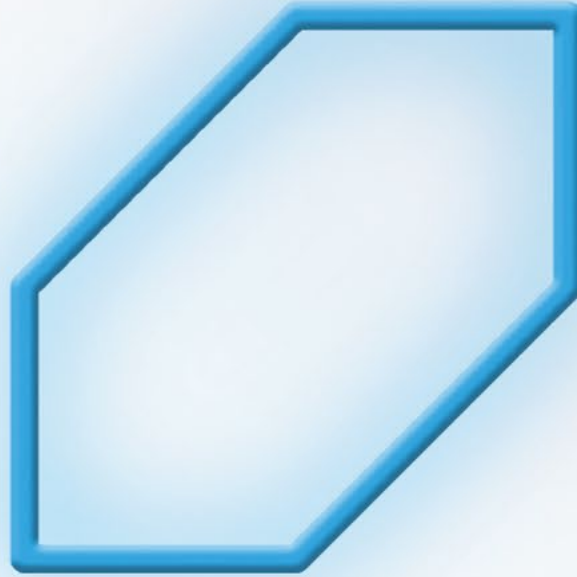




**CYBERSECURITY
LUXEMBOURG**



LUXEMBOURG
CYBERSECURITY
ECOSYSTEM

KEY INSIGHTS



NOVEMBER 2020



TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
INTRODUCTION	5
CYBERSECURITY IS A KEY PILLAR OF THE LUXEMBOURG STRATEGY FOR A SUSTAINABLE AND COMPETITIVE ECONOMY	5
MAPPING THE CYBERSECURITY ECOSYSTEM IN LUXEMBOURG	5
ADDRESSING THE NATIONAL AND EUROPEAN “TECHNOLOGICAL SOVEREIGNTY”	5
FOSTERING THE NATIONAL ECOSYSTEM AND PROMOTING IT INTERNATIONALLY	5
THE CYBERSECURITY ECOSYSTEM DASHBOARD	8
KEY INSIGHT 1: LUXEMBOURG, A FRONT-RUNNER COUNTRY IN CYBERSECURITY	12
KEY INSIGHT 2: A GOVERNANCE SYSTEM ADDRESSING CYBERSECURITY AS A NATIONAL SECURITY AND ECONOMIC ISSUE	14
KEY INSIGHT 3: A STEADILY GROWING ECOSYSTEM	16
KEY INSIGHT 4: A HIGH SHARE OF SMALL COMPANIES, A CHARACTERISTIC OF THE EUROPEAN CYBERSECURITY ECOSYSTEM	18
KEY INSIGHT 5: AN ALMOST EXHAUSTIVE SUPPLY OF CYBERSECURITY SOLUTIONS COVERING THE RISK MANAGEMENT SUPPLY CHAIN	20
SOURCES	22

MARKET INTELLIGENCE REPORT

Authors

Sara Bouchon, Head of Market Intelligence, Luxinnovation

Pascal Steichen, CEO, SECURITYMADEIN.LU

With the contribution of Francois Thill, Director of e-Commerce and Information Security, Ministry of the Economy

EXECUTIVE SUMMARY

Digitalisation is at the heart of the Luxembourg strategy for a sustainable and competitive economy. A strong national cybersecurity ecosystem is a key pillar for building a **trusted and secure environment**. Cybersecurity has indeed become a key factor of attractiveness of an economy. Together with SECURITYMADEIN.LU, Luxinnovation's Market Intelligence department is mapping the cybersecurity ecosystem in Luxembourg.

Technological sovereignty in terms of products, services and processes has become an essential geopolitical issue, addressing the importance of developing European and regional technological solutions to reduce our dependence on non-European tech providers. In this context, the cybersecurity mapping aims at better understanding what services and solutions are available in Luxembourg. Key insights on the **Luxembourg cybersecurity ecosystem** are listed below.



#1

Luxembourg is among the **front-runner countries in Europe** and in the world for its cybersecurity commitment. According to the *Global Security Index*, it ranks 11th globally and 7th in Europe.



#2

The national cybersecurity ecosystem relies on an active **collaboration between public and private stakeholders**. The key role of the **Ministry of the Economy** makes Luxembourg a unique case in Europe, where cybersecurity is seen not only as a defence issue but also as an economic issue.



#3

With 310 companies, the Luxembourg cybersecurity ecosystem is **steadily growing**: it has been growing for 20 years and has accelerated over the last 5 years (50% of companies are less than 5 years old). It is also attractive for start-ups (65% of the new players since 2019 are start-ups).



#4

While traditional IT companies provide almost half of the cybersecurity supply in Luxembourg, companies having cybersecurity as core business represent around ¼ of the ecosystem. The ecosystem is characterised by the important role played by companies originating from the **BFSI sector** (banking, financial services and insurance) that provide cybersecurity services to local customers. The role played by **small companies** (79% of core business companies), and the limited number of cybersecurity key market players is typical for the EU cybersecurity supply, where market opportunities for emerging EU solutions remain open.



#5

As one the **European cyber valleys**, Luxembourg is expected to play a key role in structuring the supply of European cybersecurity solutions in a still fragmented market dominated by non EU players. Solutions offered by the national ecosystem cover almost in an exhaustive manner the risk management supply chain with a **slight specialisation in risk identification and systems protection**.

INTRODUCTION

CYBERSECURITY IS A KEY PILLAR OF THE LUXEMBOURG STRATEGY FOR A SUSTAINABLE AND COMPETITIVE ECONOMY

Digitalisation is at the heart of the Luxembourg strategy for a sustainable and competitive economy. A strong national cybersecurity ecosystem is a key pillar of building a trusted and secure environment. The emergence of the Luxembourg cybersecurity ecosystem started about 20 years ago: the Grand Duchy of Luxembourg, under the lead of the Ministry of the Economy and following the OECD guidelines "Towards a culture of security," has considerably invested in cybersecurity and thus created a competitive, dynamic, and growing ecosystem.

Together with SECURITYMADEIN.LU, Luxinnovation's Market Intelligence department has produced [a mapping of the Luxembourg cybersecurity ecosystem](#). This report aims at analysing the main outputs of the mapping exercise.

MAPPING THE CYBERSECURITY ECOSYSTEM IN LUXEMBOURG

The final objective of the cybersecurity mapping is to provide an exhaustive view of the main public-private stakeholders of the ecosystem, with a strong focus on the solutions and services provided by national companies. Luxinnovation's Market Intelligence department has developed a mapping methodology (Table 1), combining an as-exhaustive-as-possible set of information on the ecosystem with the expertise of SECURITYMADEIN.LU to classify the cybersecurity supply. The use of the ECISO Cybersecurity Market Radar allows comparing the national ecosystem with other European ecosystems.

