ENTERPRISE IRELAND

#GlobalAmbition

THE EUROPEAN CYBERSECURITY MARKET

MAPPING THE OPPORTUNITIES AND ROUTE TO MARKET FOR IRISH SMEs

KEY TAKEOUTS

ceis

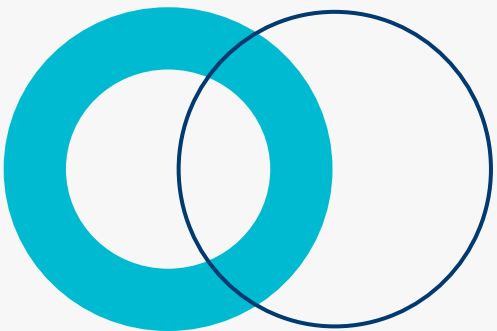
The European Cybersecurity Market

Mapping the Opportunities and Route to Market for Irish SMEs

REPORT SUMMARY

At a glance

- The research showed that although there are significant differences between the Cybersecurity markets of the eight countries studied, there are continued levels of growth across each market.
- Three opportunity clusters were identified in the European Cybersecurity markets that were investigated. These clusters were categorised by the size of the market, level of competition, maturity, policy framework and market accessibility.
- The clusters can be used as a guide for Enterprise Ireland client companies in prioritising their target export markets- either invest in a more challenging entry ticket to a mature, but high value-added market or focus their efforts on less mature but therefore also less saturated market.
- Confronted by the necessity to improve European Cybersecurity in order to ensure the safety and resilience of the economy and society, EU institutions and Member States are strengthening the relevant regulatory framework.
- The report provides nine recommendations for the Route to Market strategy for Cybersecurity companies, taking into account local cultural, political and economic factors.



An introduction to the report

This is the summary of a detailed report which presents an overview of the European Cybersecurity market opportunities for Enterprise Ireland (EI) client companies in eight targeted countries (Belgium, France, Germany, Italy, The Netherlands, Poland, Spain and the United Kingdom) and international institutions (European Union and NATO).

Research methodology

The study was divided into three distinct phases, which included desk research, qualitative interviews and data analysis:

- **Phase 1:** Initial Market Analysis aiming to address situation assessment of both offer-side (EI client companies) and demand-side (country-based market studies).
- **Phase 2:** Business Opportunity Identification based on the crossed analysis of key findings elaborated during Phase 1.
- **Phase 3:** Market Entry Strategy presenting recommendations and tools tailored for EI company clients, to be used for market prioritisation and market entry approach.

Purpose of the study

The study aims to provide EI client companies with bases from which to assess the selected eight markets and form a market entry strategy, with a view of increasing their export activities, by providing key findings, recommendations and tools.

Key Take Away

The identified country clusters can be used as a guide for EI client companies in prioritising their target export markets- either invest in a more challenging entry ticket to more mature, but high value-added markets, or focus their efforts on less mature, but therefore also less saturated markets. Furthermore, nine specific recommendations are given for the Route to Market strategy for Cybersecurity companies, taking into account local cultural, political and economic factors.

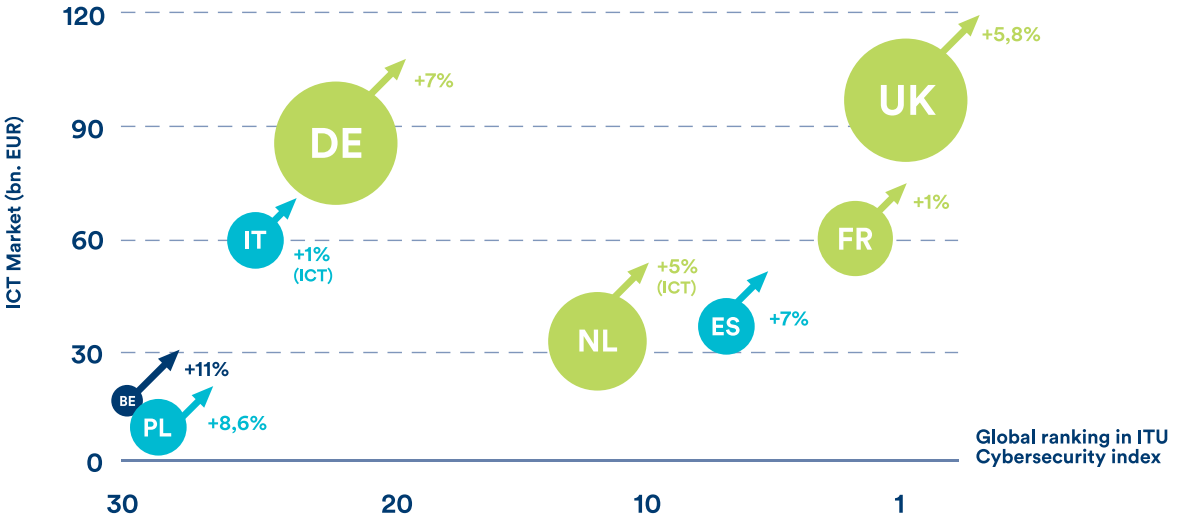
An overview of Cybersecurity in Europe

Over the past decade, Cybersecurity has become a priority for governments, companies and citizens across Europe. With the digital transformation of all sectors of society, Cybersecurity is now a crucial issue with growing needs for smart and user-friendly solutions designed to secure digital systems at large.

