Entering the European market for cyber security products and services

Last updated:
01 November 2021

On the European market, you need to comply with mandatory requirements and additional requirements that buyers may have. European service providers and intermediaries are your most realistic market entry channels. Competition is strong. You still have a good chance if you focus on quality and/or specialise.

Contents of this page

1. What requirements should cyber security products and services comply with to be allowed on the European market?

On the European market for cyber security services, requirements vary per industry, per segment and even per country. Different industry-specific standards, rules and regulations exist for the automotive industry, education, healthcare and so on. New legislation is always in the making. As it would be impossible to list (or to know) all possible requirements, this chapter discusses the most common requirements. For more information, see our study about the requirements outsourcing services must comply with on the European market.

What are mandatory requirements?

Legal requirements

There are different rules you have to follow:

- Cyber security-specific rules (in the NIS2 Directive);
- Rules about copyright (in the Directive on the legal protection of computer programs);
- Privacy protection rules (in the General Data Protection Regulation or GDPR and the ePrivacy Directive).

If you do not follow these rules, you may be subject to enforcement actions and/or possible claims[A1] . Being located outside of the European Union does not free you from these consequences.

We advise you to check the exact rules in your European target market. On the ePing website, you can find an overview of country-specific measures that affect trade and that are not the same as the international standards.

On the ePing website, you can also find the contact persons per country that the World Trade Organisation (WTO) has appointed.

You can subscribe to receive ‘e-Ping alerts’ that might be relevant for your product or service.

Tips:

Pay attention to copyright and infringement (the act of breaking or disobeying the contract) clauses in the contracts you sign with European buyers.

If you are dealing with personal data, study the GDPR’s new European data protection rules and principles for a good understanding of what is allowed and what is not. For software development-specific GDPR information, check the 7-step guide to GDPR-compliant software development. Be aware of what data you store and where, to be able to comply with potential consumer requests.

Use IDC’s GDPR Readiness Assessment to determine how compliant you are and what you may need to improve.

Set up clear consent request forms and privacy policies that inform customers how you process their personal data. Look at the GDPR consent guidance from the British Information Commissioner’s Office (ICO) and Econsultancy’s GDPR: How to create best practice privacy notices. Keep records of your obtained consent. For more information, see ICO’s advice on how to record consent.

Read more about digital privacy on the website of the European Commission. This is also where you can keep up to date on the reforms of the European ePrivacy rules.

What additional requirements do buyers often have?

European buyers of cyber security services often have additional requirements. Most are about security, quality and corporate social responsibility (CSR).

Data protection and data recovery systems

Many European buyers expect you to implement an information security and management system. Especially when security is essential, like in the finance and healthcare sector or when making mobile applications. Although there is no specific legislation on this, the ISO 27000-series contains common standards and guidelines for information security.

Tips:

Make sure you have effective security processes and systems in place, from business continuity and disaster recovery to virus protection.

Ask your buyer to what extent they require you to implement a security management system like the ISO 27001 standard.

Consider obtaining the ISO/IEC 27701:2019 certification. To do so, you will need to either have an existing ISO 27001 certification or implement ISO 27001 and ISO 27701 together as a single implementation audit.

Quality management systems

Some European buyers only do business with companies that have a quality management system in place. Although it does not automatically guarantee good-quality cyber security services or solutions, it proves that you have a repeatable process and that you are a serious company that values standardisation.

The IEEE Standards Association has developed several IT and BP standards. You can search for cyber security standards and find a list of cyber security standards that are linked with a particular product or service. For example: cyber security standards for intelligent electronic devices, autonomous vehicles or electrical power systems.

Acknowledged and common quality management systems are ISO 9001:2015 and the Capability Maturity Model Integration. Other ISO standards that can be applicable to cyber security are ISO/IEC 9126, ISO/IEC 9241-11, ISO/IEC 25000:2005 and ISO/IEC 12119.

There has always been a debate within the sector about the importance of quality certification. If anything, it can show your commitment to your product or service and proves that you are a serious service provider focusing on your clients' needs, quality and continuous improvements.