As a result, the mapping helps investors, service providers, IT integrators, financial investors and the general public to quickly obtain a picture of the available players and their products and services in the field of cybersecurity.

ADDRESSING THE NATIONAL AND EUROPEAN "TECHNOLOGICAL SOVEREIGNTY"

The mapping is a key element to promote the national cybersecurity solutions provided by Luxembourg companies, but it is also used at the European level (the mapping feeds the [EU cyber valleys project](#), which promotes the different cybersecurity ecosystems in Europe).

Technological sovereignty has become a strong geopolitical issue, addressing the importance of developing European and regional technological solutions to reduce our dependence on non-European tech providers. In this context, the cybersecurity mapping aims at better understanding what services and solutions are available in Luxembourg.

FOSTERING THE NATIONAL ECOSYSTEM AND PROMOTING IT INTERNATIONALLY

Under the high patronage of the Ministry of the Economy, the national ecosystem initiative, brand and platform CYBERSECURITY LUXEMBOURG was launched in 2019 to foster and enhance public-private cooperation in cybersecurity aligned with and integrated into the national cybersecurity strategy.

CYBERSECURITY LUXEMBOURG is led and driven by key national cybersecurity stakeholders: the High Commission for National Protection and SECURITYMADEIN.LU.

It is actively supported by the national innovation agency, Luxinnovation, which also promotes Luxembourg's expertise internationally.

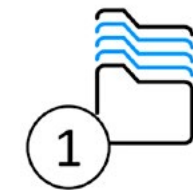
This national brand was created to foster, promote and give common visibility to the cybersecurity ecosystem. It will enable the endorsement by all stakeholders of the market to promote the Luxembourg expertise in cybersecurity at national as well as international level.

A dedicated online platform depicting all the relevant players will be developed in the near future. This web portal will become the central and neutral place for the ecosystem where relevant news, services and information about cybersecurity in Luxembourg can be found.

SCOPE AND METHODOLOGY OF THE CYBERSECURITY MAPPING

Cybersecurity is no longer defined as “just firewalls and off-the-shelf virus software”, but rather as “the collection of tools, technologies, processes and practices that can be used to protect networks, computers and data from unauthorised access or attack”.

While the **High Commission for National Protection** focused on mapping the public stakeholders involved in the cybersecurity ecosystem, SECURITYMADEIN.LU and Luxinnovation focused on the private stakeholders. To map the current **cybersecurity offering** in Luxembourg, Luxinnovation's Market Intelligence department proposed a three-step methodology.



1
Build a database of the LU cybersecurity ecosystem members (LXI-Market Intelligence)



2
Expert's review and classification of companies using the ECSO cybersecurity market radar (SECURITYMADEIN.LU)



3
Analysis of the ecosystem (LXI-Market Intelligence & SECURITYMADEIN.LU)

1. The **database** of companies providing cybersecurity services or solutions aims at being as **exhaustive** as possible, combining different sources. Specific attention was dedicated to identifying companies not having cybersecurity as core business but still delivering relevant cybersecurity solutions or services..
2. Tools and solutions provided by Luxembourg companies were classified using the [ECSO Cybersecurity Market Radar](#), following the five main steps of the risk management cycle: Identify, Protect, Detect, Respond and Recover.
3. The results of the mapping are presented in the Luxembourgish [Cybersecurity Ecosystem Dashboard](#), expected to be regularly updated to monitor the evolution of the ecosystem.

Table 1- Methodology to map the cybersecurity ecosystem in Luxembourg

THE CYBERSECURITY ECOSYSTEM DASHBOARD



LUXEMBOURG CYBERSECURITY ECOSYSTEM



80 COMPANIES WITH CYBERSECURITY AS A CORE BUSINESS

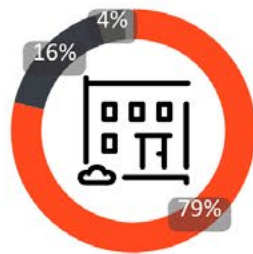
EMPLOYMENT



957

employees in total*

SIZE

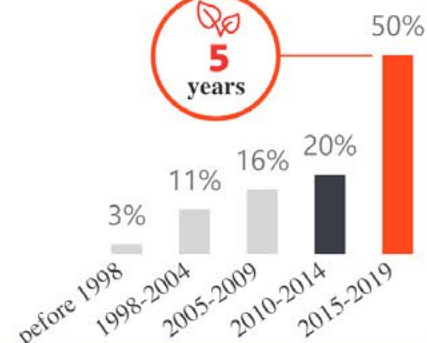


1-10 employees

AGE



5 years



50% of companies have been created during the past 5 years

The emergence of the Luxembourg cybersecurity ecosystem started around 20 years ago

(*) Estimated by Luxinnovation based on last available figures in Editusdata and LBR