Three Opportunity Clusters

The analysis of national Cybersecurity markets led to the identification of three clusters among the targeted countries:

- **Cluster 1:** UK, Germany, France, The Netherlands: large and competitive markets supported by strong regulation from national authorities, and an important role played by and strong capacities of the public authorities.
- **Cluster 2:** Belgium: smaller and less mature market, presence of international organisations and large firms in the private sector, market attraction from neighbouring European countries.
- **Cluster 3:** Spain, Italy and Poland: relatively small size of Cybersecurity markets, significant structural economic challenges and/or lack of public investment.



National Cybersecurity market maturity assessment

- **Bubble:** Cybersecurity market size in billion €.
- **x-Axis:** ICT market size in billion €.
- **y-Axis:** Country's global ranking in ITU 2017 Cybersecurity index (GCI).
- **Arrow:** Growth rate of Cybersecurity market in percent and of ICT market, when information on Cybersecurity market growth rate is not available.

EU Cybersecurity Legislation

Confronted by the necessity to improve European Cybersecurity in order to ensure the safety and resilience of the economy and society, European institutions and the Member States are strengthening the relevant regulatory framework.

A European Union (EU) level Cybersecurity strategy was first adopted in 2013, and the first EU-wide Cybersecurity legislative act was the **NIS Directive** (Network and Information Security directive, part of the EU Cybersecurity Strategy), adopted in 2016. The NIS Directive sets mandatory minimums for Cybersecurity capabilities in the Member States for the protection of critical sectors. Seven categories of OES (Operators of Essential Services) are identified in the Directive: Financial market infrastructures, Banking, Transport, Drinking water supply and distribution, Healthcare, Energy and Digital infrastructure.

The second major legislative evolution, which took effect on June 2019, is the **EU Cybersecurity Act**. It follows an array of regulations setting the legal framework of the Digital Single Market, updating the mandate of the EU Agency for Cybersecurity (ENISA) and enabling the creation of an EU Cybersecurity certification scheme for ICT products, services and processes, the so-called Digital Single Market. Its objective is to eliminate unnecessary regulatory barriers in the digital sphere. In the long run, the Digital Single Market initiative will likely generate significant market opportunities for Irish companies.

A Report to Guide Market Entry

EU Member States reveal significant differences in terms of culture, organisation, investments, political will and capacities in the Cybersecurity domain. This study identifies a number of market trends and potential commercial opportunities which could provide valuable input into EI client companies' market entry strategy.

Opportunity Assessment Table

The table below presents a simple visual representation of the studied countries' key characteristics, such as the size of the market, nature of competition and market accessibility. It aims to provide an overview of the detailed information gathered during the country analysis.

	Market Attractiveness				Market Accessibility		
	Size	Growth	Competition	Comercial Opportunities	EI Client Experience	Information accessibility	Certification
European Union	Large	N.A	Large ICT companies				
NATO	Large	N.A.	Large ICT companies			NCIA opportunities	
Belgium	Small	SMEs	Few local actors	Market openness	Strong presence	Cybersecurity needs	
France	Large	Public Sector	National competitors	Finance Public		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 firms	Finance Public		Low trusted market estimations	Foreseen necessity for public sector
Netherlands	Relatively 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 international & local players	Strong demand		Commercial opportunities	Excepted catch-up effect
Spain		Catch-up effect		Important cybersecurity needs		Low information on National Strategy actions	Cryptologic certification
UK	Large Innovative	Public sector	High number of UK & foreign companies	Finance Public	1st export market		Large range of certifications

Negative **Neutral** **Positive**

Close-up of National Cybersecurity Markets

This section presents information about potential business opportunities in the countries studied, with a focus on the government and financial & banking sectors. As shown in the table below, each studied country was analysed across three factors: size and maturity, policy framework, and analysis of the national industrial ecosystem. The full report details these factors further and presents a more focused country-by-country opportunity assessment.

