European Investment Advisory Hub

Europe's gateway to investment support

CONTRIBUTION OF INVESTMENT PROJECTS TO THE EUROPEAN SECURITY INITIATIVE – CYBERSECURITY

15/04/2021

FINAL REPORT

European Investment Bank The EU bank

European Commission

Disclaimer:

This Report should not be referred to as representing the views of the European Investment Bank (EIB), of the European Commission (EC) or of other European Union (EU) institutions and bodies. Any views expressed herein, including interpretation(s) of regulations, reflect the current views of the author(s), which do not necessarily correspond to the views of the EIB, of the EC or of other EU institutions and bodies. Views expressed herein may differ from views set out in other documents, including similar research papers, published by the EIB, by the EC or by other EU institutions and bodies. Contents of this Report, including views expressed, are current at the date of publication set out above, and may change without notice. No representation or warranty, express or implied, is or will be made and no liability or responsibility is or will be accepted by the EIB, by the EC or by other EU institutions and bodies in respect of the accuracy or completeness of the information contained herein and any such liability is expressly disclaimed. Nothing in this Report constitutes investment, legal, or tax advice, nor shall be relied upon as such advice. Specific professional advice should always be sought separately before taking any action based on this Report. Reproduction, publication, and reprint are subject to prior written authorisation from the authors.

CONTENTS

FIGURES

TABLES

Final Report

CONTRIBUTION OF INVESTMENT PROJECTS TO THE EUROPEAN SECURITY INITIATIVE – CYBERSECURITY

1. KEY DATA

Framework Contract	Framework agreement to support EIB advisory services (EIBAS) activities inside and outside EU-28 Lot 4: Smart Growth, Social Infrastructure and Horizon 2020 AA-001250-001-D
Specific Contract Number:	CC11814
Name of Project:	Contribution of Investment Projects to the European Security Initiative – Cyber Security
Contractor:	NTU International Danish Energy Management A/S (DEM) (Lead Implementing Partner)
Contracting Authority:	European Investment Bank
Start/End Date:	January 2020 – November 2020
Task Managers:	Pierre-Alain FRANÇOIS Özhan YILMAZ Eleni GIOTI
Working Group Members:	Christian ZELLNER Pieter COPPENS Frédéric PERRIN Marianna MAVROMATI Marcin GOLEC

2. QUALITY ASSURANCE STATEMENT

Version: Final Report		
Prepared by:	**Name**	**Position**
	Rimtautas Černiauskas	KE 1: Team Leader
	Sigitas Rokas	KE 2: Cybersecurity Consultant
	Akvilė Giniotienė	NKE: EU Cybersecurity Policy Expert
	Prashanth Pattabiraman	NKE: Cybersecurity Consultant
Checked by:	Ingrid Leth-Møller	Project Manager – DEM
	Jørn Lykou	CEO – DEM
	Ana Anton	Project Manager – NTU

3. EXECUTIVE SUMMARY

This report marks the completion of work for the development of a consistent approach to identify the cybersecurity related investment within the EIB financed projects that contribute to the European Security Initiative (ESI) and validation of the estimated cybersecurity investments through targeted engagements with select project promoters. The report was prepared by Danish Energy Management A/S (DEM) (Lead Implementing Partner) experts designated for the Project "Contribution of Investment Projects to the European Security Initiative – Cyber Security".

Cybersecurity is a very sensitive topic and therefore information is sparely available publicly. Organisations are also very reluctant to share transparent information pertaining to their cybersecurity position, particularly with regards to their vulnerabilities, solutions deployed, budget, staffing, etc., with the fear that it may expose their gaps or weaknesses. Given this lack of data and information, the consultants have developed a comprehensive model based on a statistical approach that enables the identification of cybersecurity related investments using several multipliers that attempt to estimate the investment based on the limited data that is available. Reliable and credible data sources were analysed and used in the development of the statistical approach and to calibrate the values used for the different multipliers. Additionally, the proposed methodology also considers the country and economic sector dimension when estimating the cybersecurity investments. Furthermore, it allows for the estimation of the cybersecurity related investment within projects with only basic information such as overall investment value, specific investments towards ICT infrastructure and the criticality of the sector.

The consultants have developed an Identification of Cybersecurity Related Investment methodology (ICRI), which can be used to estimate the cybersecurity investment values from overall level of ICT investments in a semi-automated and traceable way, using a series of steps enumerated in an excel document. The ICRI was practically applied during the engagement with project promoters on selected EIB financed projects to estimate the cybersecurity investment. These estimates were

further compared with reported cybersecurity spending, both to validate the methodology and to discuss the Consultants' observations and opinion.

