The European market potential for cyber security products and services

Last updated:
01 November 2021

The European market for cyber security is booming. There is an increase in the use of technology that needs cyber security solutions, there is an increase in cyber security policies and there is increasing awareness of the importance of cyber security.

Contents of this page

1. Product description

Cyber security protects systems, software and networks against unwanted access. These attacks are generally aimed at theft, disruption or even extortion. Cyber security is also known as computer security or information technology security (IT security). The market is segmented into cyber security services and cyber security solutions.

Examples of cyber security services include: identity & access management, infrastructure security, governance, risk & compliance, unified vulnerability management services offering, data security & privacy services.

Cyber security solutions prevent, detect and respond to the abovementioned security risks. The solution segment consists of hardware and software. Examples are antivirus software and firewalls.

The complexity of these solutions has grown significantly over the past years. They have proven to be effective at preventing threats and attacks, such as malware, Trojans and phishing. The success of these solutions has led to rapid development of the cyber security industry. Implementing technical defences has become a standard best practice in every European company.

There are many types of information security applications, including:

- antivirus
- back-up and recovery
- information encryption
- information erasing
- information masking
- firewall; and
- spyware removal.

These applications can provide a specific service, or a combination of several.

2. What makes Europe an interesting market for cyber security products and services?

The European cyber security market was estimated at €17.29 billion in 2019 and is expected to grow with a Compound Annual Growth Rate (CAGR) of 22.6% to €38.13 by 2025. This growth is driven by General Data Protection Regulation (GDPR) compliance. Additionally, there are numerous projects initiated by European governments and major vendors operating in the market.

The increase of phishing and malware attacks on databases of European companies creates the need for cyber security. Also, the adoption of technologies such as Artificial Intelligence, machine learning and blockchain ensures interesting opportunities for market growth.

The cyber security solution segment is the most lucrative, but the cyber security services segment is also growing very fast and therefore also offers good opportunities.

Skills shortage

There is a large gap between the number of cyber security jobs and the number of available specialists. Finding and keeping a large workforce of cyber security professionals remains difficult. This goes for both the technical (product) side of cyber security as well as the cyber security service-related jobs.

To fill the gap, many companies in Europe try to hire cyber security specialists from abroad. An easier option is to outsource cyber security to offshore providers like you. The recent increase in remote working due to COVID-19 lockdowns may only speed up this process, because it decreases the difference between in-house, nearshore and offshore teams.

Tips:

Find the right people. Consider hiring people with the necessary qualities, but not yet the right requirements. You can train them on the job. Also, make sure you have access to the right people in order to scale up operations and serve clients on a short time frame.

Keep your skills up to date. If possible, obtain certification and clearly communicate you are certified in your marketing and client interactions. If you develop cyber security software, specialise in a few programming languages, rather than working with several languages you do not fully control.

Attend specialised online or offline events or conferences in Europe, such as the Gartner Security & Risk Management Summit and Infosecurity Europe.

Cost reduction

Cost reduction remains an important reason for European companies to outsource cyber security to providers abroad. Specialists in developing countries normally cost less per hour than those in Europe. The lack of the right skilled staff in Europe increases the cost of the available specialists. This is good news for outsourcing companies in developing countries.

Although cost savings are no longer the main reason for outsourcing, companies that have been affected by the COVID-19 crisis have tighter budgets than before. This could make offshoring to developing countries more attractive. Be aware, however, that if your offer is ‘too cheap’, European buyers may assume that it is too good to be true and that your quality is low.

Tips:

Offer competitive pricing, but do not compromise on the quality of your services. Try not to compete only on prices.

Be transparent in your pricing: avoid hidden costs.

In addition to your competitive prices, promote your expertise, experience, references, capacity, flexibility, reliability and communication capabilities.

Limit the possible disadvantages of being offshore. You need to be trustworthy, communicative, always reachable and available in the required time zone, and you need good security and privacy measures.

Nearshoring countries want to keep their prices competitive

Prices in nearshore countries are rising. This makes service providers in these countries less competitive than offshore service providers. This means that, if providers based in Central and Eastern Europe (CEE) work with you, they can keep the price low. This can offer you huge opportunities.

When outsourcing abroad, European companies prefer providers in nearshore locations because of proximity, language, cultural similarities and the minimal time difference.

Traditionally, the buyer markets for cyber security are Western and Northern European countries. The most popular nearshoring locations for companies in these countries are CEE countries. Countries that are members of the European Union are particularly attractive to them, as contracts and payments are governed and protected by the same legislation as in the buyer countries.