75 STARTUPS



STARTUPS REPRESENT 24% OF THE NATIONAL CYBERSECURITY ECOSYSTEM

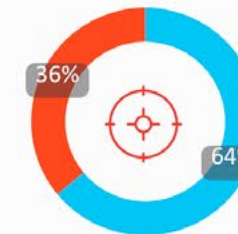
EMPLOYMENT



356

employees in total*

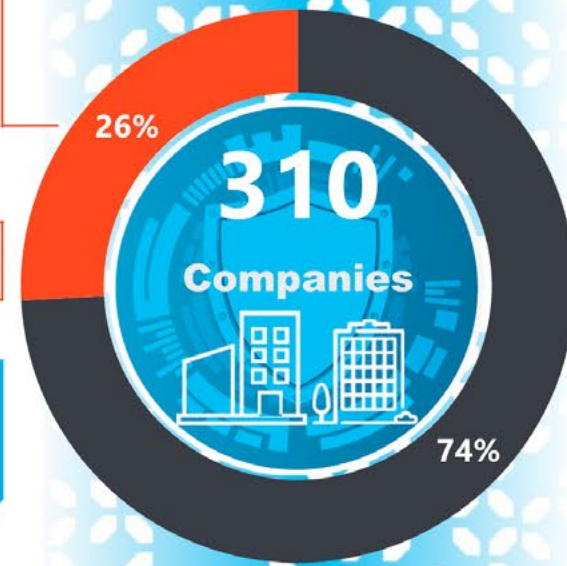
CORE BUSINESS



One third of startups have cybersecurity as a core business

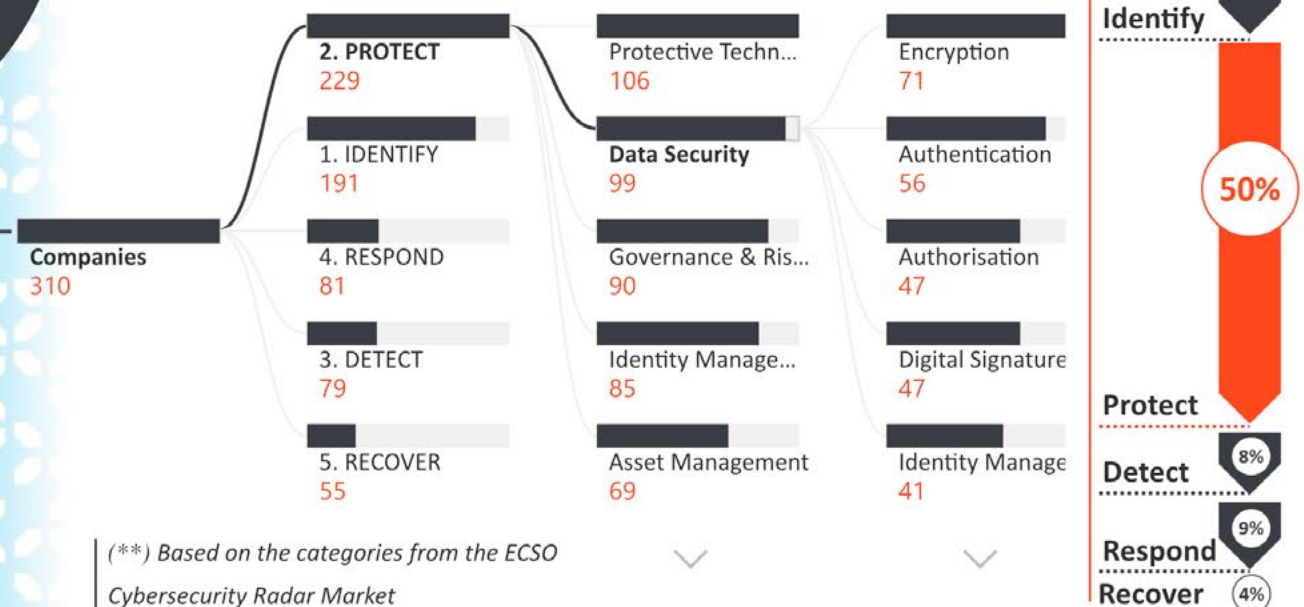
TOP 5 SOLUTIONS OFFERED

Data Security	Govern...	Pro...
39	24	15
Identity Management & ...	Asset Managem...	
32		



DIVERSIFIED SOLUTIONS**

Value chain | Solution | Service Group



(**) Based on the categories from the ECISO Cybersecurity Radar Market

Welcome to the interactive dashboard of the Luxembourg Cybersecurity Ecosystem. It presents a complete overview of all relevant cybersecurity key figures in the Grand-Duchy.

METHODOLOGY

- Data was gathered from different sources by the Market Intelligence service of Luxinnovation
- Each company was then reviewed and classified by SECURITYMADEIN.LU based on the ECISO Cybersecurity Market Radar.

NAVIGATION

- Click on any part of a visual to see other visuals updated based on the filter.
- By clicking on this icon (on the top middle of the dashboard), all the filters applied will be reset.

KEY INSIGHTS



01

LUXEMBOURG, A
FRONT-RUNNER
COUNTRY IN
CYBERSECURITY



02

A GOVERNANCE
SYSTEM ADDRESSING
CYBERSECURITY AS A
NATIONAL SECURITY
AND ECONOMIC ISSUE



03

A STEADILY GROWING
ECOSYSTEM



04

A HIGH SHARE OF
SMALL COMPANIES,
A CHARACTERISTIC
OF THE EUROPEAN
CYBERSECURITY
ECOSYSTEM



05

AN ALMOST
EXHAUSTIVE SUPPLY
OF CYBERSECURITY
SOLUTIONS COVERING
THE RISK MANAGEMENT
SUPPLY CHAIN

KEY INSIGHT 01

LUXEMBOURG, A FRONT-RUNNER COUNTRY IN CYBERSECURITY



Luxembourg is among the front-runner countries in Europe and in the world for its cybersecurity commitment. According to the *Global Security Index* ranks 11th globally and 7th in Europe.

Luxembourg appears among the **top 15 countries in the world highly committed to cybersecurity**, according to the *Global Cybersecurity Index (GCI)*¹.

- Luxembourg ranks 11th globally in the GCI, which benchmarks, monitors and compares the level of cybersecurity commitment of 194 countries ([Global Cybersecurity Index](#), 2018).
- GCI also highlights best practices from Luxembourg in the technical and capacity-building fields.
- Luxembourg ranks 2nd worldwide and 1st among EU Member States in [Cisco's 2019 Digital Readiness Index](#).

The front-runner position of Luxembourg is not new. After a first cyber security master plan at the level of the Ministry of the Economy in 2003 and the initiation of projects in key cybersecurity areas: awareness raising and electronic signature, Luxembourg was **one of the first EU countries to issue a National Cybersecurity Strategy** in 2011 (table 2).

- National cybersecurity strategies emerged in Europe mainly after the 2007 Estonian cyber-attacks, which brutally raised European awareness on cybercrime. In Luxembourg, the 2011 National Security Strategy was updated two times in 2015 and 2018 and a new update is currently prepared.
- In line with the "Digital Lëtzebuerg" initiative, the third national cybersecurity strategy (2018-2020) aims at 1) strengthening public confidence in the digital environment 2) enhancing the security of information systems, improving the ability to identify cyber-attacks, protecting critical digital infrastructure and 3) raising stakeholders' awareness on security and resilience.
- Whereas the legitimacy of the European Union to address security and defence issues is sometimes questioned, Luxembourg demonstrates its commitment to building the EU's abilities to forge common cyber security policies. Luxembourg is for instance the only country in Europe with organisations participating to three of the four Horizon 2020 pilots projects aiming at establishing a network of European cybersecurity competence (Concordia, Sparta and CyberSec4Europe).

As a result, Luxembourg currently appears as one of **the safest countries** in Europe.

- Luxembourg ranks 8th among the most cyber secure countries in Europe in 2019 (Figure 1) ([Statista, Specops Software, 2020](#)).