Tips:

If you specialise or aim to specialise in particular sectors, find out which certifications are relevant. When considering a particular quality certification, ask yourself 3 questions before working out the details: is it good for my company? Is it good for my clients? Does it have marketing value?

Check if you can apply for financial support to achieve quality certification. Contact your national IT association (such as TAG Georgia or BPESA from South Africa) or a business support organisation in your country responsible for export promotion or IT export promotion.

Corporate Social Responsibility

Corporate Social Responsibility (CSR) refers to companies taking responsibility for their impact on the world. Not only in the products or services they offer, but also when it comes to:

- Consumer rights;
- Education and training of staff;
- Human rights;
- Health;
- Innovation;
- The environment;
- Working conditions.

Its importance for the IT outsourcing (ITO) industry is debated, as the impact from small companies in this business is often marginal.

Documented CSR policy

CSR is becoming particularly important to large companies and governments in Northern and Western Europe. Many European companies involve their suppliers in their CSR policies. Having a well-documented CSR policy may give you a competitive advantage over companies without such a policy. The ISO 26000 standard provides guidance on CSR. For small software companies, the most relevant and practical aspects of this standard are

labour practices, fair operating practices and community involvement.

Impact sourcing destination

You can also match the CSR policy of your potential buyer by becoming an impact sourcing destination. This is a relatively new term. It is a sourcing model that aims to improve people's lives, families and communities through meaningful employment in ITO and BPO. This can be achieved either through outsourcing or by setting up remote or virtual teams using digital technology. Impact sourcing has good potential for companies that wish to make their business more socially responsible (buyers and sellers of cyber security solutions). And it can be a Unique Selling Point (USP) for your business.

Fair trade software

Another example of how CSR initiatives extend to small IT businesses is fair trade software. This is software that is developed for better prices, under decent working conditions, supporting local sustainability and with fair terms of trade. In essence, fair trade software is a part of impact sourcing. Impact sourcing has a wider reach than fair trade software.

Tips:

Clearly communicate your commitment to CSR in your marketing activities. Also, show that you care about your impact on society and the environment by implementing your own CSR policy. It can be a unique selling point (USP) when your buyer has to select a provider.

Consider profiling yourself as an impact sourcing provider or a fair trade cyber security provider. See if you meet the requirements for an impact sourcing supplier. For more information about fair trade software, see the Fair Trade Software Foundation and Web Essentials' video on what fair trade software development actually means.

Consult the ITC Sustainability Map for a full overview of certification schemes addressing sustainability in the outsourcing sector.

Up-to-date knowledge and skills

As European buyers expect you to work with the latest technology, it is very important to stay informed about the latest platforms, frameworks and innovations and to keep your skills up to date.

Tips:

Continuously train your staff to stay up to date on the required software and hardware skills for your product and/or market. An example is personal Unity certification for your game designers.

Provide references, testimonials and examples of recent work, preferably on your website, as European companies often require proof of your technical skills.

European buyers may expect you to work according to the Agile concept. This is based on the Agile Manifesto, representing the ability to respond to change. It focuses on how people work together, letting solutions evolve through collaboration between self-organising and cross-functional teams. Agile development advocates adaptive planning, visualisation, evolutionary development, early delivery and continual improvement. With about 56% of companies using Agile methodologies using Scrum, this is the most widely-used Agile framework.

What are the requirements for niche markets?

European buyers often require you to comply with a sector-specific and/or industry-specific standard or code of practice. There are also many technologies, technical standards, protocols and frameworks related to software. They are developed and maintained by a large number of organisations, and they can differ significantly between niche markets.

In the automotive industry, for example, there are standards regarding cyber security, like ISO/SAE 21434 and WP29 Cyber Security. This last 1 will be mandatory for all new vehicle types in the European Union from July 2022.

Keep in mind that these are only some examples. The requirements for niche markets vary greatly, because the market is very diverse. There is a lot of different technology, and companies often focus on horizontal and/or vertical markets, so you have to research your own specific situation, market and requirements.

Tip:

Check which sector-specific standards or codes are available for your specific product (for example, by asking your sector association or your buyer) and to what extent your buyers want you to implement them.

2. Through what channels can you get cyber security products and services on the European market?

How is the end market segmented?