Country	UK	Germany
ICT market (bn. EUR)	97	85
Global 2017 ranking in ITU ICt Index	5	12
Cybersecurity market (bn. EUR)	6,4	5.7
Global 2018 ranking in ITU Cybersecurity Index	1	22
Policy framework	– Leading CS market in the world – Open & regulated – Dominant role of public security actors	– Public actors support – Strong investment – Leading role of Federal authorities – Effort by military actors
Domestic industry and ecosystem	– 846 CS firms – Major city concentration – Dynamic innovation system – NB: defence & security actors	– Strong foreign vs. local competition – Market close to saturation
Initial opportunity assessment	– Current healthcare & financial sector focus – Highly competitive – Strong presence of large foreign companies	– Niche tech opportunities – Lots of mid-size enterprises – Industry 4.0 focus
Major customers	**Government:** – Natonal Cyber Security Centre – National Cyber Security Programme **Finance & Banking:** – Financial Conduct Authority (FCA)	**Government:** – Federal Ministry of the Interior, Building and Community – Federal Office for Information Security – Central Office for IT in the Security Sphere **Bundeswehr (army):** – Focus on military CS – Cyber innovation Hub (2018) **Financial & Banking:** *Public sector* – German Central Banks – German Financial Supervisory Authority *Private sector* – DZ Bank – Volksbannk – N26
Flagship programmes	**Government:** NSCS Cyber Accelerator, GCHQ, CISP, Defence Cyber Protection Partnership **Finance & Banking:** – Finality – The Financial Services Sector Cybersecurity Profile – CBEST	**Government:** Allianz für Cyber-Sicherheit, Trust seal: *"IT Security made in Germany"* delivered by TeleTrusT, CIP plan, Brvarian Region Cybersecurity Strategy & initiative
Major providers	– BAE Systems – Qinetiq – Clearswift: focus on data protection – Silobreaker	**Government** *German actors:* – Bitkom – Airbus Defence & Space HQ – Rohde & Schwarz Cybersecurity *Value added Reseller Cybersecurity:* – Konica Minolta – SVA System Vertrieb – Logicalis Germany – Infinigate Deutschland – Ingram Micro Distribution **Finance & Banking:** *German actors:* – Funsters – Auxmoney – FinCompare *Foreigon actors:* – TransferWise – iZette – After Pay – Kredittech
Potential partners & market influencers	**Government:** *Clusters and associations:* – Cybersecurity Association UK Cyber Security Forum IISP **Finance & Banking:** *Clusters and associations:* – Financial Sector Cyber Collaboration Centre – UK Finance	**Government:** *Clusters:* – Blockchain Bundesverband – Bavarian IT Security and Safety Cluster – Nrw.unITS / Cyberforum /Cyber Security Cluster Bonne e.V. **Finance & Banking:** *Clusters:* – Digital Hub Cybersecurity – Frankfurt Finech Hub

Country	France	Netherlands
ICT market (bn. EUR)	60	33
Global 2017 ranking in ITU ICt Index	15	7
Cybersecurity market (bn. EUR)	2,5	3,8
Global 2018 ranking in ITU Cybersecurity Index	2	12
Policy framework	– Mature, regulated – ANSSI – Government support	– Mature, regulated – Government support NB role in private sector – Efforts to strengthen military CS
Domestic industry and ecosystem	– Global Franch It Companies in CS – Innovation ecosystem – SMEs difficulty in scaling – NB: defence & security actors	– Private-public partnerships – Natonal actors: CS distributors & services – No national leading companies
Initial opportunity assessment	– Mature, strong demand for CS – Partnerships with local actors – Need to engage with ANSSI	– Highly digitised economy – International workforce – Small internal market, may become overcrowded
Major customers	**Government:** – Ministry of Economics and Finances – Miinistry of Armed Forces – ANSSI **Financial & Banking:** – Société Générale – BNP Paribas	**Government:** ***Funds allocated to:*** – Ministry of Interior and Kingdom Relations – Ministry for Security and Justice – Ministry of Defence – Ministry of Foreign Affairs – Ministry of Infrastructure and Environment – Ministry of Economic Affairs **Procurement:** TenderNed **Financial Banking:** – Bank of the Netherlands ***3 bank conglomerates dominate the market:*** – ABN AMRO – Rabobank – ING Bank
Flagship programmes	**Government:** ANSSI - National Cybersecurity Plan, Sponsored projects like WooKey **Finance & Banking:** – BNP Paribas, Natixis & Societé Générale joined R3 open source blockchain platform – Société Général: 1st French banking CERT (2009).	**Government:** Global forum for Cyber Expertise (GFCE), National Cyber Security Agenda, Security Innovation in the International Zone **Finance & Banking:** – Holland Fintech – TIBER-NL and TIBER-EU
Major providers	**Technology leaders:** – Thales – Airbus – Defence and Space – Orange Cyberdefens **Integrators & IT services providers:** – Cap Gemini – Atos – Sopra Steria	**Government:** ***Large companies:*** – Orange (FR) acquired SecureLink (NL) offering CS services – Dutch Defence Cyber Command (DCC) and Thales entered into a contract in 2016 – Thales NL – Fokker Technologies – Fox-IT – SMEs: – Zivver – EclecticIQ – BWise ***Value Added Reseller Cybersecurity:*** – Copaco Netherlands – Micro Media BV – UBM Netherlands **Finance & Banking:** – SECURA – Dutch banks (ABN AMRO, Rabobank and IBM) receive security services from Akamai (US)
Potential partners & market influencers	**Government:** ***HEXATRUST:*** Luster of French innovative companies **Finance & Banking:** ***Banque de France:*** Cybersecurity seminar	**Government:** – Netherlands Foreign Investment Agency – Hague Security Delta Cluster