Tip:

Limit the possible disadvantages of being offshore. You need to be trustworthy, communicative, always reachable and available in the required time zone, and you need good security and privacy measures.

3. Which European countries offer most opportunities for cyber security products and services?

The European cyber security market can be divided into 2 groups of countries, and 1 group of 5 countries holds more than half of the market. Those countries are the United Kingdom, Germany, the Netherlands, Italy and France. Italy is the smallest market of the 5, but it shows the highest growth rate. We have also added Poland, because it is both an interesting outsourcing destination as well as a country that is in need of subcontractors and outsourcing providers itself.

We highlight the 6 countries that offer most opportunities for cyber security service providers from developing countries. They were mainly selected based on a report by Enterprise Ireland – The European Cybersecurity market. This report also provides information about the European Union market in general, the NATO market and the markets of Belgium and Spain.

Figure 1: Market Attractiveness and Market Accessibility for Cyber Security Services in European countries

	Market Attractiveness	Market Accessibility				
	Size	Growth	Competition	Commercial Opportunities	Information Accessibility	Certification
France	Large	Public sector	National competitors	Finance and public sector	Commercial opportunities	Added value of national certification
Germany	Large	Continuous	Close to saturation	Conservative customers	Commercial opportunities	Competitive advantage
Italy	Small	Catch-up effect	US companies	Finance and public sector	Low trusted market estimations	Foreseen necessity for public sector
The Netherlands	Relatively Small	Small	Lack of national champions	Risk of overcrowded market	Mandatory publication for public sector	Local accreditation for classified information
Poland	Low profit margin rates	Catch-up effect	Strong presence of international and local players	Strong demand	Commercial opportunities	Expected catch-up effect
United Kingdom	Large and innovative	Public sector	High number of UK & foreign companies	Finance and public sector	Neutral	Large range of certifications

Source: Enterprise Ireland

The United Kingdom – remaining attractive despite Brexit

The United Kingdom is the second-largest economy in Europe. Among its main sectors are finance and banking. According to the European Cyber Security Organisation, the government in the United Kingdom financed around €1.9 billion to execute various projects in cyber defence and research in 2020.

In our study about the demand for IT outsourcing in Europe, you can read how the United Kingdom's withdrawal from the European Union (Brexit) made British companies more cautious about outsourcing, which contributed to a decline in outsourcing after 2016.

Of all European markets, the United Kingdom is the most open to offshore outsourcing and the least cautious about doing business with developing countries. This openness is due to the nation's cost-saving business culture and historical ties to many countries across the globe.

Germany – Europe's largest economy

Germany is the largest economy in Europe, home to 19% of the European Union's population. The German economy is widely considered the stabilising force within the European Union, historically showing a higher growth rate than other Member States. In fact, according to the Economist, Germany will be the first major European economy to recover from the current COVID-19 crisis. This expectation is based on both the country's

healthy finances before the crisis and its large industrial sector.

The country's main industries include the automotive, electrical and chemical sectors. These increasingly rely on software to optimise production, improve products and remain competitive. Also, the German government is investing in internet security solutions to secure its high volume of confidential data and information. All these solutions need cyber security solutions.

However, the market is nearing saturation, and there is strong competition from both local and foreign companies.

Although its size makes Germany an interesting market, companies are less open to offshore outsourcing than in countries like the United Kingdom and the Netherlands. However, as German businesses continue to face skills shortages and become more experienced in offshoring, their attitude towards it is improving. In addition, the COVID-19 crisis has softened Germany's generally stiff corporate culture and shown companies what is possible with remote working and outsourcing.

There could be some language barriers when providing outsourcing services to Germany, as companies generally prefer to work and collaborate in German. Generally, you need an intermediary in Germany to communicate with existing or potential clients for you.

The Netherlands – a mature and highly digitalised European IT hub

The Netherlands has the sixth-highest GDP per capita in Europe. An impressive 60% of all Forbes 2000 IT companies have established operations in the Netherlands, making the country a real IT hotspot. It also has the most tech-related start-ups out of the smaller countries.

In 2019, the Dutch software industry was projected to grow from €5.4 billion in 2018 to €6 billion in 2021, at an average annual rate of 3.7%. With 19 professional developers per 100,000 inhabitants, the Netherlands has the highest density of software developers in the European Union. Despite this, the country has reported the highest percentage of hard-to-fill software developer vacancies in Europe. This shortage could drive many towards outsourcing solutions and makes the country a particularly interesting market, despite its size.