The market for cyber security products and services can be segmented by horizontal market (type of service) and by vertical market (type of industry). The 2 deployment types of cyber security are cloud and on-premises.

Figure 1: Horizontal and vertical market segments with opportunities for service providers

Type of service

On the service provider side, there are generalists and specialists. Specialist cyber security service providers focus on (and have extensive experience in) a specific vertical or horizontal market. Generalists, on the other hand, do not specialise in any particular segment.

Positioning your company as a specialist in specific industries strengthens your offer as a provider of cyber security services.

Type of industry

Banking, Financial Services and Insurance (BFSI), the public sector and healthcare are predicted to grow the most from 2020 to 2027. There is also a significant growth in the demand for cloud-based cyber security solutions. Cloud computing is widely adopted due to its powerful and flexible infrastructure. Cloud computing also allows organisations to combine supplementary infrastructure technologies such as software-defined

perimeters to create more secure platforms.

Tips:

Consider offering cloud-based solutions or services to tap into this trend. However, keep in mind the guidelines and regulations many European governments have issued regarding cloud platform security. The Cloud Industry Forum has released a Code of Practice for Cloud Service Providers. Cloud service providers aiming for the European market are recommended to follow this code of practice.

The European Union Agency for Cybersecurity (ENISA) is developing a cybersecurity certification scheme for cloud infrastructures and services. More information about ENISA's upcoming action will be announced on ENISA's website.

Specialise in a particular industry. Industries with specific security needs, for example because they deal with highly sensitive personal information, require specialists rather than generalists.

Research the industry that you want to focus on. This allows you to effectively market your company.

Through what channels do cyber security products and services end up on the end market?

You can use several trade channels to enter the European market. Figure 2 provides an overview of the trade structure for outsourcing. This structure is more or less the same in every European country.

Figure 2: Trade structure for outsourcing cyber security solutions in the European market

What is the most interesting channel for you?

Your most common and most promising market entry channels are:

- European service providers;
- consultants/matchmakers; and
- sales/marketing representatives.

Other possible channels are working with a local sales office or direct sales (including through online platforms).

Selecting a channel depends on:

- Your type of company;
- The nature of your product or service;
- Your target market;
- The available resources for market entry.

Regardless of the channel you choose, your own marketing and promotion is a vital part of your market entry strategy, and you are responsible for it.

European service provider

Your most realistic market entry channel is subcontracting for a European service provider. A European service provider that is similar to your company would be your most suitable contractor. Ideally, this company should design, develop, market, sell and maintain its own software products and offer IT services that are similar to

yours. And it should be located in your target country.

The relationship between this service provider and a subcontracted supplier is generally characterised by:

- Trust;
- Interdependence;
- A structured relationship (functions, tasks, communication and procedures);
- Potentially limited marketing visibility and market access opportunities for the subcontracted supplier;
- No intellectual property (IP) rights, or a loss of IP rights for the subcontracted supplier;
- Work orders on an if/when necessary basis.

You can find a European service provider either directly or by working together with a matchmaker and/or a sales representative. Because many European companies prefer to deal with a local contact person, an intermediary is a good option.

Tips:

Attend leading offline or online European trade fairs to meet competitors and potential customers, such as Gartner Security & Risk Management Summit and Infosecurity Europe. Do your homework and select events that fit your profile well. Create a list of relevant events using trade event directories such as 10Times, Expo Database and UK Exhibitions, and update this list regularly.

Use industry associations to find potential customers in Europe, such as the European Cyber Security Organisation ECSO, and IT associations like Bitkom in Germany, NLdigital in the Netherlands and techUK and BIMA in the United Kingdom. If you specialise in a particular industry, you can also use associations for those specific niches, such as the Association of British HealthTech Industries.

Use outsourcing associations to find potential customers, such as the Global Sourcing Association, the German Outsourcing Association and Sourcing Nederland.

Consultant/matchmaker

A consultant/matchmaker is a person or a company with a large number of relevant contacts in a specific market segment or industry. As an intermediary, they are a ‘door opener’ and not an agent to make cold calls or send cold emails.