Country	Belgium	Spain
ICT market (bn. EUR)	16.6	36
Global 2017 ranking in ITU ICt Index	25	27
Cybersecurity market (bn. EUR)	0,4	1,3
Global 2018 ranking in ITU Cybersecurity Index	30	7
Policy framework	– Government Support – Regional dispaties – €15bn CS investment plan	– Slow digitisation – Public and private actors CS interest – NB role of security & military players
Domestic industry and ecosystem	– Shortage of CS experts – Few national CS companies – Brussels and Antwerp concentration	– Large Spanish defence & security firms dominate – Economic regional disparities – Rapid consolidation of market
Initial opportunity assessment	– Importance of industry – Niche tech & management services – Complexity of national institutional organisation – Growing need of SMEs	– Expanding CS market – Catch-up effect could open opportunities – Possible spillover in Latin American countries
Major customers	**Government:** – Centre for Cybersecurity Belgium (CCB) – Federal Computer Crime Unit – SPF BOSA **Financial Banking:** – EUROCLEAR – SWIFT	**Government:** – Defence Minister – Interior Ministry – Ministry of Energy, Tourism and Digital Agenda – Centro Nacional de Inteligencia – INCIBE – Procurement gateway for private & public actors – Procurement gateway for ministries of Industry, Trade and Tourism & the Secretary General for SMEs and Industry **Financial Banking:** – Banco Santander – CaixaBank – Bankia
Flagship programmes	**Government:** ***Belgium:*** Cyber Security Coalition, B-CENTRE, MoU with NATO ***Brussels:*** Programmes with Federal Agencies, the Police and the CCB, BICI ***Flanders:*** CS plan by Flemish Innovation Agency, dedicated initiative website, Cybersecurity in Flanders **Finance & Banking:** – TIBER BE - National Bank of Belgium (NBB) – B-HIVE - European collaborative innovation fintech platform – Belgian Mobile ID - Secure electronic identification service – The CCB's Early warning system	**Government:** Telefonica + Microsoft partnership, S2 Grupo, Eleven Paths (Telefonica Digital), Airbus BizLab, S21Sec **Financial Banking:** – BBVA innovation support program – Invest in Spain
Major providers	– Thales – Huawei – Sweepatic	**Government:** ***Market leaders:*** – Telefonica – Indra – Microsoft – S21Sec – Axians ***Market leaders:*** – Randed – Continuum Security – Titanium Industrial Security **Financial Banking:** – Kreditech (DE) – Ebury partnership with Spain Unicaja Banco – Oberthur Technologies – IBM – Redtrust
Potential partners & market influencers	**Government:** – L-SEC Association of Belgian Cybersecurity companies **Finance & Banking:** – Start it @KBC - community/accelerator – AGORIA – FEBELFIN	**Government:** – AEI Cibersugridad (working with public Cybersecurity entities) **Finance & Banking:** – Spanish Association of Fintech and InsureTech

Country	Italy	Poland
ICT market (bn. EUR)	61	9,9
Global 2017 ranking in ITU ICt Index	47	49
Cybersecurity market (bn. EUR)	1,1	1,2
Global 2018 ranking in ITU Cybersecurity Index	25	29
Policy framework	– Small CS market – Positive catch-up effect – Support for digitisation of public admin and industry	– Growing IT sector – Government support – CS hub aspirations – NB of EU funds in investment efforts
Domestic industry and ecosystem	– Dormant role of defence and security enterprise – Many SMEs entered CS market	– Dynamic IT security sector – Few high-tech companies developing domestically
Initial opportunity assessment	– Positive catch-up effect – Increasing maturity of actors and frameworks – Increasing awareness of CS need	– Growing spend on CS – 5th largest EU country (population, consumers) – Positive spillover effect in neighbouring countries possible
Major customers	**Government:** ***Call for tenders:*** – Ministry of Interior – Ministry of Defence – Ministry of Economic Development – Agency for Digital Italy **Financial Banking:** – Poste Italiane – Banca d'Italia – CERTFin	**Government:** – The Ministry of Digital affairs – The Ministry of National Defence **Financial Banking:** – Bank Polski
Flagship programmes	**Government:** Italian Army's first cyber range, Digital Public Administration projects (SPID, PagoPa, ANPR, FSR) **Financial Banking:** – Global Cyber Security Centre – ABI Lab – Spunta Project	**Government:** e-dowód (from Ministry of Digital Affairs), CyberSecIdent, cyber.mil.pl, N6 project, CyberSecIdent programme
Major providers	**Government:** ***Foreign players:*** – Deep Cyber & EclecticIQ – Huawei/ZTE – Kaspersky – US companies ***Italian players:*** – Leonardo's ***Value Added Reseller Cybersecurity:*** – Computer Gross Italia – Ultimobyte – Cybersel **Financial Banking:** – R3 – NTT Data (JP) – Sia (IT)	**Government:** – EXATEL **Financial Banking:** – Kreditech (DE) – Comarch – Asseco Poland
Potential partners & market influencers	**Government:** ***Clusters:*** – CYBAZE / Confindustria Digitale – Clusit – AIPSI – CIS Sapienza **Financial Banking:** ***Clusters:*** – Italian Banking Association	**Government:** – CYBERSEC HUB initiative in Krakow **Financial Banking:** – The Polish Bank Association

Cluster 1

United Kingdom

- **Leading Cybersecurity market in the world**
- **Open and legally structured to welcome foreign companies, yet highly competitive**
- **Dominant role of public security actors (48% in 2018)**

With an average growth of 3,9% over the past 5 years and 5,8% over the past 3 years, the UK Cybersecurity sector benefits from its large IT domestic market (5th largest worldwide).

