to obtain the company's bank details.

In this regard, it is very useful to heed the advice given by official bodies such as the Bank of Spain or the National Institute of Cybersecurity.

CONSEQUENCES: The new amendment to the Payment Services Directive Act focuses on improving customer security when shopping online and preventing digital fraud.

Therefore, as of 1 January 2021, all online shops will have to reinforce the identification processes that their customers carry out when buying in e-commerce and, in the payment gateway, a double validation of their identity will have to be carried out.

Until now, when a consumer bought a product/service over the Internet, he/she only entered an electronic signature or a credit card and some data (e.g. a code) sent by the bank to a mobile phone to validate the purchase. With the new modification, at least two of the following authentication elements will have to be fulfilled in the payment gateway:

Some piece of information known only to the customer. For example: a password.

Something that only the consumer has. For example: A mobile phone where to receive a password.

Something that verifies your personal identity. For example: Fingerprint.

Although it is up to the payment service providers to adapt to this new regulation, merchants will have to inform their customers of this change and check that the providers comply with these requirements.

Despite the fact that this is a general European regulation, there are some exceptions. For example, for payments of less than 30 euros this regulation will be exempt from application as long as they are not more than 5 times a day or reach 100 euros in less than 24 hours. On the other hand, non-EU merchants operating in Europe will have to adapt their payment processes and comply with this new regulation.

3. Transnational Phase

3.1 Best practices in application of blockchain technology in finances

Name of the company	we.trade
Website	https://we-trade.com/index.html
Sector	ICT: serves Finance, Banking, Business Trading
Country	Ireland
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	Traders, particularly SMEs, who traditionally did not have access to bank guarantees, invoice financing and credit insurance, use we.trade to enhance their cashflow and digitise their existing paper-based processes. Companies are using we.trade's digital platform to address challenges such as the late payment of invoices, cyber fraud and where pre-payments are requested by sellers.
Desciption of the blockchain stategies that the company adopted.	A secure digital platform that makes it easier for buyers and sellers to trade globally. we.trade develops and licenses the world's first enterprise-grade blockchain-enabled trade finance platform. Through distributed ledger technology and smart contracts, we.trade makes it easier and more reliable for buyers and sellers to trade globally.

Name of the company	block.co
Website	https://block.co/
Sector	ICT: serves Accounting & Audit, Banking – Financial Services, Education, Government, Maritime & Shipping, Legal – Corporate Services
Country	Cyprus
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	Identified a need in education for secure and self-verifiable documents. A growing market in forged documents and the vulnerability of certification documents in the face of manmade and natural disasters meant a solution was increasingly necessary. It quickly became clear that it was not solely academia that could benefit from the reliable credential authentication that blockchain technology offered.

Desciption of the blockchain stategies that the company adopted.	The ONLY truly decentralized solution to secure PDF documents from fraud without intermediaries. Block.co transforms the way organizations leverage open-source vPDF technology in the issuance, revocation, and validation of self-contained and self-verifiable documents.

Name of the company	Kraken Ltd
Website	https://www.krakenltd.org/
Sector	Investment
Country	UK
Description of the company's challenges before the application of blockchain technology (if applicable).	It has been a great experience, Kraken Ltd offers it's investors constant returns from an inconsistent market
Description of the blockchain strategies that the company adopted.	It's very easy to start up. You need to set up an account with the company and have funds invested, your investment will be moved to the trading pool to be traded daily by our team of traders. You get credited daily depending on how much you invested and the package you signed up for.

Name of the company	BEEZ &TOYS
Website	www.beezandtoys.com
Sector	Manufacturing
Country	Serbia
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	-
Desciption of the blockchain stategies that the company adopted.	BEEZ& Toys is a manufacturing company in the toys sector. The company decided decided to adopt a blockchain-based solution from company Infidia because it thought that this solution can help it use some financial instruments that it would not be able to use without blockchain. Infidia app is a blockchain-based solution

	that keeps records of the business process prior to invoice creation. In both web and mobile apps, Infidia verifies invoices for invoice financing, in order to help small businesses, to solve liquidity issues, and fund their growth.

