



CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

EU Cybersecurity Market Opportunities and Irish Solution Mapping

April 2026

Cyber Ireland / Munster Technological University



Rialtas na hÉireann
Government of Ireland



Co-funded by
the European Union



CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



Funding note: This report was published by Cyber Ireland and Munster Technological University (MTU) in collaboration with the National Cyber Security Centre (NCSC), as part of the NCC-IE Cyber Community Project.

The project was supported by the NCC-IE, funded by the Government of Ireland and European Commission. It is co-funded by the European Union under the Digital Europe Programme, Project: 101127902 – NCC-IE – DIGITAL-ECCC-2022-CYBER-03.



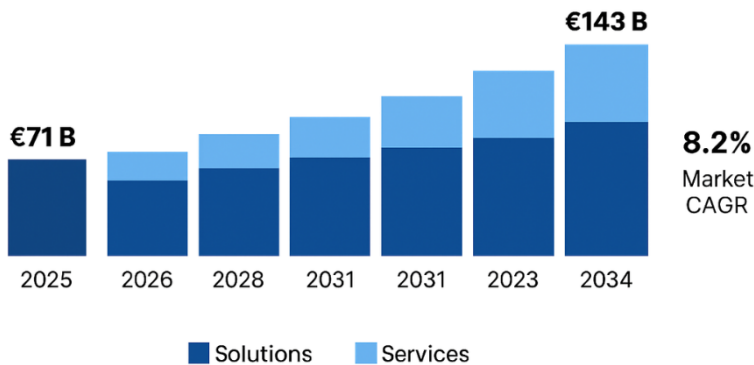


EXECUTIVE SUMMARY

EU CYBER MARKET GROWTH

Europe Cybersecurity Market Forecast

Size, By Component, 2025–2034 (€ Billion)



KEY EU LEGISLATION IMPACTING MARKET DEMAND

NIS2

DORA

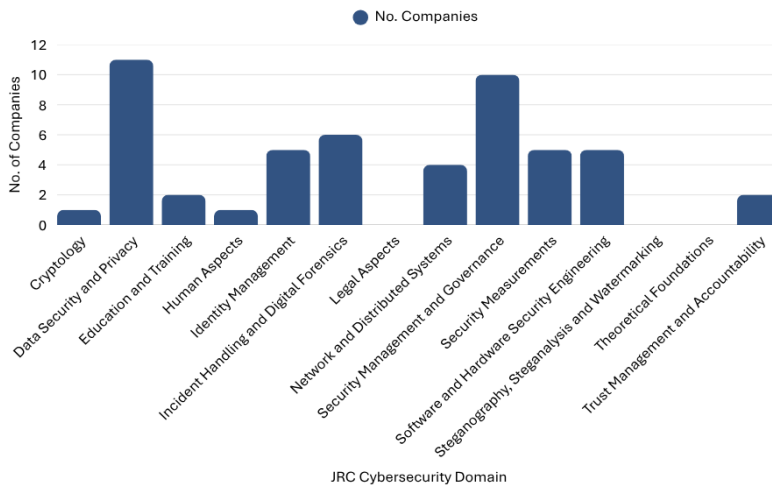
CRA

CYBERSECURITY ACT

AI ACT

IRISH CYBERSECURITY SOLUTION MAPPING

52 Irish cybersecurity companies (export-focused) analysed:



CERTIFICATION ANALYSIS

- Top certification – ISO 27001 (10 companies)
- 36 - Companies with no certification listed

MARKET OPPORTUNITIES

1. EU Market Growth and Expansion
2. Enhancing Security and Trust with Certification
3. Supporting a pipeline of cybersecurity skills
4. EU Funding Opportunities in cybersecurity

MARKET CHALLENGES

1. Compliance Cost and Complexity for cybersecurity companies
2. Increased Market Competition:
3. Technological Sovereignty Restrictions
4. Skills Competition and Shortages



CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



Contents

1. Introduction.....	5
2. Methodology.....	5
Limitations and Future Research.....	6
3. EU Cybersecurity Regulation and Market Demand	6
4. Irish Cybersecurity Solutions Mapping.....	8
Certification Analysis.....	10
5. Recommendations – Market Opportunities and Challenges.....	12
Opportunities	12
Challenges.....	12
Appendix – Key Legislations and Market Impact.....	14





CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



1. Introduction

The European Union (EU) is taking an increasingly central role in cybersecurity through cybersecurity legislation such as the NIS2 Directive and Cyber Resilience Act to legislation with specific cybersecurity provisions such as those found in the AI Act. These regulations, first and foremost, aim to strengthen the EU's cyber resilience, safeguarding communications and data, and keeping our online society and economy secure. The regulations will also drive increased demand for cybersecurity solutions, both products and services, and with harmonised cybersecurity standards it will make the EU cybersecurity market more open.

Irish cybersecurity companies should prepare, develop and market solutions, but product and services, tailored to the specific requirements of these regulations. This has the double effect of meeting the EU market opportunity, while also scaling Irish companies who can then provide cybersecurity domestically.

Cyber Ireland was tasked by the National Cybersecurity Coordination and Development Centre (NCC-IE) to investigate the potential for Irish companies to meet this increased demand for cybersecurity solutions through mapping the cybersecurity solutions available in Ireland from export-focused, Irish-owned suppliers. This research aims to understand where strengths and gaps exist in relation to the provision of cybersecurity solutions, with potential market opportunities in the European Union from cybersecurity regulation and digital sovereignty.

The results are of value for Irish cybersecurity providers to understand the impact of EU regulation and market opportunities. It also assists government bodies responsible for cybersecurity and industrial development to identify opportunities and address challenges to growth.

2. Methodology

The research first reviewed EU regulations including: 1) cybersecurity focused legislation, 2) sector specific cybersecurity initiatives, 3) legislation with cybersecurity provisions and broader legislation that has an impact on cybersecurity. It assessed their impact on the cybersecurity market to understand which solutions will be in higher demand and where new opportunities may emerge for Irish solution providers.

A mapping of Irish cybersecurity companies who are export-focused was conducted, utilising Enterprise Ireland's (EI) cybersecurity client list. These companies' cybersecurity solutions were classified using [JRC Cybersecurity Domains](#) taxonomy, as it has a manageable 14 categories and is replicable at EU-level. Furthermore, the company size, export focus, and publicly available cybersecurity certifications were assessed.





CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



Limitations and Future Research

While Enterprise Ireland's client list provides a good foundation for identifying export focused indigenous companies, it may miss companies that are not in EI's portfolio, or those that are not designated pure-play cybersecurity and may provide a cyber offering, such as managed service providers. Additionally, it misses cybersecurity companies focused on the domestic market that may have potential for expansion into the EU. Further research is recommended to broaden the mapping of Irish solution providers.

Three taxonomies were assessed as to their suitability for solution mapping; a dedicated EU cybersecurity solution taxonomy linked to a cybersecurity framework, such as [Cyber Fundamentals](#) (CyFun) would be more appropriate for future research.