The UK Cybersecurity market, however, remains vulnerable due to several factors. Firstly, a reduced talent pool, increasingly constrained by a growing market: this shortage affects SMEs in particular because of salary inflation. Secondly, the UK government covers many different public entities and agencies in the Cybersecurity field, thus leading to a multiplicity of governmental initiatives and increasing complexity.

Market makeup and support

There are a number of national and sectoral Cybersecurity strategies and tools. Public authorities and the private sector strongly focus on strengthening the healthcare and financial sectors' cyber resilience.

The UK Cybersecurity market is fragmented and highly polarised between SMEs and large firms, lacking mid-to-large Cybersecurity actors. The market tends to be dominated by non-specialised companies such as consulting firms (EY, PwC and KPMG), some forging partnerships with Cybersecurity technology firms (such as PwC with Tanium), defence companies proposing Cybersecurity products and services, big telecom players such as BT, offering managed cloud security, DDoS mitigation, SIEM threat monitoring; and information security/software societies such as Clearswift or Sophos.

Enterprise Ireland's initial opportunity assessment indicated that a strong presence of foreign companies can be observed, with a number of foreign companies acquiring UK Cybersecurity companies. The objective of these foreign companies is also to establish a part of their activities in the UK to benefit from the national ecosystem.

Germany

- **Very mature market**
- **Opportunities remain for those offering niche, high-quality technology in the industrial sector**
- **Dominant role of public security actors (48% in 2018)**

The German Cybersecurity market is expected to grow by 15% between 2018 and 2020, confirming its rapid expansion. The “Self-Determination and Safety in the Digital World 2015-2020” plan, launched by the federal government, aims to invest around €35 million annually into research in these key areas: High-tech for IT security, secure and trustworthy ICT systems, IT security in fields of application, privacy and data protection.

Market makeup and support

With a large industrial market that attracts cybercriminals, 2 out of 3 German manufacturers have been hit by some sort of cyberattack. Cybersecurity is high on the agenda with strong public-private sector cooperation.

Germany is marked by strong competition between large foreign players serving a myriad of clients from diverse industries. Yet there is still a strong role of medium-sized companies. In the Cybersecurity market, those medium-sized companies have managed to develop highly technical tools in niche technologies.

- Enterprise Ireland’s initial opportunity assessment indicated niche technology can counter market saturation. Client companies wishing to enter the market may also need to consider investing in a local office as German companies prioritise companies with a German-based presence, seen as a proof of reliability.

France

- **One of the most mature and regulated Cybersecurity markets in Europe with plenty of Government support**
- **Growth is still expected, although polarised by a handful of large players and small/micro-firms**
- **Through potential partnerships with local actors, there is an opportunity for SMEs willing to innovate**

The French Cybersecurity market is described as dynamic and high value, and compared to other leading markets, a catch-up effect has been happening in the last few years with 10% annual growth between 2015-2020. Three main drivers of future market development are Cloud, Industry 4.0 and IoT.

Market makeup and support

A small number of companies account for 75% of the total turnover of French Cybersecurity firms, and diverse types of customers shape the market:

- Public authorities and operators of vital services purchase Cybersecurity products and services under regulatory constraint
- A small number of mature organisations have specific and advanced needs in terms of products and services (e.g. Société Générale, LVMH, Enedis, Airbus, Total or Renault)
- A larger number of maturing customers have growing Cybersecurity needs, mostly medium and large SMEs

The French government established a strong public framework to help and stimulate the French Cybersecurity market. The ANSSI (the National Cybersecurity Agency) is a cornerstone of the Cybersecurity sector in France, developing a national strategy and vision on Cybersecurity.

The market is extremely polarised with a handful of big players, a myriad of small and micro-firms, and only a few mid-sized companies. Yet there is a vital SME and start-up ecosystem. Start-ups tend to collaborate with larger firms, who integrate their solutions into end-to-end services and products. And while the market enjoys strong innovation capability which enables the emergence of innovative SMEs and start-ups, these face difficulties in attaining critical size, defining their business models and attracting investors.

Enterprise Ireland's initial opportunity assessment indicated that there is a need to engage with French counterparts and to obtain ANSSI certification or qualification, which gives a product added-value by testing its compliance to French standards – enabling it to be integrated into French public systems.