Name of the company	mBrainTrain
Website	mbraintrain.com
Sector	Innovation
Country	Serbia
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	The company had to deal with long payments delays from is costumers (institutes, universities, etc).
Desciption of the blockchain stategies that the company adopted.	mBrainTrain aims to make EEG (method of brainwave recording) a method that that will be used in everyday activities. The company adopted InfidApp to change the above mentioned problem. In general, the company sees Infidia's as a cash-flow solution. Also, the company provided feedback to the Infidia for examing the opportunity to: - Verify the business transactions behind the invoice that provides the basis for invoice discounting -Link orders with invoices and various documents -Reduce invalid invoices -Create a new pool of clients for banks -Unlocking small invoices -Enable a bundle package and define the level of risk

Name of the company	NBK LV
Website	https://www.nbkbv.com/en/
Sector	Forwarding and Shipping
Country	Netherlands

Description of the issues that the company was facing before the application of blockchain technology (if applicable).	NBK's former income models of logistics providers needed to change as a result of the integration of goods, financial and information streams. The solution for this was found in the application of new technologies, collaborations and business models that are compliant with ever-changing legislation and regulation and the need for supply chain transparency.
Desciption of the blockchain stategies that the company adopted.	Enabling transactions

Name of the company	Eligma Ltd.
Website	https://elly.com/en/
Sector	Payment services
Country	Slovenia
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	NA
Desciption of the blockchain stategies that the company adopted.	Eligma Ltd. is a Slovenian start-up which aims to make crypto part of daily business, life and ecommerce, The start-up has created an infrastructure that allows instant accepting different crypto payments at local/online stores thanks to the Go Crypto network. Company wants to combine and connect different types of payments, like card payment, digital payments and crypto payments in one place. Thank to them stores (online and physical) can accept secure crypto payments. Their product are: - Elly POS - GoCrypto - Ellly wallet

3.2 Best practices in the application of blockchain technology in security

Name of the company	iExec

Website	https://iex.ec/
Sector	Business
Country	France
Description of the company's challenges before the application of blockchain technology (if applicable).	iExec strives to develop the best technologies and to invent new protocols that will bring cloud decentralization economy for business. The aim of Blockchain is to resolve business issues related to multi-enterprise interactions and facilitate the creation of new business models. iExec specialize in: Smart Contracts, Record Keeping, Transfer of Value, Digitized Assets, Off-Chain Computing, Confidential Computing & Marketplace Creation.
Description of the blockchain strategies that the company adopted.	Decentralized Marketplace for Cloud Resources and for Scaling blockchain applications with open-source software and protocols. A decentralized network giving applications access to trusted off-chain computation and data. iExec introduces a new paradigm for cloud computing. Cloud resources can now be traded on a global market, just like any other commodity. Instant access to a large capacity of computing power from the provider offering the best rate.

Name of the company	Limechain
Website	https://limechain.tech/
Sector	Supply Chain, Real Estate, Pharma, Healthcare
Country	Bulgaria
Description of the company's challenges before the application of blockchain technology (if applicable).	Blockchain and its application has the potential to impact most problematic industry challenges like supply chain management, asset tracking, claims management, proof of origin, KYC and KYS, eliminating middlemen, reducing costs, eliminating frauds and others.
Description of the blockchain strategies that the company adopted.	Propy takes holistic approach to solving real estate challenges with blockchain-based platform.

Name of the company	Blockchain reactor
Website	https://bcreactor.com/
Sector	Banking, Finance
Country	Serbia and Ireland
Description of the company's challenges before the application of blockchain technology (if applicable).	International payments are slow, costly, and lack transparency. Big companies can negotiate a good deal from their bank, but consumers and SMEs get a bad deal, and there are three reasons why. Also, another issue that reducing e-fraud, enabling safer transactions and getting more people through the online sales pipeline.
Description of the blockchain strategies that the company adopted.	Blockchain reactor makes international payments easier through blockchain. A conglomerate of European banks has come together to find a secure, scalable solution for their clients to pay international bills. As the solution provider, Blockchain Reactor is liasing with these banks to provide a user-friendly and intuitive application for their end-users. Also, Blockchain reactor delivered a complete end-to-end design, development, testing and maintenance of an AI-backed fraud detection system.