Make sure you properly inform your consultant/matchmaker about your company. They speak with many potential customers and are often involved in creating long lists of potential outsourcing providers. The more information they have on your company and the better they understand your capabilities, the more they can spread the word about you.

If you work with a consultant/matchmaker:

- The consultant/matchmaker makes appointments with prospects for you;
- The presentation and sales process remains in your own hands;
- You pay a retainer + success fee (which can be expensive);
- The consultant/matchmaker usually has multiple clients;
- You need to set clear expectations and objectives to measure their performance.

A retainer + success fee construction can be expensive. While the success fee depends on what the intermediary has delivered, you have to pay the retainer (usually a fixed monthly payment) regardless of their performance. Together, they should provide a strong motivation for the intermediary to deliver: the retainer

should be high enough to cover some of the costs, but low enough to encourage delivery. A properly drafted contract, by a lawyer, is a must!

You also need to determine an exit strategy in the contract, with a clearly defined period after which the contract can be terminated without any further consequences. This period is usually not longer than 3 or 4 months, after which the contract will be evaluated and can be terminated or prolonged. For this period, there should be clearly defined delivery expectations and targets for the consultant/matchmaker (such as the number of relevant contacts, meetings and leads). You could also negotiate a trial period.

Tips:

When contracting an intermediary, involve a good lawyer who knows the applicable law of the country where the intermediary resides and has previous experience with this type of contracting. Pay special attention to exit clauses, success criteria, deliverables and payments.

Try to avoid limitations to your marketing coverage and activities in your contracts.

Some food for thought: although convenient, your uncle who lives in Germany might not be the best intermediary for your company.

Sales/marketing representative

Another type of intermediary is a sales/marketing representative. These representatives are more involved in the sales process than consultants/matchmakers.

When working with a sales/marketing representative:

- The sales/marketing representative contacts prospects for you;
- The sales/marketing representative also makes the sales and sometimes manages projects;
- You pay a retainer + success fee (which can be expensive) or a fixed monthly fee;
- The sales/marketing representative can have multiple clients or work exclusively for you.

A good sales/marketing representative has a large, relevant network, so they do not make cold calls to provide services for you. Their success fee is often a percentage of the projects they bring in. Your expenses will rise by having to pay a sales/marketing representative, but you will be free to focus on your core business and search for other markets yourself.

Tips:

Like with consultants/matchmakers, involve a good lawyer when contracting a sales/marketing representative and include exit clauses, success criteria, deliverables and payments.

Be cautious if intermediaries (both consultants/matchmakers and sales/marketing representatives) work based only on a success fee, because either they are excellent at their job or they are desperate and may not (be able to) deliver. Also, be cautious if intermediaries want to work for you part-time besides their regular job, because they are often so busy that they do not deliver.

Local sales office

Ideally, you should establish a local sales office in your European target market. A local presence makes it easier to build up long-term relationships with customers through personal contact. It also increases your credibility, builds trust and allows you to retain complete control over your marketing and sales activities. However, this is very difficult in practice, as it requires a lot of experience and large investments. Most companies in developing countries are simply too small and do not have the financial strength for this.

Tips:

Be aware that establishing a local sales office will be very costly, and you will need to have a strong financial position.

Consider establishing your own office if you have already established a client base in the target country/region, or if you have a well-founded indication of the demand for your services/products. If you decide to establish an office, involve your sales/marketing representative.

Look for alternatives to lower your costs, such as business incubators or government incentives to bring your business to a particular country or region.

Direct sales and online marketplaces

You can also try to sell your cyber security services directly to European end users. Many European companies are looking for cost reduction and delivery capacity, which developing countries can often provide. This is 1 of your unique selling points. However, you should be aware that these end users might not have qualified IT staff to work with. And European companies are generally hesitant towards outsourcing their security processes entirely.

Electronic marketplaces are a cheap marketing tool that may make direct sales easier. They also make it easier to find companies to work with as a subcontractor. Possibly as an independent consultant (someone from your team could do that) or as a subcontracting team. These platforms used to focus on freelancers, but they are increasingly suitable for SMEs.