3. EU Cybersecurity Regulation and Market Demand

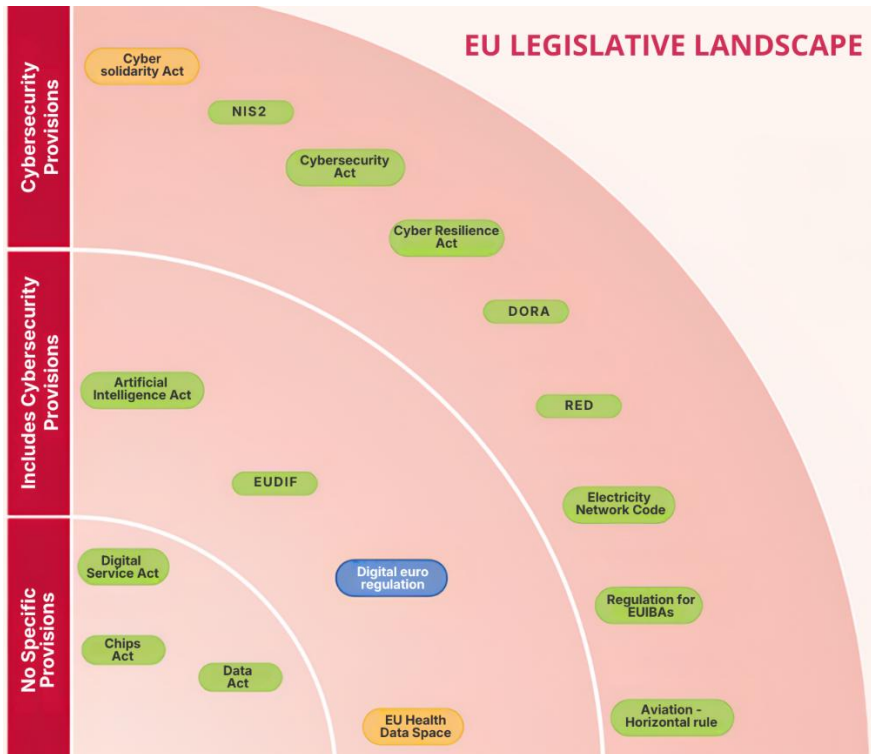
The EU is taking an increasingly central role in cybersecurity with specific cybersecurity regulations that aim to improve the EU's cyber resilience, safeguarding communications and data, and keeping the online society and economy secure. These include:

- a. Cybersecurity focused legislation and sector specific cybersecurity initiatives
- b. Legislation with cybersecurity provisions
- c. Broader legislation that has an impact on cybersecurity.



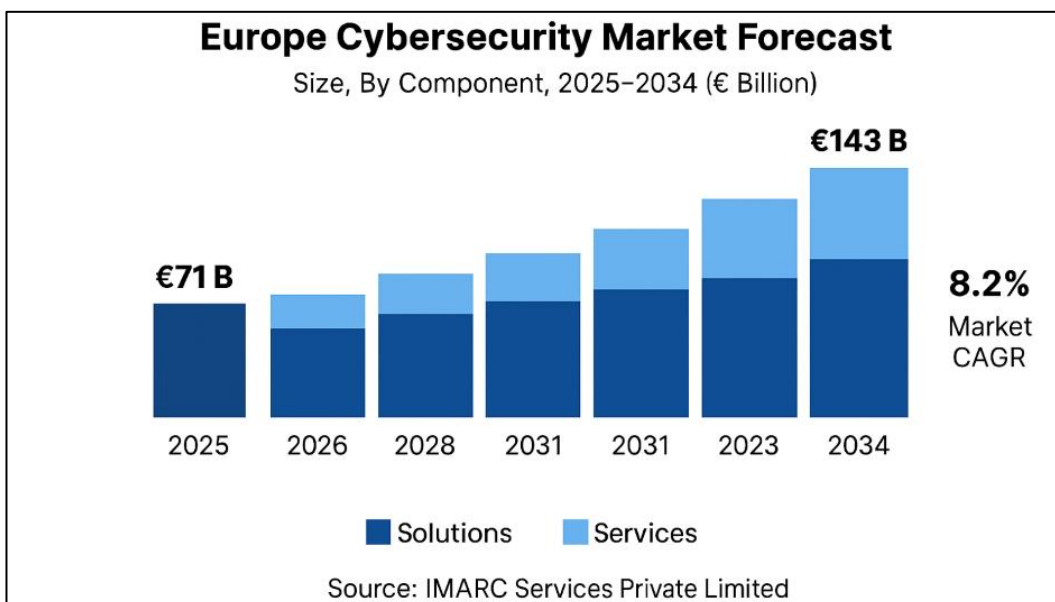


Figure 1: Overview of EU cybersecurity legislative landscape (ENISA 2024)



The cybersecurity market consists of products (such as anti-virus, patch management, identity access management, encryption, compliance, etc.) and services (consulting, risk assessments, training and education, managed security services). The cybersecurity market has been growing steadily due to increasing adoption of digital technologies, heightened regulatory compliance and the cyber threat landscape.