Name of the company	Hdac Technology
Website	https://www.hdactech.com/en/index.do
Sector	Security
Country	Switzerland
Description of the company's challenges before the application of blockchain technology (if applicable).	NA
Description of the blockchain strategies that the company adopted.	Hdac Technology owns a platform for IoT devices that aims to support safety during, among other things, money transfers or data transfers through the use of blockchain technology.

	The company is currently focusing on using blockchain technology to ensure the cyber security of IoT devices.

Name of the company	ING BanK
Website	https://www.ingwb.com/themes/distributed-ledger-technology-articles/blockchain-the-future
Sector	Banking
Country	Netherlands
Description of the company's challenges before the application of blockchain technology (if applicable).	Security in transactions – need to eliminate intermediaries – fast transactions. Blochchain technology necessary for doing international business.
Description of the blockchain strategies that the company adopted.	The Dutch bank has long been interested in blockchain and cryptocurrency and is paying close attention to how the market is developing. In fact, ING conducts a yearly international survey documenting global sentiments towards the blockchain and cryptocurrency industry.

Name of the company	Piegāde69
Website	www.piegade69.lv
Sector	Transport
Country	Latvia
Description of the company's challenges before the application of blockchain technology (if applicable).	The company is a third party delivery service provider and it wanted to collect trustworthy data and show this information to its b2b customers.
Description of the blockchain strategies that the company adopted.	The company established in 2018 with the aim to provide transporting services accross Latvia. The company setted as goal to collect proof about the quality of its delivery. Piegad69 understands that blockchain-based applications will have legally binding power in the future, and because the company is a third party delivery service provider, it wants to collect

	trustworthy data and show this information to its b2b customers.

Name of the company	AlBicchiere
Website	www.albicchiere.com
Sector	Food and Beverage
Country	Italy
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	AlBicchiere wanted to find a way to control a complex logistic chain with many different actors.
Desciption of the blockchain stategies that the company adopted.	For that reason, the company has tested, validated and adopted Datarella's blockchain-based solution. Datarella has developed "TRACK & TRUST", a digitized and secure tracking solution for valuable goods on their supply chain journeys. AlBicchiere adopted the platform as they believe that a distributed ledger in the control of logistic chain would encourage consumers to purchase from it (as they will be efficient transparency and control for transportation processes) and would also support wine producers when using the company's system.

Conclusions

In all 5 European countries (Greece, UK, Netherlands, Cyprus, Spain, Poland) SMEs represent the vast majority of enterprises. The financial problems that the SMEs face are common among countries, as the joint economy of EU, and the relevant economical and monetary policies affect all the countries in some way. The COVID-19 pandemic has created a “new normal”, as the financial capacity of SMEs has been seriously affected. On top of that, due to Brexit SMEs have to confront a different situation for those that many SMEs from other countris face.

Access to financing seems to be the most important issue for the Member countries as many studies showed that this most serious issue for companies in Netherlands, Cyprus and Greece. That means tha companies have difficulties in accessing bank lending, while Dutch SMEs are obtaining bank loans less often than other SMEs in the eurozone. At the same time in Greece, there has been reported a negative perception of banks' willingness to lend (-30%, down from -22%) and access to public financial support (-51%, down from -36%) during the last years. A similar problem applies to the UK, in which

access to banking financial programs remains an issue during the last years. Though in Cyprus and Poland, alternative lending options such as Venture Capital (VC), Business Angels (BA) and other crowdfunding services have becoming popular during the last years, this is not the case for Greece as Venture Capital is not available and crowdfunding services are very limited.

Another important factor that can be identified as the most important in financial management is the limited cash flows. That is a very common problem that businesses face and in fact 57% of UK small business owners reported relevant problems. In Greece, and Spain several similar issues have been reported, while in Greece, most SMEs operated with limited liquidity in 2018 due to the economic crisis. The limited cash flows often come as a result of the loan financing gap, but delays in payments are another important factor that deteriorates the situation even more. Many Polish SMEs are confronting lack of timely payments from contractors and in Netherlands numerous companies manage late or unpaid invoices.