Publication of first national cybersecurity strategy	Country publishing a national cybersecurity strategy
2005	Germany
2006	Sweden,
2008	Estonia, Finland, Slovakia
2011	France, Luxembourg issues "Stratégie nationale en matière de cyber sécurité" updated two times since then (in 2015 and 2018).
2013	Poland, Italy, Hungary
	EU: <i>Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace</i>
2016	Directive on security network and Information systems (NIS Directive).
2018	EU General data Protection Regulation (GDPR)

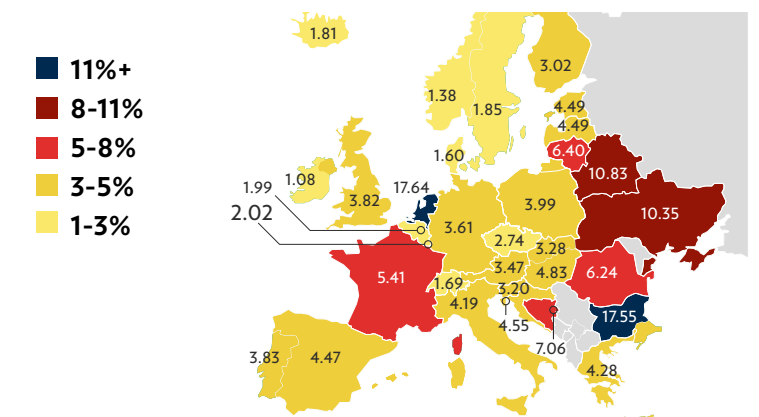
Table 2 - Luxembourg is among the first EU countries to issue a national cybersecurity strategy (after Giantas, Liaropoulos, 2019).

Europe region			
Member State	Score	Regional Rank	Global Rank
United Kingdom	0.931	1	1
France	0.918	2	3
Lithuania	0.908	3	4
Estonia	0.905	4	5
Spain	0.896	5	7
Norway	0.892	6	9
Luxembourg	0.886	7	11
Netherlands	0.885	8	12
Georgia	0.857	9	18
Finland	0.856	10	19
Turkey	0.853	11	20
Denmark	0.852	12	21
Germany	0.849	13	22
Croatia	0.840	14	24
Italy	0.837	15	25
Austria*	0.826	16	28
Poland	0.815	17	29
Belgium	0.814	18	30
Hungary	0.812	19	31
Sweden*	0.810	20	32
The Republic of North Macedonia	0.800	21	34
Switzerland	0.788	22	37
Ireland	0.784	23	38

Table 3 - Final ranking GCI 2018 for the Europe region ([Global Cybersecurity Index, 2018](#))

CYBERCRIME: EUROPE'S MOST & LEAST SECURE COUNTRIES

Percentage of machines that experienced cyberattacks (Jan-Oct 2019)*



* Cloud provider-related incoming attacks and cryptocurrency mining, malware and ransomware encounters.

Figure 1 - Cybercrime-Europe's most & Least secure countries ([Statista, Specops Software, 2020](#))

¹ The *Global Cybersecurity Index (GCI)* is a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cybersecurity commitment of countries with regard to the five pillars of the Global Cybersecurity Agenda (GCA), i.e. legal, technical, organizational, capacity building, cooperation.

KEY INSIGHT 02

A GOVERNANCE SYSTEM ADDRESSING CYBERSECURITY AS A NATIONAL SECURITY AND ECONOMIC ISSUE



The national cybersecurity ecosystem relies on an active collaboration between public and private stakeholders. The key role of the Ministry of the Economy makes Luxembourg a unique case in Europe, where cybersecurity is seen not only as a defence issue but also as an economic issue.

The **Inter-ministerial coordination committee for cyber prevention and cybersecurity** (2017), chaired by the High Commission for National Protection (HPCN), has the mission to ensure a national coordination on cybersecurity matters (Figure 2).

Le **Centre des Technologies de l'Information de l'Etat (CTIE)**, the National Information System Security Agency (ANSSI) and GOVCERT.lu address cybersecurity issues for the **public sector** and operators of critical infrastructures.

- CTIE is the central player in the setting up and development of eGovernment, guaranteeing a high level of security.
- ANSSI is the national agency with responsibility for the security of both classified and non-classified information systems used by the State.
- The main missions of the CERT Gouvernemental are to constitute a single point of contact dedicated to handling large-scale security incidents affecting State administrations and departments ([Infocrise.lu](http://infocrise.lu))

SECURITYMADEIN.LU (including C3, CIRCL and CASES), the cybersecurity agency for the Luxembourg economy, focuses on supporting the **private sector**. This focus laid on cybersecurity as an **economic issue makes Luxembourg stand out in Europe**.

- CASES.LU - Cyberworld Awareness and Security Enhancement Services devotes itself to develop tools and services for the management and prevention of risks for public and private entities in Luxembourg.
- CIRCL.LU - Computer Incident Response Centre Luxembourg is an initiative designed to provide a systematic and fast response to IT security threats and incidents. CIRCL is the CERT specifically dedicated to the private sector, municipalities and non-governmental entities in Luxembourg.
- C3.LU - the Cybersecurity Competence Centre, in close cooperation with private sector partners aim at empowering businesses to better protect themselves through its threats and Vulnerabilities Observatory, its testing facility, as well as its training and simulation platform.

Other key players of the ecosystem include **academic and research institutions** working in cybersecurity as well as current **public-private partnerships (PPP)**.

- The [Luxembourg Institute for Science and Technology](#), the [Interdisciplinary Centre for Security, Reliability and Trust](#), [University of Luxembourg](#) and the [Luxembourg Centre for Systems Biomedicine](#) have developed expertise in cybersecurity;
- A good example of a PPP is [INFRACHAIN](#), a non-profit organisation created by the emerging blockchain-related industry and supported by the Luxembourg government. It aims at bridging the gap between blockchain technologies and the regulatory and legal requirements.