Figure 2: Europe Cybersecurity Market Forecast (Source: IMARC Group)





According to research by [IMARC Group](#), the European cybersecurity market, including the United Kingdom, generated a revenue of USD 81.81 Billion in 2025 (€71B) and is projected to reach a revenue of USD 165.73 Billion by 2034 (€143B), growing at a compound annual growth rate of 8.2% from 2026-2034. Regulatory frameworks including NIS2 and DORA establish permanent security spending floors while expanding coverage to mid-market firms previously exempt from mandatory cybersecurity requirements.

This figure may even be under-estimating the increased demand from other legislations including CRA, AI Act and other EU legislation. The demand for cybersecurity solutions from these regulations are captured in the **Appendix – 'Key Legislations and Market Impact'**.

4. Irish Cybersecurity Solutions Mapping

A total of 52 companies in Enterprise Ireland's cybersecurity client list were analysed, each classified using the [JRC Cybersecurity Domains](#) as a solution taxonomy. Furthermore, the company size¹, export focus, and publicly available cybersecurity certifications were assed.

Table 1: Cybersecurity Companies by Domain

JRC Cybersecurity Domain	No. Companies	Percentage
Cryptology (Cryptography and Cryptanalysis)	1	2%
Data Security and Privacy	11	21%
Education and Training	2	4%
Human Aspects	1	2%
Identity Management	5	10%
Incident Handling and Digital Forensics	6	12%
Legal Aspects	0	0%
Network and Distributed Systems	4	8%
Security Management and Governance	10	19%
Security Measurements	5	10%
Software and Hardware Security Engineering	5	10%
Steganography, Steganalysis and Watermarking	0	0%
Theoretical Foundations	0	0%
Trust Management and Accountability	2	4%
Total	52	100%



To clearly identify the level of capability within each cybersecurity domain, the following colour coding based on company size has been used:

- **Green – Strength:** Domains where there are several companies, including medium and/or large size are present. These firms provide scale, export readiness, and advanced solution capability.
- **Orange – Potential Strength / Gap:** Domains represented by a low number of companies who are micro and/or small-size. These areas have emerging capability and show potential for future scaling.
- **Red – Gap:** Domains without medium or large companies and with only one or no small company involvement. These represent capability gaps requiring attention, support, or strategic development.

Table 2: Number of Cybersecurity Solutions by Company Size

JRC Cybersecurity Domain	Micro	Small	Medium	Large	Total
Cryptology (Cryptography and Cryptanalysis)	0	1	0	0	1
Data Security and Privacy	3	7	1	0	11
Education and Training	0	2	0	0	2
Human Aspects	0	1	0	0	1
Identity Management	0	4	1	0	5
Incident Handling and Digital Forensics	0	4	2	0	6
Legal Aspects	0	0	0	0	0
Network and Distributed Systems	0	4	0	0	4
Security Management and Governance	3	6	0	1	10
Security Measurements	2	3	0	0	5
Software and Hardware Security Engineering	1	2	2	0	5
Steganography, Steganalysis and Watermarking	0	0	0	0	0
Theoretical Foundations	0	0	0	0	0
Trust Management and Accountability	0	2	0	0	2
Grand Total	9	36	6	1	52
Percentage	17%	69%	12%	2%	100%



Strengths to build on:

- There are mature Irish cybersecurity providers (Medium and Large) in high-demand domains such as Data Security & Privacy (21%), Security Management & Governance (19%), and Incident Handling & Digital Forensics (12%).
- There are 43 companies, 83%, with more than 10 employees (small, medium and large). Export-focused companies are generally larger than domestic focused companies, providing scale and maturity.
- There is coverage across all but three domains, when small companies are included.
- There is potential to scale those small companies in domains where there is an absence of a medium / large supplier such as: Cryptology, Education and Training, Human Aspects, Network and Distributed Systems, Security Measurements, Trust Management and Accountability.