Companies in the Netherlands are traditionally fairly open towards outsourcing. In fact, 79% of the top IT-spending organisations plan to continue outsourcing at their current rate or even more in the next 2 years (2021 and 2022). Language barriers are generally not an issue, as the Dutch are very proficient in English. Some Dutch government sources on cyber security are the Global forum for Cyber Expertise (GFCE) and the National Cyber Security Agenda.

Italy – is catching up

Italy is not considered to be a frontrunner in the European cyber security market. However, it has a lot of potential, as it is catching up on years of lagging behind.

The domestic cyber security industry sees a dominant role of defence and security enterprises. There are many active local SMEs working in the cyber security sector.

France – in need of more cyber security talent

France is a mature and regulated cyber security market. Also, the French government is investing in internet security solutions to secure its high volume of confidential data and information. There is a trend in France that local SMEs have trouble upscaling their cyber security services, due to a lack of local talent.

France is generally a difficult market for ITO and BPO service providers, because outsourcing services abroad is not very popular among French companies. However, this sentiment is changing, and if you can offer French

speaking services, the threshold for outsourcing is even lower.

Poland – may need offshore partners to keep up with demand

Within Central and Eastern Europe, Poland is a major player in the software development industry. The country is home to about 25% of the developer population in the region. This adds up to around 300,000 professional developers, in various hubs across the country. These professionals rank as the number 3 best developers in the world, which adds to Poland's popularity as a nearshoring destination for European buyers.

In 2019, the Polish software industry was projected to grow from €2.1 billion in 2018 to €2.4 billion in 2021, at an average rate of 4.0% per year. The country also has the highest number of tech-related start-ups in the region. Its domestic cyber security market is dynamic, and the sector is growing due to government support, cyber security hub aspirations and a significant amount of EU funding investments.

To meet the demand from its flourishing software industry, Poland may increasingly need to turn to offshore partners. As the country has the highest hourly rates for developers in Central and Eastern Europe (€34 to €47), Polish software companies can actually save quite some costs by outsourcing some development tasks or projects to you.

Tips:

Select your target market not only based on size, but also by looking at factors such as cultural similarities, historical ties and shared languages.

Use the member lists of relevant industry associations to identify potential buyers, such as Digital Europe and Bitkom. You can also attend online or offline industry events such as the Gartner Security & Risk Management Summit and Infosecurity Europe.

Make sure you have access to skilled professionals, for example by working with universities, setting up training courses or centres, systematically collecting and analysing CVs and having a partner network of companies and individuals.

Emphasise your professional skills in your marketing, as well as the lower costs you offer.

For more ideas, see our tips for finding buyers on the European outsourcing market.

4. What trends offer opportunities or pose threats on the European cyber security products and services market?

Currently, the most important trends are the accelerated digital transformation, the Internet of Things (IoT), holistic security approaches, mobile developments and online banking.

Digital transformation was stimulated by the COVID-19 pandemic

Digital transformation refers to the use of new, fast and frequently changing digital technology to solve problems. Non-digital or manual processes are digitalised, and existing digital processes are modified and improved to keep up with new needs and possibilities. Digital transformation is also known as DT or DX.

The pandemic is stimulating the need for new IT solutions that enable companies to continue their operations in these types of situations. This is forcing companies to accelerate their transformation. According to recent data, digital adoption has made 5 years' worth of progress in just 8 weeks during the crisis.

This transformation was already a priority for European companies before the COVID-19 crisis. For example, around 30% of British companies had a digital transformation strategy in place, and another 50% were in the process of implementing one. Almost all of the remaining 20% were planning to have a strategy within 12 months.

Now that working partly or fully from home is becoming the norm, staff need remote access to their files and programmes. Consumers have further embraced online shopping, and retailers need web shops and apps. Agricultural companies need apps to make their supply chain transparent and communicate with their farmers, and the travel industry needs digital solutions to provide a contactless experience. All these new solutions require their own security.

Currently, 41% of European companies believe remote working is still not as secure as the office. This means there is work to do for cyber security experts.

Tips:

Consider offering cyber security solutions and services aimed at remote working or cloud-based business models.

For more information about guiding a company through crisis situations, see our study on how to respond to COVID-19 in the IT and Business Process Outsourcing sector (ITO/BPO).

For more information on how the pandemic may increase digital transformation, see for example McKinsey's article on how the COVID-19 recovery will be digital and UNIDO's COVID-19 implications and responses – digital transformation and industrial recovery.