The Netherlands

- **A highly digitised economy and one of Europe's leading Cybersecurity markets**
- **A strong international player presence, which both facilitates the entry of foreign actors and raises the risk of future saturation**

The Netherlands enjoys a Cybersecurity market in steady growth. From 2010 to 2014, the turnover and added value of Cybersecurity within the ICT sector increased by 14,5% annually.

Market makeup and support

The Dutch government puts Cybersecurity high on the national agenda via both legislation and capacity building. This is seen in the recent establishment of the Global Forum for Cyber Expertise in The Hague and the National Cyber Security Strategy released in 2018.

Dutch public and private actors are proactively scaling up their cyber capabilities. Currently, these are mainly Cybersecurity distributors and service providers but there is a keen focus on supporting start-ups in the market. In December 2018, TIIN Capital launched the Tech Security Fund, which focuses on early-stage companies and start-ups active in Cybersecurity and IoT Security solutions.

Enterprise Ireland's initial opportunity assessment indicated that although there is strong support from Government, public and private actors in the Cybersecurity sector, the internal market remains rather small and it is at risk of becoming overcrowded, highly competitive and saturated.

Cluster 2

Belgium

- **Government support and a €15bn Cybersecurity investment plan**
- **Opportunities for niche Cybersecurity technologies and services**
- **Mature market with regional disparities and territorial inequality: Antwerp and Brussels concentration**

The Belgian Cybersecurity market was worth €350 million in 2017, which is forecasted to at least double by 2022. It is a market that is difficult to characterise due to the intrinsic cultural and political divisions between the Flemish, Walloon and Brussels regions, which has led to parallel actions on Cybersecurity policy, investments and expenses.

Market makeup and support

A few large companies and a majority of SME's (95%) are at heart of the Belgian economy and these are particularly vulnerable in terms of Cybersecurity readiness: 8 out of 10 Belgian companies do not have any plans to counter cyberattacks. And while awareness of the need for Cybersecurity is high, there is a critical shortage of highly trained Cybersecurity experts, which could present an opportunity for foreign partners entering the market.

Government and public actor support for digitisation and Cybersecurity are evident with policies and frameworks such as the "Digital Belgium" plan; a €15 billion allocation for Cybersecurity between 2019-2030. There are also initiatives for public-private partnerships such as the Cyber Security Coalition; an initiative made up of members from the public, private and academic sectors which aims to build strong cooperation to tackle cybercrime.

Three different regional agencies with three different strategies to assist the private sector exist: the Flemish Agency for Innovation and Entrepreneurship (VLAIO), Evoliris (Brussels) and the Digital Wallonia agency. This has led to strong disparities, with the Flemish region taking the lead.

Enterprise Ireland's initial opportunity assessment indicated that there is an openness to external actors, with Belgian companies tending to outsource their Cybersecurity and data protection to other EU counterparts, a lack of qualified staff and need for prepared SMEs.

Cluster 3

Spain

- **A rapidly expanding Cybersecurity market driven by a handful of large companies**
- **Opportunities for niche Cybersecurity technologies and services**
- **Plenty of public and private actors' interest in Cybersecurity and potential to facilitate future market entry into Latin America**

The Spanish Cybersecurity market is estimated to grow by 7% between 2018 and 2019. It has initiated a catching-up (partly due to the implementation of the GDPR) that has strongly impacted the market. There is a recent move towards digitisation in the private sector, with a majority of Spanish companies only recently realising the potential of digitisation. The market is thus likely to grow rapidly in the coming years as companies will need competent partners to secure their new activities and tools.

A lack of preparedness dominates the Cybersecurity market in Spain. 1 out of 3 Spanish citizens has declared being a victim of some sort of cyberattack and only 1 out of 5 Spanish business owners feels "well-prepared" to face a cyberattack. This is leading to support from Government, private and public sectors.

Market makeup and support

In 2019, Spain launched a €130 million investment plan for digitisation of the private sector. The "Plan for Digital technologies" is likely to accelerate the ongoing digitisation of the private sector, opening up a new market of companies in need of Cybersecurity services and products.

- Enterprise Ireland's initial opportunity assessment indicated that Spain is a rapidly expanding Cybersecurity market driven by a handful of large companies and that there could be a real entrance point for companies which have developed high-level cyber defence-related technologies and tools.

Italy

- **Smaller and less mature Cybersecurity market compared with European counterparts**
- **Support for the digitisation of public administration sector and industry**
- **Positive catch-up effect which could lead to commercial opportunities for Cybersecurity services and products providers**

Forecasts of the Italian ICT market are optimistic with an annual growth rate of 2,7% between 2018 and 2020. The market is currently driven by European regulatory developments (GDPR and NIS directives) rather than a risk-based expansion. This is increasing awareness about the need to invest in Cybersecurity amongst Italian companies.

Market makeup and support

Italy published two documents in 2013, making up a comprehensive national Cybersecurity strategy:

- The National Strategic Framework for Cyberspace Security which provides strategic and operational guidelines for improvement.
- The National Plan for Cyberspace Protection and ICT Security which is an implementation plan identifying tools and procedures to enhance Italy's cyber preparedness.