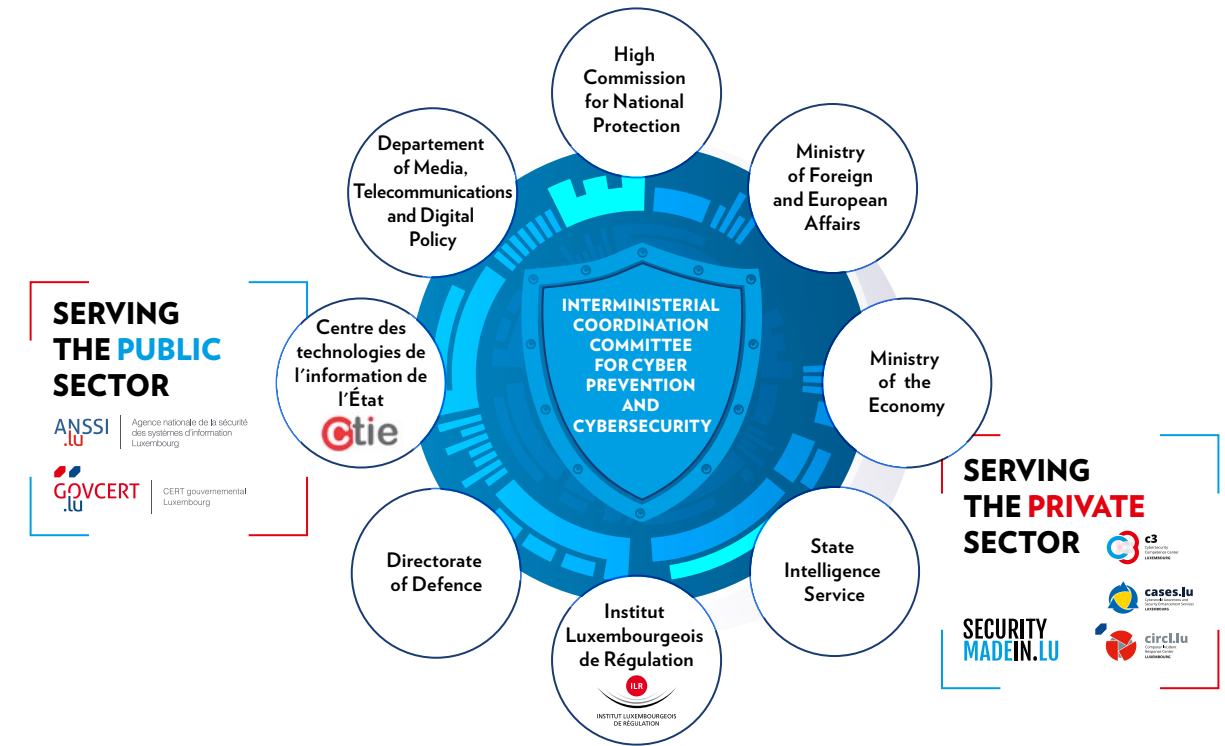


Figure 2-Main stakeholders in the Luxembourg cybersecurity ecosystem



Figure 3-National legal framework for cybersecurity and main authorities and regulators

KEY INSIGHT 03

A STEADILY GROWING ECOSYSTEM



With 310 companies, the Luxembourg cybersecurity ecosystem is a steadily growing ecosystem: it has been growing for 20 years and has accelerated over the last 5 years (50% of companies are less than 5 years old). It is also attractive for start-ups (65% of the new players since 2019 are start-ups).

In 2020, **310 companies are active in cybersecurity** in Luxembourg, compared to 304 companies in 2019, confirming the continuous growth of the number of cybersecurity companies in the national ecosystem (Figure 4 and 5).

- As shown in Figure 5, the emergence of the Luxembourg cybersecurity ecosystem started around 20 years ago².
- Almost half of current companies that have cybersecurity as core business were created over the past 5 years.

The growth of the national ecosystem results from the **importance taken worldwide by cybersecurity** as well as the **increasing number of cybercrimes** (Figure 6).

- Between 2004 and 2017, the cybersecurity market grew by roughly 35 times ([Cybersecurity Ventures, 2019](#)),
- Between 2014 and 2015, the number of cybersecurity companies worldwide increased by 23% ([PwC, LSEC, 2018](#))
- In Luxembourg, the growth of the ecosystem also results from the 2011 national strategy, as well as the first European Cybersecurity Strategy published in 2013. .

The growth of the ecosystem has been strongly supported by **start-ups**³.

- They represent 24% share of the number of companies (75 companies altogether) and 36% of them have cybersecurity as a core business.
- More than half of these start-ups (55%) are or have been hosted in a Luxembourg incubator.
- The role of start-ups is essential for the growth of the core business ecosystem as they specialise in the technologies expected to be key in cybersecurity in the next 5 years. Identity & Access management technologies, Governance & compliance and Encryption represent 54 % of the solutions provided by Luxembourg start-ups (Figure 7).

² For companies having cybersecurity as core business, still being in activity in 2020

³ A start-up is defined here as a company: 1) being less than 5 years old; 2) employing < 100 employees worldwide; 3) having an innovative product, service or business model.

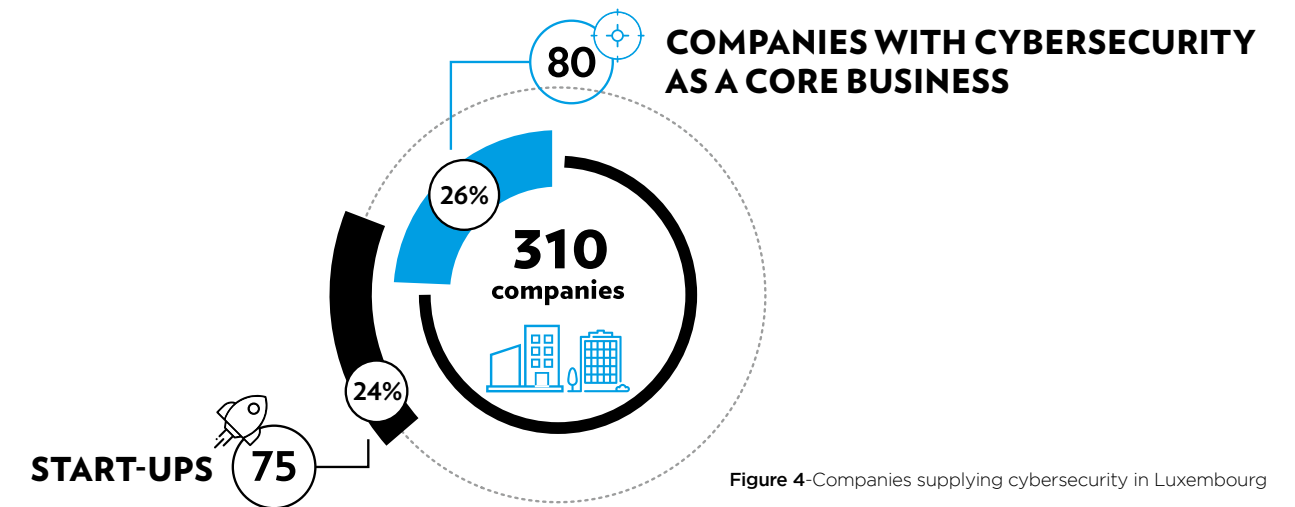


Figure 4-Companies supplying cybersecurity in Luxembourg

CREATION DATE OF CURRENT COMPANIES HAVING CYBERSECURITY AS A CORE BUSINESS

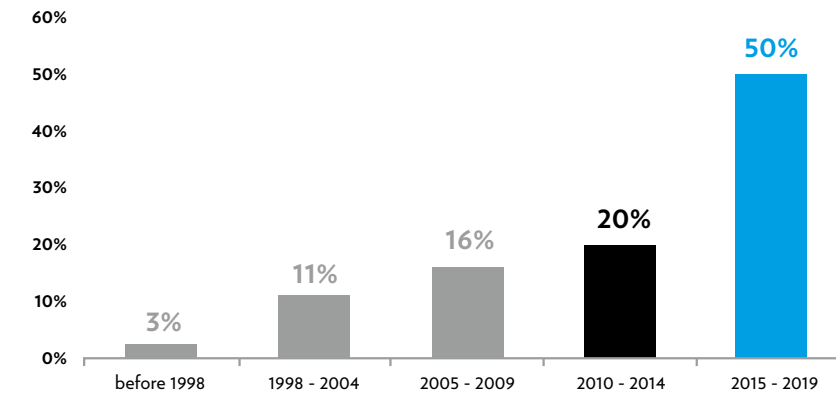


Figure 5-Creation date of current companies having cybersecurity as a core business