4. EU CYBERSECURITY POLICY LANDSCAPE

The EU's approach to cyber-related issues has evolved from addressing policy-specific challenges – such as high-tech crime or security of networks and information systems – towards a more comprehensive and dynamic concept of cyber resilience. That means moving away from crisis containment to a more structural and long-term approach to vulnerabilities, with an emphasis on anticipation, prevention and preparedness. The Communication on the EU Strategic Approach to Resilience [EUSTAR] defines resilience as 'the ability of an individual, a household, a community, a country or a region to withstand, adapt and quickly recover from stress and shocks'.

The EU Cyber Security Strategy [EUCSS] adopted defined five key pillars of the EU's cybersecurity policy:

- Increasing cyber resilience;
- Reducing cybercrime;
- Developing EU cyber defence policy and capabilities related to Common Security and Defence Policy (CSDP);
- Developing the industrial and technical resources for cybersecurity; and
- Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

The adoption of the Digital Single Market Strategy for Europe [DSMSE] in 2015 created a broad framework for enhancing the EU's position as a world leader in the digital economy. It seeks to strengthen the EU's role in digital technologies, including through reinforcing trust and security aspects of digital goods and services.

The Directive on Security of Networks and Information Systems [DSNIS] (NIS Directive), adopted in 2016, is the first comprehensive, EU-wide cybersecurity legislation. It sets benchmarks for what constitutes a desirable level of institutional, policy and regulatory capacity to minimise the impact of cyber threats and lays down measures with a view of achieving a high common level of security of network and information systems within the Union. The NIS directive defines specific sectors and subsectors which provide services that are essential for the maintenance of critical and societal and economic activities and which require a higher level of protection

from cyber-threats and harmonised approach to cybersecurity across the EU. These sectors and sub-sectors include:

1. **Energy**:
   - Electricity (supply, distribution, transmission);
   - Oil (transmission, production, refining and treatment, storage and transmission); and
   - Gas (supply, distribution systems, transmission systems, storage systems, liquefied natural gas (LNG) systems, natural gas, natural gas refining and treatment.
2. **Transport**:
   - Air transport (air carriers, airport managing bodies, airports, entities operating ancillary installations contained within airports;
   - Rail transport (infrastructure managers, railway undertakings);
   - Water transport (inland, sea and coastal passenger and freight water transport companies, port managing bodies, entities operating works and equipment contained within ports, operators of vessel traffic services); and
   - Road transport (road authorities responsible for traffic management control, operators of Intelligent Transport Systems).
3. **Banking** – credit institutions.
4. **Financial market infrastructures** – operators of trading venues and central counterparties.
5. **Health**:
   - Health care settings, including hospitals and private clinics.
6. **Drinking water supply and distribution** – suppliers and distributors of water intended for human consumption and excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services.
7. **Digital Infrastructure** – IXPs, DNS service providers, TLD name registries.

Article 14 of the NIS Directive requires Member States to ensure that operators of essential services take appropriate and proportionate technical and organisational

measures to manage the risks posed to the security of network and information systems which they use in their operations. These measures may include:

- Information system security governance and risk management;
- Ecosystem management;
- IT security architecture;
- IT security administration;
- Identity and access management;
- IT security maintenance;
- Physical and environmental security;
- Detection;
- Computer security incident management;
- Continuity of operations; and
- Crisis management.

In 2019, EU adopted EU Cybersecurity Act [EUCSA] to further improve cybersecurity of the Union by strengthening protection of ICT products, services and process from cyber-threats through cybersecurity certification and reinforcing supply of cybersecurity products and services inside the Union.

These developments indicate that the EU is stepping up in improving its cybersecurity and incident-response capacity and aims at making Europe a leading player in the cybersecurity security industry. The EU NIS Directive and EU Cybersecurity Act are some of the factors that been taken into consideration to develop a methodology that can estimate cybersecurity investments made by the EIB under the ESI.

5. APPROACH TO IDENTIFICATION OF CYBERSECURITY RELATED INVESTMENTS UNDER THE ESI

By following the concept suggested after the kick-off meeting and elaborated during the inception activities [EIBASIR], the consultants have developed a comprehensive model based on a statistical approach that enables the identification of cybersecurity related investments. This approach was further fine-tuned considering the influencing factors and challenges identified during the project execution stage and documented in the 1st Interim Report [EIBASFIR]. The following sections describe in detail the methodology for the identification of the cybersecurity related investment under the ESI.