Gaps – improvement opportunities:

- Five domains show limited (one small company) or no representation from medium or large companies (orange or red), signalling capability gaps where targeted support or strategic initiatives could help strengthen the ecosystem.
- Cryptology, Human Aspects, Legal Aspects, Steganography / Steganalysis / Watermarking, and Theoretical Foundations have either no companies or only one company active in these areas. These domains could be prioritised by helping existing domestic or small suppliers scale or incentivising other companies into these areas.
- For Ireland to deliver high-complexity, enterprise-level cybersecurity solutions and compete consistently in foreign markets, increasing the number of medium/large firms—or supporting high-growth scaling—will be essential.

Certification Analysis

To compete effectively in the European cybersecurity solutions market, Irish indigenous companies must demonstrate strong operational security and compliance. Certifications are not just badges—they are essential indicators of trust, resilience, and regulatory alignment.

Companies' certifications advertised publicly on their websites were recorded and analysed.



Table 3: Number of companies with common cybersecurity certifications

Certification	No. Companies	Percentage
ISO 27001 - Information security management systems (ISMS)	10	18.18%
ISO 27701 - Privacy Information Management System (PIMS)	2	3.64%
ISO 20000-1 - IT Service Management (ITSM)	0	0.00%
SOC 2 - System and Organization Controls 2	4	7.27%
ISO 22301 Business Continuity Management Systems (BCMS)	0	0.00%
NIS2 Compliance via CyFun	0	0.00%
EUCS (EU Cloud Services Scheme)	0	0.00%
UK Cyber Essentials	3	5.45%
None	36	65.45%
Total	55	100.00%

Strengths to build on

The most common certification is ISO 27001 with 10 companies accounting for 18% of the total. ISO 27001 is a globally recognized standard for information security management, which strengthens trust and compliance with international requirements.

Gaps – improvement opportunities:

Four certifications are not present in any company: ISO 20000-1, ISO 22301, NIS2 Compliance via CyFun, EUCS (EU Cloud Services Scheme).

There are 36 companies (65%) which don't hold any certification, or it was not noted publicly on their website. 16 companies (38% of the group) hold at least one certification. Given the regulatory trajectory of the EU and the increasing importance of certification for trust, procurement, and market access, this represents a strategic gap for the Irish cybersecurity sector.

The CyFun Framework provides an opportunity for export-focused Irish companies to attain a nationally recognised certification for NIS2 compliance, when the scheme is implemented, with the potential for it to become EU-wide.

In future research, range of certifications analysed could be expanded to include: CREST, TEMPTTEST, IEC62443, OWASP, CSA STAR.



5. Recommendations – Market Opportunities and Challenges

Opportunities

1. **EU Market Growth and Expansion:** Cybersecurity companies should prepare, develop and market solutions tailored to the specific requirements of these regulations, such as risk assessments, compliance tools, managed security services, and AI security. Companies should partner or acquire local cybersecurity providers to gain access to new EU markets.
2. **Enhancing Security and Trust with Certification:** Cybersecurity companies should invest in obtaining certification, such as EU Cybersecurity Certification Framework, ISO 27001, or CyFun, to ensure compliance and build trust with customers and partners. Highlighting certification in marketing materials can increase leads and meet customer requirements.
3. **Supporting a pipeline of cybersecurity skills:** Education and training providers in Ireland should develop and provide accredited training to upskill industry professionals for in demand cybersecurity roles relating to EU cybersecurity regulation. The training should utilise competency mapping of the skills required for these roles, leveraging frameworks such as the European Cybersecurity Skills Framework (ECSF).
4. **EU Funding Opportunities:** Irish cybersecurity companies should explore EU programmes and funding opportunities that support cybersecurity research, development, deployment and training, which aligns with their strategy.