Apart from online marketplaces, direct sales require experience in the European market. This strategy is most suitable for relatively large service providers that want to target large European end users. Your best bet is to focus on a small, underserved niche market.

For most suppliers from developing countries, it is very challenging to sell cyber security services directly. Sometimes, they work together to make a direct sales offer. Having 1 or more existing customers in Europe will help, as references are a must when you want to enter this market through direct sales.

Tips:

There are platforms that specialise in SMEs, like Appfutura and Talent Alpha, platforms that specialise in freelancers and platforms for both. Some examples are UpWork, Freelancer, Fiverr, ITeXchange, Clutch and pliXos. As a provider, you can usually join these types of platforms for free. For more information on online marketplaces, please read our news item about Open Talent Platforms.

Combine offline and online promotion channels to develop as many contacts as possible. This maximises your chances of finding suitable partners/customers. Use professional or other social media platforms as a marketing tool to reach potential customers. LinkedIn can be particularly useful for

making initial contacts and conducting market research.

Have a professional, high-quality company website, where you can present full, accurate and up-to-date details of your offering at low cost. Make it compatible with mobile devices and invest in Search Engine Marketing and Search Engine Optimisation, so potential customers can easily find you online.

3. What competition do you face on the European cyber security products and services outsourcing market?

Which countries are you competing with?

India, Romania, Poland, Czechia, Vietnam and the Baltics can be considered your strongest competition. We selected these countries based on their location, their ITO and BPO sector and the Global Services Location Index (GSLI).

The GSLI ranks the competitiveness of ITO/BPO destinations based on 4 categories: financial attractiveness, people skills and availability, business environment and digital resonance. The GSLI weighs the following selection criteria: digital resonance 60%, business environment 20%, financial attractiveness 10% and people and skills 10%.

In general, European companies prefer to outsource services to providers within the same country (also known as homesourcing, or simply as outsourcing). For more information on nearshoring versus offshoring, see our study on the European market potential for cyber security services.

India

India continues to lead the GSLI, mainly due to the combination of excellent English language skills and low-cost services. Because when it comes to digital resonance, India only takes 17th place.

Example: do not only compete on price
India was 1 of the countries to successfully tap into the first ITO and BPO demand wave and has been consistent in developing low-skilled workforces to meet traditional demand. However, with the current digital transformation, a gap has emerged between the demand for digitally savvy professionals and the talent pool that India is producing.

This illustrates that, although offering competitive rates is important, you should not compete only on price. As relatively simple (and therefore cheap) tasks can be automated, your focus should be on excellent skills, knowledge and creativity, which have a higher value. Demonstrating your commitment to quality through references and quality management systems is key to building trust among potential European clients, especially when it comes to cyber security services.

Romania

Romania is an Eastern European IT and BP outsourcing destination powerhouse. The IT sector is constantly growing and developing. There is a high level of digital technology adoption, and it has a large talent pool. It currently ranks number 32 on the GSLI. Romanian cyber security specialists have a strong knowledge of the English language.

The value of Romanian IT service exports is estimated at EUR 4 billion in 2020. Over 95,000 IT professionals are engaged in its IT sector. Around 32,500 graduates annually enter the market. Learn more about Romania as an ITO or BPO destination by reading its destination guide, issued by the German Outsourcing Verband.

Poland

As a Central and Eastern European (CEE) country, it benefits from European buyers' preference for nearshore providers due to proximity, language, cultural similarities and relatively small time differences (if any).

Cyber security professional rates are higher than in offshore destinations. However, these rates generally do not deter European buyers, who are often prepared to pay for the benefits that nearshoring offers them. Poland ranks number 14 in the GSLI and has increased in ranking by 10 points. This is primarily due to its financial attractiveness and start-up activity. Learn more about Poland as an ITO or BPO destination by reading its destination guide, issued by the German Outsourcing Verband.

The country is home to about 25% of the software developer population in the region, adding up to around 300,000 professional developers. These professionals rank as the number 3 best developers in the world, with a score of 93% in 2019, which further adds to Poland's popularity as a nearshoring destination. Polish people also score very high on English proficiency, making it relatively easy for European clients to communicate with them. This makes the country a particularly fierce competitor for you.