5.1. Methodology

The methodology for the identification of the cybersecurity related investment is based on an assumption that the cybersecurity component of investments exists in all investments that have an ICT component and, following international good practices and cybersecurity benchmarks, a certain range of the ICT budget should be directed to cybersecurity investments (the ICT investment is a proxy for the cybersecurity budget and investment).

The methodology identifies the cybersecurity related investment as a quantified value for a new, ongoing, or completed project. Figure 1, together with an explanation of every step in Table 1, presents the methodology in detail.

Figure 1. Methodology Diagram for identification of cybersecurity related investments

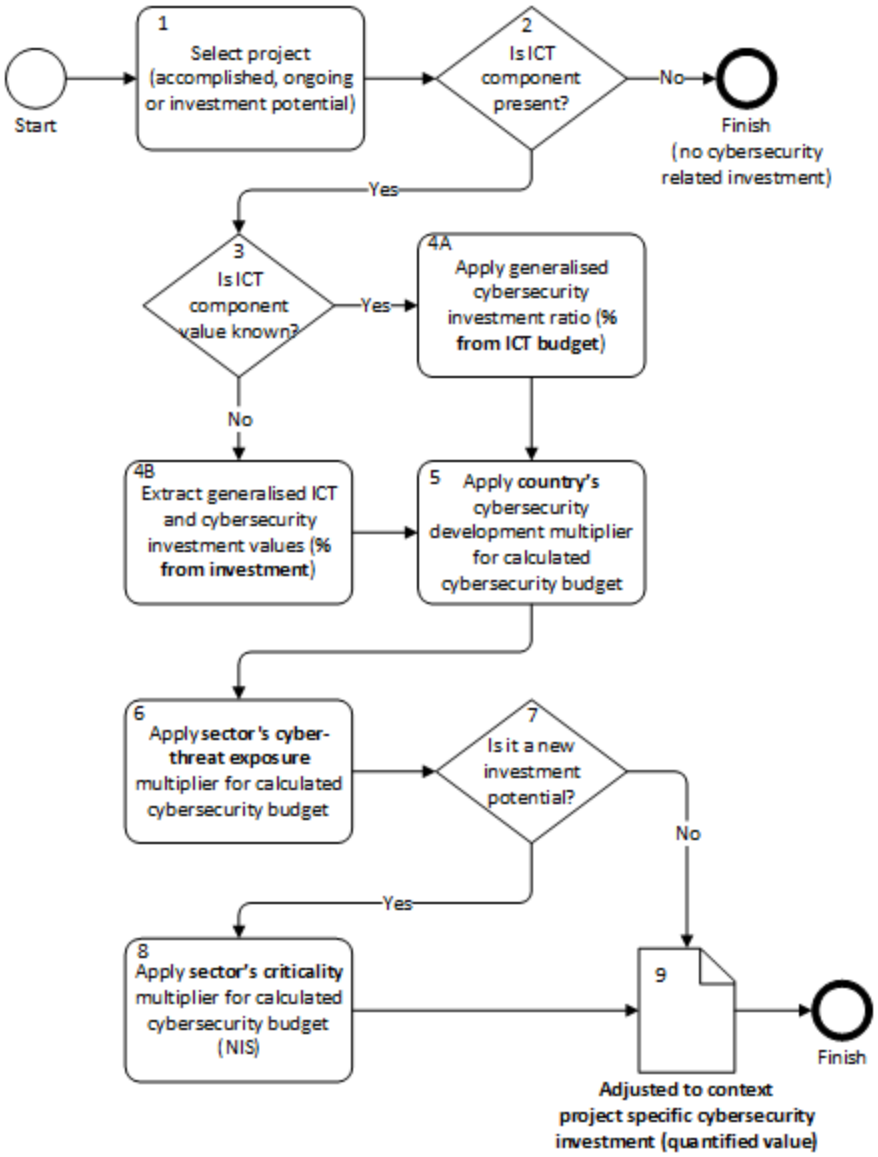


Table 1. Description of Methodology Diagram for identification of cybersecurity related investments

No	Step	Description
1.	Select project (accomplished, ongoing or investment potential)	Selection of project. The project has to have a minimal set of data available, to be eligible for the application of the methodology: – Project name; – EIB reference ID; – Project release date;