The Italian Cybersecurity market has long been driven by large enterprises, however a growing number of SMEs have recently entered the Cybersecurity market.

Enterprise Ireland's initial opportunity assessment indicated that the Italian public sector could offer commercial opportunities for Cybersecurity services and products providers. In the industrial sector, the "Industria 4.0" National Plan represents a major opportunity for companies who wish to take advantage of the incentives offered.

Poland

- **Growing IT sector with Governmental support**
- **A market far from saturated with Cybersecurity hub aspirations**
- **Importance of EU funds in investment efforts**

Poland has noted a stable growth trend in recent years, with an average annual increase of turnover amounting to over 8.6%. There is an increasing level of awareness of the importance of Cybersecurity in Polish companies. The number of cyber-attacks in Poland in the first half of 2018 was twice as high as for the same period of 2017.

Market makeup and support

In May 2017, the Polish Government adopted "The National Framework of Cybersecurity Policy of The Republic of Poland for 2017-2022". This policy aims to raise the level of Cybersecurity in Poland and to identify the necessary mechanisms and measures to strengthen Poland's Cybersecurity capabilities by 2022.

Several global IT players are present in Poland and there are currently very few Cybersecurity start-ups. The National Framework Policy states that the Polish government "aims to invest in the development of industrial and technological resources for Cybersecurity, by creating the conditions needed for the development of enterprises, scientific research centres and start-ups in the area of Cybersecurity".

- Enterprise Ireland's initial opportunity assessment indicated that Poland has a dominant demographic, political and economic position in the region. Investments in Poland may, therefore, have positive spill-over effects into neighbouring countries. The government proactively supports the Cybersecurity sector and is looking to position the country as a regional Cybersecurity hub. Companies investing in Poland can receive assistance from the Polish government, including for the creation of industrial and high technology zones allowing a synergy with companies working in the same sector.

Recommendations and tools for Route to Market

The key recommendations presented in this section were developed based on the analysis of the European and national Cybersecurity market landscape, the assessment of the EI Cybersecurity cluster and the operational insights of Cybersecurity stakeholders and experts. The sample of EI client companies analysed for this study reveals a diversity of profiles. The following recommendations are general best industry practices, however there is no “one size fits all” approach.

Recommendations

1. Have your product/service included in major ICT companies, integrators and Cybersecurity providers' offer to large customers.

The trend in large European companies is towards a reduction of the number of Cybersecurity solutions deployed, in effect reducing the opportunity spectrum for niche-technology providers. Major companies tend to privilege large prime contractors, and SMEs tend to be excluded from such tenders.

2. Obtain the relevant European or national certification for competitive advantage.

The certification of products or services brings real added value. While respecting regulatory requirements ensures conformity, and as such is a sine qua non for customers in mature markets, certification provides additional proof of the high quality of a Cybersecurity product or service.

"As a Cybersecurity provider, we do not handle the compliance or certification process of a partner's solution – some rare examples were done in France for niche technology start-ups."

- European integrator (Belgium)

"The KSO3C project is developing a national evaluation and certification body ... by 2021, with a "shadow certification" scheme ready by 2020. Poland is a member of the EU SOGIS agreement, but we need this body to select components for current projects (like the French ANSSI and German BSI)."

- Polish government official

Recommendations and tools for Route to Market

3. Find a sponsor in your target end-customer.

To increase chances of being selected by a large prime contractor, as recommended above, direct contact with the right decision-maker in the end-customer entity can go a long way, by allowing the SME to present its product or service and pitch its relevance to the end-customer's needs. Once convinced, the end-customer decision-maker may encourage the prime contractor to integrate the SMEs product/service into its offer.

"Large companies remain sensitive to the qualities of SMEs: more flexible and dynamic, less administrative, more reactive, more innovative."

- Large French bank

"SMEs are the backbone of the Italian economy and are present in the supply chain across the economy, yet have very limited awareness of Cybersecurity and aren't investing enough. They mostly buy less expensive off-the-shelf products from US firms. Even in large Italian firms, there is an awareness gap."

- Italian government official

4. Ensure compatibility and interoperability with target customer's systems.

Products and services must be compatible with existing systems and architectures in place in targeted markets. A Cybersecurity solution can be innovative and respond to a pressing need, but if it is not interoperable with legacy systems, its integration will constitute an often insurmountable cost for potential customers.

"If a provider's offer is compatible with the most common IT systems, it can reach 85-95% of French industrial actors."

- Large French bank

5. Leverage available networks to gain access to new markets.

Less mature markets face structural, political, economic and cultural difficulties. Without a presence on the ground, navigating these difficulties can be complex. Entering a foreign market can require a local presence.

"There is no law mandating working with a local entity, but without it, foreign companies don't stand a chance of working for the Italian government, especially SMEs."

- Italian government official

"The French market is highly competitive, new actors should strongly consider building a local partnership."

- Large French bank

"The French market is highly competitive, new actors should strongly consider building a local partnership."

- Large French bank

6. Join European Commission research projects for network and reputation (e.g. H2020 programme related to Cybersecurity, European Defence Fund).