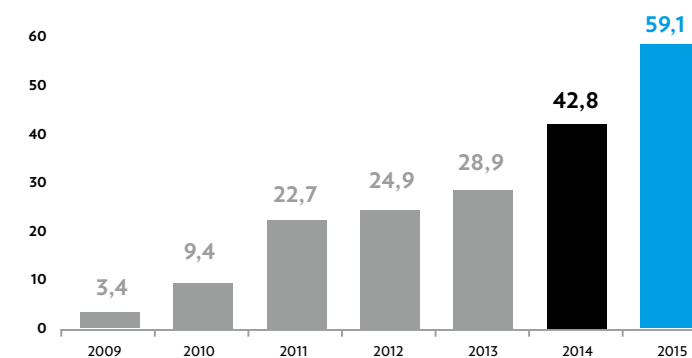


Figure 6-Number of annual cyber attacks worldwide in millions ([Statista, 2017](#))

TOP 3 SOLUTIONS PROVIDED BY START-UPS

- 1 Identity & access management
- 2 Governance, risk & compliance
- 3 Encryption

Figure 7-Top 3 solutions provided by national start-ups

KEY INSIGHT 04

A HIGH SHARE OF SMALL COMPANIES, A CHARACTERISTIC OF THE EUROPEAN CYBERSECURITY ECOSYSTEM



Traditional IT companies provide almost half of the cybersecurity supply in Luxembourg, while companies having cybersecurity as core business represent around ¼ of the ecosystem, slightly below the EU average (34%). The ecosystem is characterised by the important role played by companies originating from the banking, financial services and insurance (BFSI) sector that provide cybersecurity to local customers. The role played by small companies (79% of core business companies), and the limited number of cybersecurity key market players is typical of the EU cybersecurity supply, where market opportunities for emerging EU solutions remain open.

EU cybersecurity products and services are mostly supplied by companies that originate from cybersecurity, ICT, security, defence, insurance and academic sectors (PwC, LSEC, 2018).

- While the share of **core business cybersecurity companies** is around 34% in Europe, Luxembourg shows a slightly lower share, with around ¼ of the ecosystem having cybersecurity as core business.
- Non-core business companies providing cybersecurity products originate mainly from the traditional IT sector (47%), where historically cybersecurity activities have primarily emerged.
- Compared to the rest of Europe, the Luxembourg ecosystem is characterised by the importance of the cybersecurity services provided by companies from the BSFI (16%), thus reflecting an important characteristic of the national economy.

In total, the core business ecosystem represents almost 1000 employees⁴, with an average of **12 employees per core business company**.

- Small enterprises are at the heart of the cybersecurity ecosystem, as 79% of the core business companies have less than 10 employees. The importance of small size businesses reflects the important share of cybersecurity services within the Luxembourg cybersecurity supply, best delivered by local companies, and where the proximity to the customer is key.
- This is in line with the EU average, where approximately 74% of the cybersecurity companies are micro and small sized enterprises.
- Only 14% of EU based cybersecurity companies are part of the global top 500 market leading cybersecurity highest growth companies (PwC, LSEC, 2018). Atos one of the major players in cybersecurity in Europe is present and very active in the Luxembourg ecosystem. Further, the main pure player in Luxembourg: Excellium Services is part of the SONAE IM group, one of the major pure players in cybersecurity in Europe (Sonae IM, 2019).

As the cybersecurity market is expected to grow, main assumptions might be that new businesses will enter the market, while current small enterprises become medium-sized enterprises, with a strong focus on the proximity with local customers.

⁴ 957 employees is the exact number estimated by LXI, based on most recently available figures from Editusdata and the Luxembourg Business Register

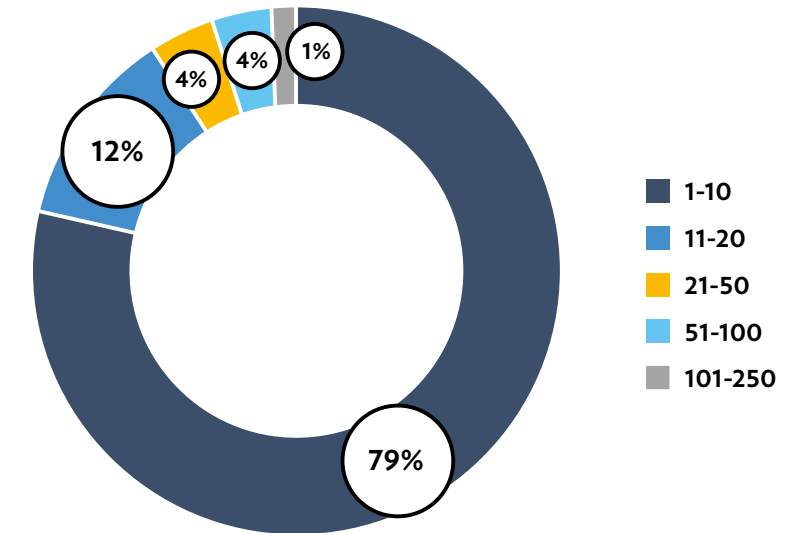


Figure 8-Size of companies having cybersecurity as core business (Luxembourg)

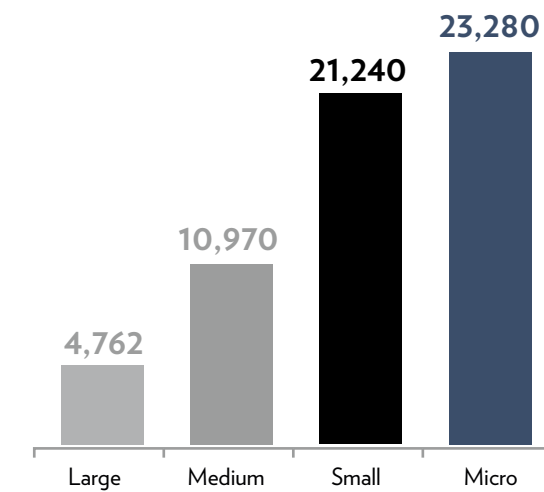


Figure 9-EU Company size ranges: large (8%), medium (18%), small (39%), micro (39%) (PwC, LSEC, 2018)