When it comes to security, the most common issue is the cybercrime which comes in many forms. According to PwC's 2017 Global State of Information Security Survey, at least 80% of companies in Europe have experienced at minimum one cybersecurity incident. An important fact is that (globally) 95% of cybersecurity breaches are due to human error (cybintsolutions.com/cyber-security-facts-stats/). Among the types of cyberattacks, phishing (79%), Advanced Persistent Threat (77%), ransomware (77%), DDOS attacks (75%) and Bring Your Own Device (74%) are the most common for businesses. As a consequence, cyber threats that can affect several business' activities and is a major danger to them and especially for smaller businesses that are more likely to lack the resources for protect themselves in such situations.

Additionally, most companies, especially in Poland and Cyprus use or plan to use could computing for data archiving and creating backup copies. Although it can be beneficial for many SMEs, there are several concerns about security and the ownership and availability of data.

Even though the above mentioned problems can be mitigated by the use of blockchain technology, the application of it is a difficult procedure for many SMEs mainly because many of them miss the manpower, skills and knowledge to develop or adopt this kind of technologies. But some SMEs across the Europe have efficiently adopted some blockchain applications, relevant to cloud resources, external payments, etc which have proved significant in handling several problems such as transactions with third parties or security of company's data.

References

Cyprus

ACCA (the Association of Chartered Certified Accountants), "Access to finance for SMEs in Cyprus: an update from ACCA", 2014, Available Online (Last Accessed: 16 April 2021): https://www.accaglobal.com/pk/en/technical-activities/technical-resources-search/2014/december/access-to-finance-for-smes-in-cyprus.html

Almeling, D. (2012), "Seven Reasons Why Trade Secrets Are Increasingly Important", Berkeley Technology Law Journal, Vol. 27, p. 1091, http://dx.doi.org/10.15779/Z38SM4F.

Commission Staff Working Document (2016), Evaluation of the Late Payment Directive/ REFIT evaluation, Available Online (Last Accessed: 15 April 2021): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0278&from=en

Duruflé, G., Hellmann, T. and Wilson, K. (2017) "From Start-up to Scale-up: Examining Public Policies for the Financing of High-Growth Ventures", Prepared for the CEPR/Assonime Programme on Restarting European Long Term Investment Finance. Date Written: 01.09.2016. Saïd Business School WP 2017-05.

European Investment Bank, Assessing the potential use of Financial Instruments in Cyprus, A study in support of the ex-ante assessment for the potential future use of Financial Instruments for SMEs, ICT, and the Low-Carbon Economy in Cyprus, Final Report, Prepared by PricewaterhouseCoopers (PwC), 21 July 2017.

European Commission (2016), "Small and Medium Sized Enterprises Access to Finance", European Semester Thematic Factsheet, 2016.

European Commission (2019a), Performance Review – 2019 SBA Fact Sheet, CYPRUS, Available Online (Last Accessed: 15 April 2021): https://ec.europa.eu/docsroom/documents/38662/attachments/6/translations/en/renditions/native

European Commission (2011a), "Report from the Commission to the European Parliament and the Council on the implementation of Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions", COM/2016/0534 final. Available Online (Last Accessed: 15 April 2021): https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2016%3A534%3AFIN

European Commission (2011b), "Internal Market, Industry, Entrepreneurship and SMEs – Late Payment Directive", Available Online (Last Accessed: 15 April 2021): https://ec.europa.eu/growth/smes/sme-strategy/late-payment_en

European Commission (2019b), "Internal Market, Industry, Entrepreneurship and SMEs – SME Performance Review", Available Online (Last Accessed: 15 April 2021): https://ec.europa.eu/growth/smes/sme-strategy/performance-review_en

European Commission (2020a), "Trade secrets: Commission decides to refer Cyprus to the Court of Justice for not transposing the Trade Secrets Directive", Press release, 30 October 2020, Brussels, Available Online (Last Accessed: 16 April 2021): https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1683

European Union Agency for Cybersecurity (2012), "Cybersecurity Strategy of the Republic of Cyprus - 2021", Available Online (Last Accessed: 16 April 2021): https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf/view

European Commission (2020b), "Digital Economy and Society Index (DESI) 2020, Cyprus", Available Online (Last Accessed: 16 April 2021): https://ec.europa.eu/cyprus/sites/default/files/desi2020-cyprus-eng.pdf