European research and innovation projects can open doors. Beyond benefits, participation in these projects can yield visibility with foreign actors in both the public and private sectors. European research and innovation projects impose dissemination activities, allowing participants to grow their network, build relationships overseas, and open up further opportunities.

"There is a current trend in regulated sectors towards externalisation of Cybersecurity as a service (incident response, pentesting)."

- European Commission official

"The "Common IT System" project will deploy a hybrid government Cloud (most sensitive data) and a public Cloud environment for local/regional administrations (with a dedicated marketplace for selected public Cloud providers (infrastructure & services)."

- Polish government official

7. Capitalise on current "hot" Cybersecurity sub-segments.

The growth of the European Cybersecurity market is driven by key sub-segments. Currently, these are mainly related to data protection, identity management, Cloud migration and IoT deployment. These sub-segments concern entities across the public-private divide, large and small, reflecting the adoption and deployment of new technologies and solutions within organisations.

"The banking and financial sector is the biggest spender after the military & intelligence services. The focus on the G7 on Cybersecurity in this sector illustrates its importance."

- Italian government official

"Identity management is a 'hot' topic: the new Polish e-ID will cover all types of public services for citizens (e.g. health, bank, communication with government). It is managed at the federal level with a protective profile."

- Polish government official

8. Keep a close eye on European and national legislative developments.

National Cybersecurity markets are stimulated by regulation: Cybersecurity remains a cost for economic actors, which depending on the sector and size

of the company can appear as non-essential. Cyber-attacks are often the deciding factor in the deployment of Cybersecurity measures and increased awareness.

In less mature markets, customers still tend to take a compliance approach to Cybersecurity (e.g. with GDPR or NIS Directive) rather than a risk-based approach. This can pose an obstacle to commercial opportunities, with some customers going for the cheapest or easiest option rather than the one most appropriate to their (real) need. But regulation progress still generates a technical and regulatory transition for European public and private stakeholders, with a more urgent need depending on the sensibility of the activity sector.

"The NIS Directive opens a market with local/regional administration and medium enterprises as end-customers."

- Polish government official

9. Develop an official Irish Cybersecurity label or certification.

"Country-labelled" products and services are a mark of trust for consumers.

"The newly created national certification scheme will play a key role: it will become necessary for a Cybersecurity company to be stamped for approval to get access to public procurement."

Tools to use to define your strategy

During the preparation of this report, we identified two visual tools to give input to EI client companies as they begin to define their strategy to address one or several of the targeted national markets:

1. Opportunity Assessment table which can be used as a market assessment tool to prioritise market attractiveness and market accessibility;
2. A comprehensive visual representation of the Cybersecurity value chain, which identifies needs in each section of the value chain;
3. A market-approach decision tree using EI client company characteristics (type of products and/or services proposed, investments capacities and risk profile).

More details on the tools and templates used in gathering data for this report are available in the full report

Conclusion

As this study demonstrates, although there are significant differences between the cybersecurity markets of the eight countries studied, there is continued levels of growth across each market.

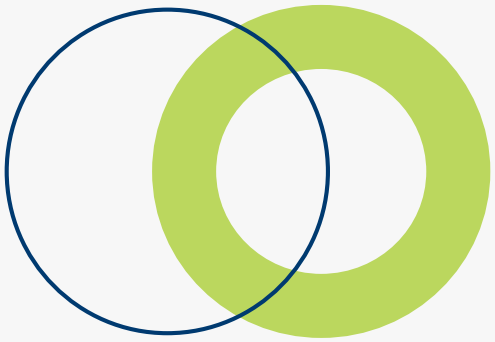
Cybersecurity has become a priority for governments, companies and citizens over the last decade. With the digital transformation of all sectors of society, Cybersecurity is now a crucial issue with growing needs for smart and user-friendly solutions designed to secure digital systems at large.

For EI client companies, two Routes to Market are suggested:

1. Invest in a stable, mature and high-value market as identified in Cluster 1, or;
2. Focus efforts on less mature Cluster 2 and 3 markets that may prove fruitful in the future.

The trends and recommendations outlined in the report provide valuable input for Enterprise Ireland client companies to determine their market prioritisation and Route to market approach.

The full report delivers insightful recommendations and operational perspectives on the eight targeted national markets and includes actionable tools, templates and resources to further support companies.



Enterprise Ireland is the government organisation responsible for the development and growth of Irish enterprises in world markets. We work in partnership with Irish enterprises to help them start, grow, innovate and win export sales in global markets. In this way, we support sustainable economic growth, regional development and secure employment. Learn more at www.enterprise-ireland.com.

CEIS was commissioned by Enterprise Ireland to execute this market scoping. CEIS is a leading strategy and risk-management consulting firm. CEIS has over ten years experience in delivering consultancy and research services to European and International, public and private clients, with key focus on areas like Cybersecurity & Digital Transformation.

Enterprise Ireland
East Point Business Park
The Plaza
Dublin 3
D03 E5R6
+353 (1) 7272000