Challenges

1. **Compliance Cost and Complexity:** Cybersecurity companies will need to invest in comprehensive compliance strategies to manage the costs and complexities associated with adhering to multiple regulations either directly or indirectly, such as NIS2, DORA, the CRA, and AI act.
2. **Increased Market Competition:** Cybersecurity companies should prepare for increased competition in the Irish and EU market particularly for large companies, regulated entities and public sector contracts. To remain competitive, companies will need to: differentiate offerings, scale and innovate.
3. **Technological Sovereignty Restrictions:** Ireland will need to navigate the challenges posed by the EU's focus on technological sovereignty. Irish companies taking on investment from outside the EU should be made aware of the impact on EU ownership and control restrictions.
4. **Skills Competition and Shortages:** Irish cybersecurity SMEs should invest in training and development programs for existing staff. Creative recruitment strategies could be adopted exploring career changers and non-traditional backgrounds.



CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



Overall, this report identifies both strong existing capabilities and clear areas for development. Ireland's cybersecurity sector is well positioned to benefit from regulatory driven EU market expansion, particularly in solution areas aligned with security governance, data protection, and incident response. To fully capitalise on upcoming opportunities, companies will need to invest in certifications, scaling, innovation, and compliance capabilities



Appendix – Key Legislations and Market Impact

Table X presents the key legislations impacting market demand for cybersecurity solutions, including a description, compliance deadline and potential solutions required.

Legislation	Description	Effective/Due Date	Compliance Deadline	Impact (Solutions Required)
NIS2 <u>(EU Directive 2022/2555)</u>	Replaces and broadens NIS1's scope and obligations. The National Cybersecurity Bill will implement NIS2. Draft is not available at time of writing.	January 2023	October 2024 In Ireland, currently past pre-legislative scrutiny.	• Cybersecurity Consulting • Infrastructure Protection • Network Security Hardware • Identity Access Management • Data Protection • Cloud Security • Application Security • Security Hardware Support • Security automation • Awareness Training • Governance, Risk and Compliance
DORA <u>(EU Regulation 2022/2554)</u>	Harmonises rules regarding digital and operational resilience (including cybersecurity) in the financial sector across Member States.	January 2024	January 2025	• Cybersecurity Consulting • Managed Security Services Provider (MSSP) • Infrastructure Protection • Network Security Hardware • Identity Access Management • Data Protection • Cloud Security • Application Security • Security Hardware Support

				• Security automation • Awareness Training • Governance, Risk and Compliance
Cyber Resilience Act (EU Regulation 2024/2847)	Aims to set harmonised rules on the design, development, production and placing on the market of products with digital elements.	December 2024	December 2027	• Cybersecurity Consulting • Network Security Hardware • Identity Access Management • Data Protection • Application Security • Security Hardware Support • Security automation • Governance, Risk and Compliance
Cyber Solidarity Act (EU Regulation 2025/38)	Seeks to strengthen capabilities in the EU to detect and respond to significant and large-scale cyber-attacks and cybersecurity threats.	December 2024	February 2025	• Cybersecurity Consulting • Infrastructure Protection • Network Security Hardware • Identity Access Management • Cloud Security • Application Security • Security automation • Awareness Training • Governance, Risk and Compliance
Cybersecurity Act Amendment (EU Regulation 2019/881) and European Common Criteria-based cybersecurity certification scheme (EUCC) EU Regulation 2024/482	Gives the EU Agency for Network and Information Security a permanent mandate and establishes a European cybersecurity certification framework for ICT products,	February 2024	February 2025	• Cybersecurity Consulting • Risk assessment • Security by design • Vulnerability management • Secure code analysis

	services, and processes.			There will be increased focus on compliance tools, audit, maturity assessment, and cybersecurity risk assessment.
<u>AI Act</u> <u>(EU Regulation 2024/1689)</u>	Intended to promote human centric and trustworthy AI while ensuring a high level of safety and fundamental rights.	August 2024	August 2026	• Cybersecurity Consulting • Risk assessment • Security by design • Vulnerability management • Secure code analysis There will be increased focus on compliance tools, audit, maturity assessment, and cyber security risk assessment.



CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre



Rialtas na hÉireann
Government of Ireland



Co-funded by
the European Union