Financial Tribune Daily and Contributors (2017), "Cyprus Says Cybercrime a Huge Threat to Economy", Available Online (Last Accessed: 16 April 2021): https://financialtribune.com/articles/world-economy/58821/cyprus-says-cybercrime-a-huge-threat-to-economy

OECD (2019a), OECD SME and Entrepreneurship Outlook 2019, OECD Publishing, Paris, https://dx.doi.org/10.1787/34907e9c-en

Organisation for Economic Cooperation and Development (OECD), "Chapter 2. Digital security in SMEs – The Digital Transformation of SMEs", OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, https://doi.org/10.1787/bdb9256a-en, Available Online (Last Accessed: 16 April 2021): https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

OECD (2019b), OECD SME and Entrepreneurship Outlook 2019, OECD Publishing, Paris, Available Online (Last Accessed: 16 April 2021): https://dx.doi.org/10.1787/34907e9c-en.

OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, Available Online (Last Accessed: 16 April 2021): https://dx.doi.org/10.1787/9789264276284-en.

Verizon (2020), "2020 Data Breach Investigation Report", Available Online (Last Accessed: 16 April 2021): https://agio.com/newsroom/key-takeaways-from-verizons-2020-data-breach-investigation-report/

Poland

Allianz.(2020). *Allianz Risk Barometer. Identifying the major business risks for 2020.* Retrieved from: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf

BiznesTuba. (2020). *4 wyzwania, z którymi muszą się zmierzyć polskie MŚP w 2020 r.* Retrieved from: https://biznestuba.pl/featured/4-wyzwania-z-ktorymi-musza-sie-zmierzyc-polskie-msp-w-2020-r/

CyberDefence24. (2018). *Cyberbezpieczeństwo sektora MŚP – wysokie ryzyko i konieczność poprawy standardów.* Retrieved from: https://www.cyberdefence24.pl/cyberbezpieczenstwo-sektora-mspwysokie-ryzyko-i-koniecznosc-poprawy-standardow

CISCO. (2018). *Małe, lecz potężne Jak małe i średnie firmy mogą wzmocnić swoją obronę przed zagrożeniami dla bezpieczeństwa?* Retrieved from: https://www.cisco.com/c/dam/global/pl_pl/solutions/small-business/pdf/cisco_2018_smb_revised_092518.pdf?fbclid=IwAR1PzstPFsz07NP2Ub1tDjHdXlYFycMlTwjDNaN1g9kcQwlmdbpYXEoRzqk

PARP. (2020). *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce*. Retrieved from: https://www.parp.gov.pl/storage/publications/pdf/ROSS-2020_30_06.pdf

Pasławski K. (2020). *Raport: MŚP bezpieczne w chmurze*. Retrieved from: https://crn.pl/aktualnosci/raport-msp-bezpieczne-w-chmurze/

Ramczyk J. (2019. *Publiczne notowanie akcji jako źródło finansowania małych i średnich przedsiębiorstw*. Retrieved from: http://ssp.amu.edu.pl/wp-content/uploads/2019/03/ssp-2019-1-11.pdf

Wierciszewski M. (2021). *Małe i średnie firmy nie korzystają z finansowania zewnętrznego. To problem, bo będą wymagać ogromnych inwestycji*. Retrieved from: https://businessinsider.com.pl/finanse/przedsiebiorstwa-msp-nie-korzystaja-z-kredytow-ostrzega-michal-gajewski-santander/99xwbjr

Witkowski R. (2020). *Kryzys w sektorze MŚP. Czy jest się czego obawiać?* Retrieved from: https://witkowski-partnerzy.pl/kryzys-w-sektorze-msp-czy-jest-sie-czego-obawiac/

Wiadomości Handlowe. (2020). *Koronawirus a sektor MŚP. 70 proc. firm może utracić płynność finansową*. Retrieved from: https://www.wiadomoscihandlowe.pl/artykul/koronawirus-a-sektor-msp-70-proc-firm-moze-utracic-plynnosc-finansowa/2

Greece

BlockStart. (2021, March 16). *Our SME Adopters*. https://www.blockstart.eu/our-adopters/