Internet of Things (IoT) devices can pose security risks

IoT refers to everyday physical devices that are connected to and interconnected with the internet. These 'things' are embedded with electronics, sensors, software, actuators and network connectivity, allowing them to collect, send and receive data and to connect and interact with other devices. This collection and exchange of data enables the optimisation of processes, monitoring of environments and performing of computations or mathematical calculations.

The purpose of consumer IoT devices is generally to improve consumers' daily lives by, for instance, making them safer, healthier or simply more enjoyable. Industrial IoT devices (IIoT) are non-consumer devices, used by organisations to enhance their operations. The purpose of IIoT devices is to allow for increased productivity, efficiency and safety, while decreasing waste.

As the IoT market is booming, so is the need for cyber security solutions that protect all these connected devices and the information they transfer. From 2019 to 2026, the global IoT security market is expected to grow by a CAGR of more than 31%. Another concern besides information security is the fact that hackers can use these connected devices in DDoS attacks, malware and phishing threats. Furthermore, the increase in IoT regulations in most European countries propels the growth of the market for IoT security.

Holistic security approaches

A trend within this IoT trend is holistic security approaches. Holistic security considers a company's system as a whole to achieve maximum security. It combines:

- Security technology (software);
- Security procedures;

- People working within the system.

Technological developments like IoT require more complex security systems. This increased complexity and digitalisation of life drives the interest in holistic security.

Tips:

Specialise in IoT-related cyber security solutions.

Find out what IoT regulation applies in your target market(s) and adjust your product or service accordingly.

Attend specialised online or offline IoT events, such as the IoT Tech Expo Europe and the IoT World Europe Summit.

Provide holistic cyber security solutions, especially if you target companies that work with large volumes of data.

For more information, see our studies on exporting (I)IoT-related services and big data services to Europe.

Increasing use of mobile devices and the rollout of 5G

The European market for mobile devices continues to perform strongly. The number of European smartphone subscriptions is very high and continues to grow. In 2020, there were 389 million smartphone subscriptions in Central and Eastern Europe. In 2026, this number is expected to grow to almost 427 million. In 2019, smartphone adoption in Europe was 76%, and this is expected to grow to 83% in 2025. Keeping up with this trend, the European mobile security market is expected to record a CAGR of more than 13.5% from 2021 to 2028.

The European Union intends to have 5G cover at least 40% of the European workforce by 2025, including 70% of European industrial sites and 80% of main logistics routes. And although the number of Europeans who could connect to a 5G network almost doubled from 13% in 2019 to 24% in September 2020, it is still far behind the United States of America (76%) and South Korea (93%).

With the rollout of 5G networks come new security challenges for companies. As 5G also facilitates the connectivity of IoT devices, this further drives the need for specialised security solutions.

Tips:

Provide information security applications for mobile devices, for both the consumer and the business market.

For more information on European 5G coverage, see Open Signal's State of the Mobile Network Experience 2020.

If you want to learn more about mobile security, you can research online. A great webcast to watch is The Importance of Mobile Security by AT&T Cybersecurity.

Online financial transactions are increasing

The number of online transactions continues to increase. In 2020, online banking penetration amongst European adults was highest in Norway (95%), followed by Iceland (94%), Denmark, Finland and the Netherlands (all 91%) and Sweden (84%). The lowest online banking penetration was measured in Bulgaria, Romania, Bosnia and Herzegovina, Kosovo and Montenegro (all less than 10%).

Regardless of the current online banking penetration rate, online banking will become the most used banking method in all European countries within the next 10 years. These financial transactions need to be secure. Their increase drives demand for financial information security applications.

Tips:

- Offer financial information security applications for browser and mobile transactions.
- Focus on Northern and Western European countries for now, but keep an eye on developments in other European countries.

Need for strong authentication methods

European companies increasingly require strong authentication functionalities to confirm that their employees access their internal networks or applications. To prevent threats of password-based authentication, companies are moving towards layers of multifactor authentication. These layers can be hardware and software tokens, a device authentication step or a biometric check.

Implementing such authentication techniques reduces the risk of cyber threats. It also encourages users to adopt effective cyber security solutions. An example of this is a leading access management company, CyberArk. This company has announced the launch of CyberArk Alero. It enables remote users to securely access critical systems managed by CyberArk from any mobile device. Thus, the abovementioned factors are expected to provide growth opportunities in the cyber security market.

Tips:

- Consider offering solutions or services for authentication and/or access management functionalities.
- Refer to our study on trends for ITO/BPO to get more information about general ITO and BPO trends.

This study was carried out on behalf of CBI by Globally Cool B.V. in collaboration with Laszlo Klucs.