	Americas	Europe	Israël	Asia	Oceania	Africa
Global company Headquarters (Top 500)	374	69	34	20	2	1
Proportion	74,80%	13,8%	6,8%	4,0%	0,4%	0,2%

Figure 10-Global locations (corporate headquarters) of top 500 cybersecurity providers (PwC, LSEC, 2018)

KEY INSIGHT 05

AN ALMOST EXHAUSTIVE SUPPLY OF CYBERSECURITY SOLUTIONS COVERING THE RISK MANAGEMENT SUPPLY CHAIN



Identified as one of the European cyber valleys, Luxembourg is expected to play a key role in structuring the cybersecurity supply of European solutions in a still fragmented market dominated by non-EU players. Solutions offered by the national ecosystem cover almost in an exhaustive manner the risk management supply chain, with a slight specialisation in risk identification and systems protection.

Solutions provided by companies in the national ecosystem cover almost in an exhaustive manner the **cyber risk management value chain** with a focus on risk identification and systems protection.

- 58 out of the 60 ECSO categories are offered by providers in Luxembourg (Figure 11)
- When comparing the national ecosystem to other cyber valleys in Europe, Luxembourg is very similar to the Bretagne region, one of the lead regions in cybersecurity in Europe (Figure 12).

Top 7 solutions represent **61% of the national market** (Figure 13).

- The importance of governance, risk & compliance and identity & governance solutions can be explained by the high number of companies targeting the finance and banking sectors.
- The implementation of the GDPR directive boosted data security services within the ecosystem.
- On average, Luxembourg companies (core and non-core business) provide 5 cybersecurity solutions.

Identified as one of the **European cyber valley**, Luxembourg has a key role to play to facilitate the development of the EU cybersecurity value chain.

- According to ECSO, Europe is both a beehive of cyber security activities and a greenfield of opportunities for traditional and emerging providers. With a domestic market valued at EUR 25 billion and a very diverse industry landscape, the European offering is not yet consolidated. This is mainly due to a strong fragmentation across the different market segments, a difficult access to the market for young companies specialised in cyber security and a lack of a critical amount of private investments (ECSO, 2019).
- The EU remains a global net importer of cyber security products and solutions and largely depends on non-European providers. This raises the issue of Europe's "technological sovereignty" and opens the way for the development of EU-based cybersecurity solution on the market.
- According to ECSO, "the EU should play as a geographic constellation of 'cyber valleys'. In this scenario, each regional ecosystem contributes to a common programme and facilitates a quick access of local cyber security SMEs to the European market. This would impede a still-missing critical mass of growth companies to stay at the leading edge and build high-growth European companies globally competitive. Finally, this would be the best to attract much more private investors" (ECSO, 2019).

DIVERSIFIED SOLUTIONS

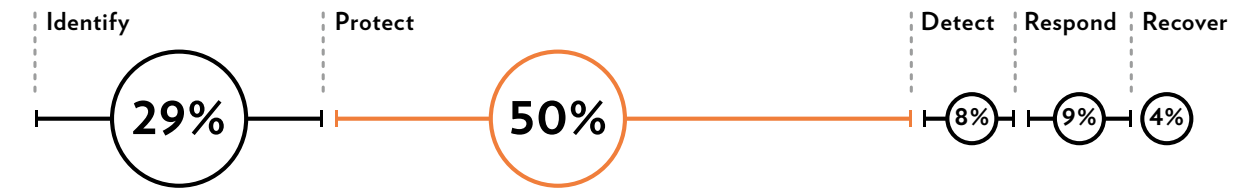


Figure 11- The Luxembourg cybersecurity supply provides solutions all along the risk management value chain with a specialisation in identification and protection

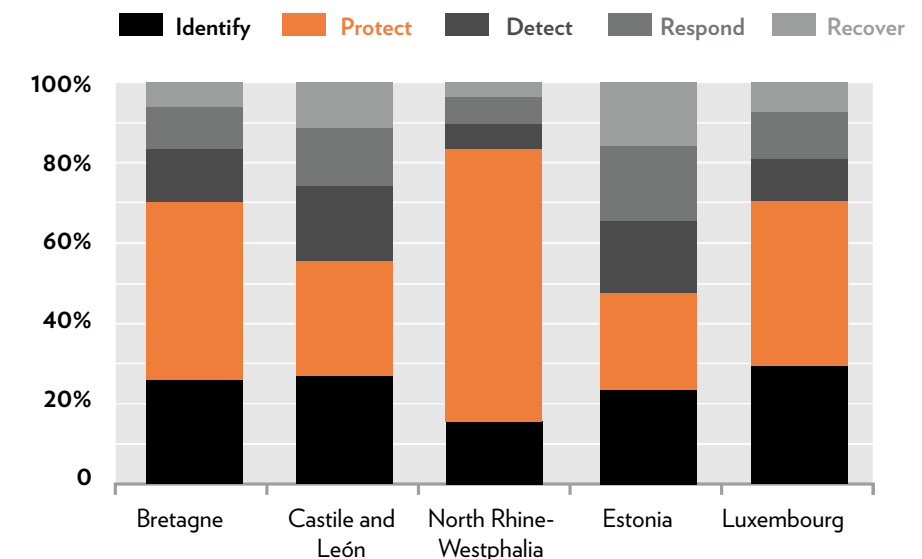


Figure 12-Luxembourg cybersecurity supply compared to European cyber valleys (European Cyber valleys, 2020)

TOP 7 SOLUTIONS

COVER 61% OF THE NATIONAL MARKET*

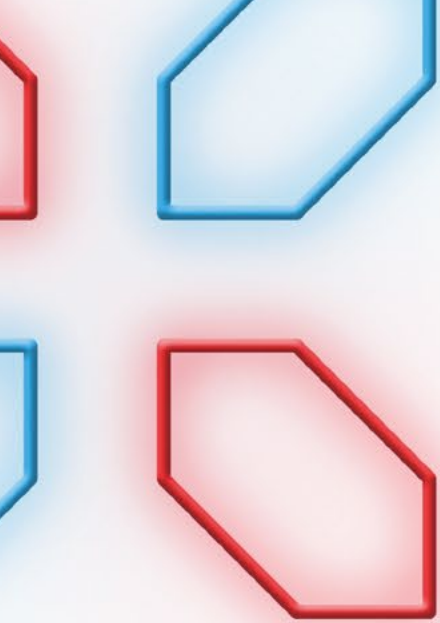


* Based on the ECSO Cybersecurity Market Radar

Figure 13-Top 7 solutions offered in Luxembourg cover 61% of the cybersecurity market