Datarella GmbH. (2021, March 18). *Home*. DATARELLA. https://datarella.com/

European Central Bank. (2015, June). *Survey on the access to finance of enterprises in the euro area*. https://www.ecb.europa.eu/pub/pdf/other/SAFE_website_report_2014H2.en.pdf?56935ca239cc0aab853703c9b2103145

European Commission. (2020b, February). *SME access to finance situation in EU Member States Final Report 2019*. https://ec.europa.eu/docsroom/documents/39645

European Union Agency for Network and Information Security. (2015, February). *Security Framework for Governmental Clouds*. https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds

Christodoulaki, M., Fragopoulou, P., Frydas, N., Iglezakis, I., & Markatos, E. (2015, August). *POLICY RECOMMENDATIONS FOR CYBER SECURITY*. Greek Cybercrime Center. http://www.cybercc.gr/m/GCC_POLICY_RECOMMENDATIONS_FOR_CYBER_SECURITY.pdf

Infid (2020, December 25). *InfidApp Invoice Financing Software for Small and Medium-sized Business*. https://www.infid.app/

Greece | Financing SMEs and Entrepreneurs 2020: An OECD Scoreboard | OECD iLibrary. (n.d.). Oecd-Ilibrary.Org. Retrieved April 14, 2021, from https://www.oecd-ilibrary.org/sites/0f52ae26-en/index.html?itemId=/content/component/0f52ae26-en

Katsioloudes, M. I., & Jabeen, F. (2013). Challenges associated with the Greek SMEs in the basin of Athens-Greece: an exploratory study. *International Journal of Entrepreneurship and Small Business*, *19*(3), 309. https://doi.org/10.1504/ijesb.2013.055305

Kertysova, K., Frinking, E., Van den Dool, K., Maričić, A., & Bhattacharyya, K. (2018, March). *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*. European Economic and Social Committee (EESC). https://hcss.nl/sites/default/files/files/reports/Cybersecurity%20ensuring%20awareness%20and%20resilience%20of%20the%20private%20sector%20acrros%20Europe%20in%20face%20of%20mounting%20cyber%20risks.pdf

NewsRoom. (2018, October 13). *Ποιες επιχειρήσεις στην Ελλάδα έχουν τεράστια προβλήματα ρευστότητας*. mononews. https://www.mononews.gr/business/pies-epichirisis-stin-ellada-echoun-terastia-provlimata-refstotitas

Seaton, D. (2020, November 27). *Cybersecurity Challenges Facing SMEs - Cyber Audit Team Australia*. Cyber Audit Team. https://cyberauditteam.com/blog/identify/cybersecurity-challenges-facing-small-to-medium-sized-businesses-smes

The State of Cloud Security 2020: Μεγάλη έρευνα για την ασφάλεια στο cloud. (2020, October 12). naftemporiki.gr. https://www.naftemporiki.gr/story/1645374/the-state-of-cloud-security-2020-megali-ereuna-gia-tin-asfaleia-sto-cloud

2019 SBA Fact Sheet (2019). European Commission

UK

What's occupying British SMEs? (2019). The Telegraph. https://www.telegraph.co.uk/business/challenges/sme-key-challenges-2019/

Jones- Evans, D. (2021, January 1). The challenges and opportunities facing SMEs. Business Live. https://www.business-live.co.uk/opinion-analysis/challenges-opportunities-facing-smes-19547782

Dutta, D. (2020, February 19). Here are the biggest challenges SMEs in the UK are facing. Dataconomy. https://dataconomy.com/2020/02/here-are-the-biggest-challenges-smes-in-the-uk-are-facing/

Williams, N. (2019, April 2). SMEs' most common issue is cashflow. UKTN. https://www.uktech.news/accountancy/smes-most-common-issue-is-cashflow-20190402

Basquill, J. (2020, February 26). UK government struggling to reverse decline in SME exports. Global Trade Review. https://www.gtreview.com/news/europe/uk-government-struggling-to-reverse-decline-in-sme-exports/

Johnson, J. (2020, December 11). 6 Security Challenges Facing SMEs Heading Into 2021. Informationsecuritybuzz. https://informationsecuritybuzz.com/articles/6-security-challenges-facing-smes-heading-into-2021/