However, as its software industry flourishes, Poland may increasingly need to turn to offshore partners to meet demand. With the relatively high developer rates, Polish software companies can actually save quite some costs by outsourcing some development tasks or projects to you.

Czechia

Czechia is another well-known Eastern European nearshoring destination. Like Poland, the country benefits from its location close to the main Northern and Western European markets. There are more than 100,000 Czech software developers, who are rated as the number 6 highest quality in the world at just 0.3% behind Polish professionals. Czech people are also highly proficient in English. This makes Czech developers strong competition for you.

Every year, approximately 9,000 technical graduates enter the Czech IT market. About 130,000 professionals are employed in its information and communication sector. The number has grown for the past 10 years and has increased by 49,400 people.

However, the market faces a challenge: attracting new employees. Many Czech companies with IT vacancies struggle to fill these positions. Czechia has reported a higher than average percentage of firms struggling to fill IT vacancies since 2012. Since 2015, Czechia has ranked number 1 or 2 in the list of EU countries that were struggling to fill IT vacancies. This may drive Czech software companies towards subcontracting.

Vietnam

The Vietnamese outsourcing industry is relatively young, compared to the Philippines or India. However, in the past 10 years (2010 to 2020), the Vietnamese government changed its policy from a strictly controlled and centrally planned system to a more outward-looking, market-oriented economy. This has boosted the outsourcing sector greatly. The Vietnamese cyber security market is highly influenced by the Chinese market.

The country has climbed from number 24 to number 20 and then to number 6 (2017, 2019 and 2021) in the GSLI by improving its infrastructure costs and business environment. Vietnam is home to a large talent pool of software developers and cyber security specialists. And although Vietnamese people generally have low English proficiency, most Vietnamese cyber security specialists have intermediate to upper-intermediate English language skills.

Baltics

The Baltic region (Estonia, Latvia and Lithuania) is known as an economically stable region within Europe. It has a high level of digital solution adoption and effective legislation that ensures data security. The region has launched e-programs, has an ease of doing business (internationally oriented) and is known for its cyber security and low corruption rates. This helps grow the IT industry in the region.

However, the pace of software development market growth and the adoption of digital technologies are still moderate compared to the more well-known Eastern European outsourcing destinations (like Romania and Poland).

Tips:

Compete on the quality of your services, rather than just on costs. Specialise in specific vertical markets and/or niche market segments to avoid competition.

Invest in country branding. For more information on this topic, see our tips on doing business with European buyers.

Visit the websites of IT outsourcing associations and cyber security associations in particular, to get a better understanding of competing countries. Examples are the Central and Eastern European Outsourcing Association (CEEOA) and the Ghana Export Promotion Authority (GEPA).

Which companies are you competing with?

The key players operating in the global cyber security market include:

- Accenture;
- Capgemini;
- Cognizant;
- F5 Networks Inc.;
- FireEye Inc.;
- HCL Technologies Limited;
- IBM Corporation;
- Infosys Limited;
- L&T Technology Services Limited;
- PwC International Limited Broadcom Inc.;
- Tata Consultancy Services;
- Tech Mahindra Limited;
- Wipro Limited.

Some of them have offices in the below-mentioned countries. Examples of cyber security service providers from the selected 6 countries are:

India

IARM Information Security. A cyber security company that was founded in 2015. It also has an office in the United States of America. It provides cyber security services to both small and large companies. It knows how to adapt its services to its clients' needs.

Find more cyber security companies in India, and their reviews, on the website of Clutch.

Romania

Codespring is a Romanian software development and outsourcing company from Cluj-Napoca. It is active on the local and global market. It develops custom solutions and add-ons covering the entire life cycle of a complex software development project.

Codespring offers added value through business process know-how and technical expertise in a number of industries. Some of its strengths are its 15 years of experience, its dedicated teams, its European business culture and the ability to fine-tune its offer to any cooperation.

Find more cyber security companies in Romania, and their reviews, on the website of Clutch.

Poland

Infradata is a Polish cyber security company. It has a lot of international clients, like T-Mobile and big European universities (like the University of Groningen). It is an example of a good practise because its website is very structured, appealing and transparent. It uses clear icons and high-quality pictures, and the website gives off a personal feel, which is very important in the cyber security industry, where trust is very important.