SOURCES

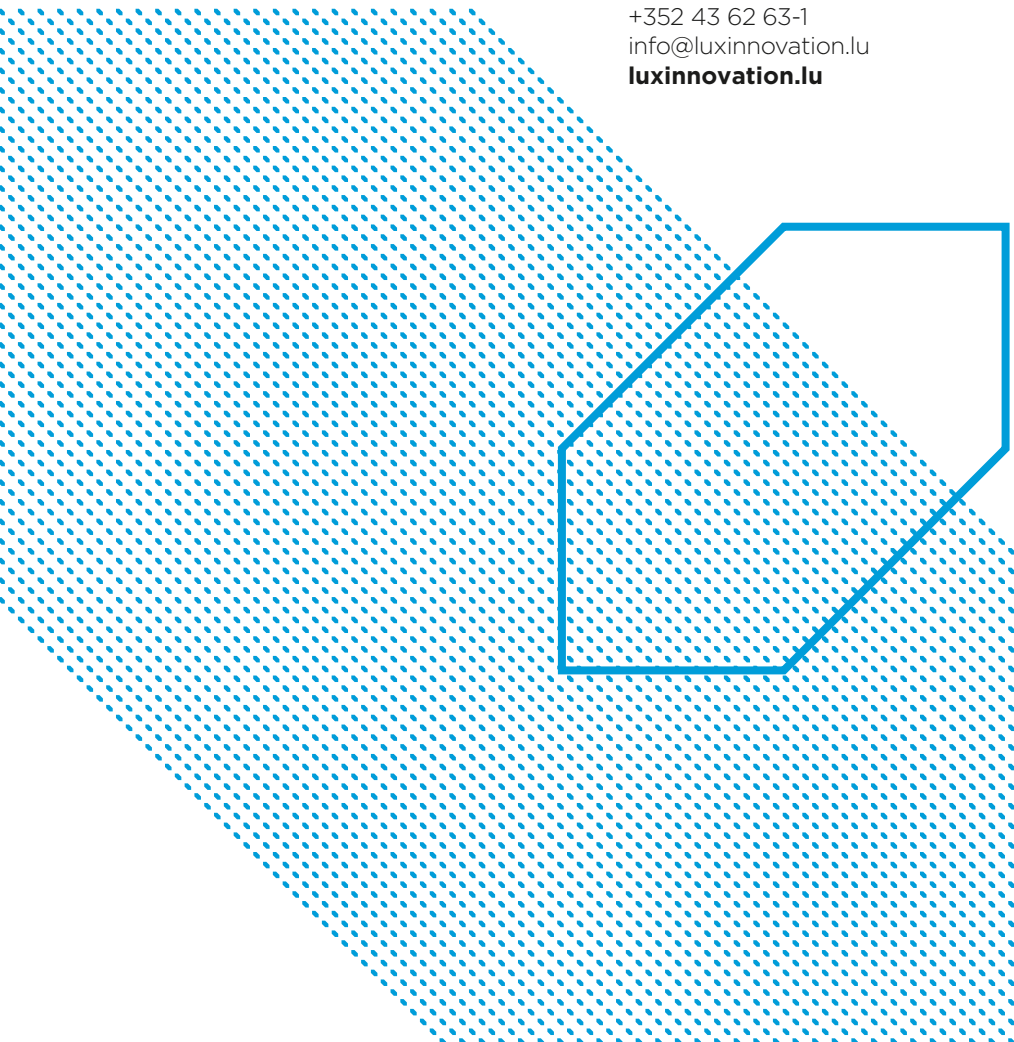
- [1] Cybersecurity - Smart Specialisation Platform.
Retrieved from <https://s3platform.jrc.ec.europa.eu/cybersecurity>
- [2] ECSO - European Cyber Security Organisation.
Retrieved from <https://ecs-org.eu/>
- [3] Global Cybersecurity Index.
Retrieved from <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- [4] Digital readiness Index 2019.
Retrieved from https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/
- [5] (PDF) Cybersecurity in the EU: Threats, frameworks and future perspectives.
Retrieved from https://www.researchgate.net/publication/335909463_Cybersecurity_in_the_EU_Threats_frameworks_and_future_perspectives
- [6] The European Countries Most at Risk of Cyber-Crime | Specops Software.
Retrieved from <https://specopssoft.com/blog/european-countries-cyber-crime/>
- [7] Infocrise.
Retrieved from <https://www.infocrise.lu/en>
- [8] Luxembourg Institute of Science and Technology.
Retrieved from <https://www.list.lu/>
- [9] Interdisciplinary Centre for Security, Reliability and Trust.
Retrieved from <https://www.wen.uni.lu/snt>
- [10] LCSB - Luxembourg Centre for Systems Biomedicine.
Retrieved from <https://www.wen.uni.lu/lcsb>
- [11] Infrachain.
Retrieved from <https://infrachain.com/>
- [12] Cybersecurity Market Analysis |CIMA2019.
Retrieved from https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Ciberseguridad_Market_Analysis_CIMA_2019.pdf
- [13] ECSO Technical paper.
Retrieved from https://s3platform.jrc.ec.europa.eu/documents/20182/386128/ECSO_Position_Paper_Role_of_Regions_in_EU%27s_cyber_security.pdf/63cfb8c5-3241-4777-a4ea-f9abc880bad2
- [14] European Cybersecurity Directory & Maps.
Retrieved from http://tools.bdi.fr/annu_craft/cybersecurity.html?dashboard=1
- [15] Phishing, Ransomware and Co. - An increasing threat | oneclick™.
Retrieved from <https://oneclick-cloud.com/en/blog/trends-en/increasing-threat-of-cyber-crime/>
- [16] Chart: Cybercrime: Europe's Most & Least Secure Countries | Statista.
Retrieved from <https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/>
- [17] Sonae IM. Retrieved from <https://sonaeim.com/news/2019/01/leading-european-cybersecurity-group-results-from-joining-s2lsec-and-excellium-through-a-new-sonae-im-investment-in-benelux>



LUXINNOVATION
TRUSTED PARTNER FOR BUSINESS

5, avenue des Hauts Fourneaux
L-4362 Esch-sur-Alzette
Luxembourg

+352 43 62 63-1
info@luxinnovation.lu
luxinnovation.lu



**SECURITY
MADEIN.LU**

16, boulevard d'Avranches
L-1160 Luxembourg
Luxembourg

+352 274 00 98 601
info@securitymadein.lu
securitymadein.lu



**CYBERSECURITY
LUXEMBOURG**