Lynch, B. P. (2020, April 16). Criminals prey on coronavirus fears to steal £2m. BBC News. https://www.bbc.co.uk/news/uk-england-52310804

Leveraging new technologies to fund fair, sustainable smallholder. (n.d.). Provenance. https://www.provenance.org/case-studies/unilever

Miller, R. (2017, December 14). Xage emerges from stealth with a blockchain-based IoT security solution. TechCrunch. https://techcrunch.com/2017/12/14/xage-emerges-from-stealth-with-a-blockchain-based-iot-security-solution/?guce_referrer=aHR0cHM6Ly93d3cuY3Nvb25saW5lLmNvbS8&guce_referrer_sig=AQAAAAmJ_BLx4QIHT4Ha5858O2jMcdLdrPO7qFWfhZSZjJOOMM5Dm2LVAlHJ97o3wvaUcQIuEgnqROygtskrdHjmbq7_zL3-7p36q6ET0sWdE1yerCf3R3Fb2bXx6QcwxuP7sKTH5kafkeya8gAsdfJgtxEzXZXXyNXuIEiraL2oi6Bt&guccounter=2

Spain

Banco de España. (2020). *Informe de Estabilidad Financiera primavera 2020*. https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinancera/20/ficheros/IEF_Primavera2020.pdf

Cantalapiedra, M. (2021, January 5). *¿A qué retos se enfrentan las pymes españolas en 2021?* Think Big. https://empresas.blogthinkbig.com/desafios-para-pymes-espanolas/

Fernández, A. (n.d.). *Los desafíos de las pymes en 2021*. Menudas Empresas. https://menudasempresas.com/los-desafios-de-las-pymes-en-2021/

Netherlands

Centraal Planbureau. (2019, July). *POLICY BRIEF - Dutch SME bank financing, from a*

European perspective. https://www.cpb.nl/sites/default/files/omnidownload/Policy%20Brief%20SME%2009072019_0.pdf

ComputerWeekly.com. (2018, March 26). *Dutch SMEs' cyber security is insufficient*. https://www.computerweekly.com/news/252437551/Dutch-SMEs-cyber-security-is-insufficient

ENISA - European Union Agency for Network and Information Security. (2019, November). *Good practices in innovation on cyber security under the national cyber security strategies.*

EUROPEAN COMMISSION. (2018, November). *SME access to finance conditions 2018 SAFE results – Netherlands.* http://ec.europa.eu/growth/safe

EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2020, November 23). *European SMEs facing increased cyber threats in changing digital landscape*. https://www.enisa.europa.eu/news/enisa-news/european-smes-facing-increased-cyber-threats-in-a-changing-digital-landscape

FACTRIS. (2020, January 08). *Dutch SMEs are Struggling with Cash Flow*. https://news.cision.com/factris/r/dutch-smes-are-struggling-with-cash-flow,c3004607

Finextra. (2019, June 18). *Blockchain: A game-changer for Small and Medium-sized Enterprises?* https://www.finextra.com/blogposting/17380/blockchain-a-game-changer-for-small-and-medium-sized-enterprises

FinTech Magazine. (2020, June 27). *How blockchain is helping SMEs*. https://www.fintechmagazine.com/banking/how-blockchain-helping-smes

Medium platform. (2019, November 19). *Should small and medium-sized enterprises adopt blockchain?* https://medium.com/akeo-tech/should-small-and-medium-sized-enterprises-adopt-blockchain-ff6c1cca784f

NL Times. (2020, August 14). *Recession: Dutch economy shows worst ever contraction.* https://nltimes.nl/2020/08/14/recession-dutch-economy-shows-worst-ever-contraction

NL Times. (2020, June 08). *Deepest recession in 100 years facing Dutch economy; better off than other EU countries.* https://nltimes.nl/2020/06/08/deepest-recession-100-years-facing-dutch-economy-better-eu-countries

Paardenkooper, K. (2019). *Creating value for SME's with logistics applications based on blockchain*. In: KennisDC Logistiek Zuid-Holland (Hogeschool Rotterdam).

STATISTA. (2020). *Total number of small and medium enterprises (SMEs) in the Netherlands from 2016 to 2020*. https://www.statista.com/statistics/818704/number-of-smes-in-the-netherlands/