Find more cyber security companies in Poland, and their reviews, on the website of Clutch.

Czechia

Cybersc – Cyber Security Consulting. This is a Czechia-based cyber security consulting company. It has ample experience in working for clients from Czechia and for clients from abroad. The services it offers include: penetration tests, purple teaming, application security design, security assessments, security consulting and cyber security awareness.

Find more cyber security companies in Czechia, and their reviews, on the website of Clutch.

Vietnam

Techlab Corporation. Clients like this company for its professional cyber security service, its focus on quality and its high-skill penetration testers and consultants. On its websites, it seems to talk to its existing and potential clients directly. It takes readers by the hand and makes them understand how working with it could improve their cyber security situation.

Find more cyber security companies in Vietnam, and their reviews, on the website of Clutch.

Baltics

The Baltic region consists of 3 countries: Estonia, Latvia and Lithuania. Trilight Security is an interesting example of a cyber security company from Estonia. It offers the following services: managed security, cyber security services, managed IT services and MSSP pricing.

Its clients praise it for client engagement, its knowledge of local legislation that the client needs, its ability to solve its clients' platform connectivity issues and its overall consistent communication and energy.

Find more cyber security companies in the Baltic region, and their reviews, on the website of Clutch: Estonia, Latvia, Lithuania.

Tip:

Search company databases to find more competing companies. These databases can be free, like company.info, or paid, via chambers of commerce (such as the Dutch Kamer van Koophandel) or commercial databases like Bold Data.

Which products are you competing with?

Everything that is connected to the internet needs cyber security measures. There are no products to compete with. The real question here is: what makes 1 service provider different from another?

The answer: technical knowledge, available capacity, references, domain knowledge, flexibility, scalability, reliability, communication and language capabilities, quality management, infrastructure, vertical and/or horizontal market focus and niche market orientation, among other things. The location (country) of the service provider is also an important factor.

Tip:

Find out how you can get a competitive advantage, based on factors such as quality, cost, technology or product characteristics. For ideas, study the annual Developer Skills Report. This includes the most popular programming languages and frameworks, the kind of frameworks hiring managers want versus the frameworks developers know (so you can see where there is more demand than supply) and much more.

4. What are the prices for cyber security products and services outsourcing?

Although price is often not the most important selection criterion for cyber security services, it has to be right and competitive. The price for cyber security products and services is influenced by technological requirements, skill levels, complexity of the project, length of the contract and other requirements written in the Service Level Agreement (SLA).

Your offer should include the price, with your hourly rates and an honest estimation of the number of hours you expect to work on the project. You also have to choose a price model for your product or service. There are 3 popular working models:

- Fixed-Price Contract;
- Time and Material Approach;
- Dedicated Team.

The most common price model for cyber security services is a Fixed-Price Contract. This is an all-inclusive offer, where clients are billed based on pre-defined milestones (in the SLA).

It is impossible to make an exact price breakdown. First of all, cyber security projects are so diverse that there is no single price breakdown that suits all (or even most) projects. Secondly, it requires so much estimating and unforeseen elements that even the process itself is an estimation. Cyber security projects change frequently, which raises other questions such as scope definition, change management and acceptance. Also, if the project uses Agile, there is no pre-determined specification, which makes estimation a big challenge.

What is clear, however, is that, if you focus on a niche market, European buyers are often less price sensitive.

Tips:

Study average prices in reports such as those by Cleveroad, DAXX, Qubit Labs or Yalantis and on SourceSeek. You can also research the average salaries for cyber security specialists via platforms like Payscale.

Create the 'ideal' client persona to help you tailor your offer. An example of a client persona is: 'a cyber security company with fewer than 200 staff members, in the Munich area, specialised in security applications for consumer IoT devices'.

Choose a type of price model for your outsourcing contract. For more information, see this paper on pricing models in outsourcing. Go beyond setting the right price and work out your pricing strategy. This could include your preferred pricing model (and your clients'), payment terms and expectations, and how and when you offer discounts.

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