No	Step	Description
		– Promoter; – Total project cost (Approximate amount), EUR, million; – Proposed EIB finance (Approximate amount), EUR, million; – Link to official EIB project website.
2.	Is ICT component present?	Not all investment projects may have the inclusion of ICT components. It is therefore logical to conclude that if there is no ICT component present- there is no cybersecurity related investment. [Yes]: Go to step 3. [No]: Go to Finish (no cybersecurity related investments). ICT component is defined as an all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software.
3.	Is ICT component value known?	The project may contain a known value for the ICT component – specific ICT budget or overall investment. Depending on the information available, different quantification methods are applied. [Yes]: Go to step 4A. [No]: Go to step 4B.
4A.	Apply generalised cybersecurity investment ratio (% from ICT budget)	If the investment has an ICT component and the ICT budget is known, the cybersecurity component is quantified as a percentage of the ICT budget of such investment. To calculate, the user needs to select the country or the region where this investment is made, as different values apply depending on selected criteria. More information on the rationale and default values applied is provided in section 0 of this document.
4B.	Extract generalised ICT and cybersecurity	If the investment has an ICT component, but the exact ICT budget is not known, the cybersecurity

No	Step	Description
	Investment values (% from investment)	component is quantified first as a percentage of the statically calculated ICT investment, which is further adjusted by applying a qualitative and relative ICT-intensity multiplier. The ICT-intensity multiplier is developed by studying market research data on the average ICT-related spending within a specific sector relative to the total operational spending within the sector. Sectors and activities that traditionally are more focussed on the construction of infrastructure such as roads, ports, railways, buildings, etc. are characterised by very low spending in ICT as compared to sectors or activities where digital or ICT components are central to them, such as intelligent transport systems or smart mobility projects, Telecom infrastructure, banking solutions, industry 4.0 related projects etc. which have relatively higher spending in ICT. Lastly, the cybersecurity component is quantified using the generalised cybersecurity to ICT percentage. More information on the rationale and default value applied is provided in section 0 of this document.
5.	Apply country's cybersecurity development multiplier for calculated cybersecurity budget	Country cybersecurity development multiplier. Different countries have different cybersecurity development maturity. ITU Global Cybersecurity Index provides information on each country in 5 cybersecurity development dimensions. In order to apply this multiplier, the user needs to select a country or a region where investment is being made, as different percentage values apply to different countries or regions. More information on rationale and default values calculated is provided in section 0 of this document.
6.	Apply sector's cyber-threat exposure multiplier for	Different economic sectors have different risk exposure to cyber-threats. Application of the sector's cyber-threat exposure multiplier enables

No	Step	Description
	calculated cybersecurity budget	more precise calculations of the cybersecurity related investments. The sector's cybersecurity development multiplier is derived and quantified by using studies found during desk research. More information on rationale and default values calculated is provided in section 0 of this document.
7.	Is it a new investment potential?	The methodology differentiates between a new and completed ESI investment in order to fine-tune new investment potentials with the EU cybersecurity policy agenda. [Yes]: Go to step 8. [No]: Go to step 9.
8.	Apply sector's criticality multiplier for calculated cybersecurity budget (NIS)	The sector's criticality multiplier is a quantified value applied to boost the cybersecurity investments in EU critical sectors as defined by the EU NIS directive. Applies to new investment potential only. The multiplier is used to increase EU critical sectors' cyber resilience. More information on rationale and default values calculated is provided in section 0 of this document.
9A	Human Labour costs within cybersecurity	Human Labour costs within cybersecurity (cybersecurity innovation cost). This value is project specific, has to be known by investment officer (not all projects finance labour costs) and has to be added manually.
9B	Adjusted to context project specific cyber-security investment (quantified value)	Estimated cybersecurity investment value received after applying all multipliers using this methodology.

5.2. Data sources incorporated

Data sources incorporated into the methodology are described in Table 2. A list of all data sources that were evaluated but not selected to be incorporated into the methodology are provided in Annex A: List of data sources evaluated but not selected.

Table 2. List of data and its sources incorporated into the methodology

No	Data source	Description
1.	OECD Gross fixed capital formation (GFCF) statistical data [ODGFCF] Data used: ICT percentage in GFCF across European union countries.	GFCF consists of resident producers' investments, deducting disposals, in fixed assets during a given period. It also presents capital investments into ICT (CAPEX) as a percentage of total GFCF. Update frequency: yearly. Latest update: Q1 2020.
2.	Joint Research Centre (European Commission), The 2019 PREDICT Data set and key facts report [ECPREDICT] Data used: ICT market size data for EU countries	The 2019 PREDICT Key Facts Report and associated data set provides a detailed analysis of the state of ICT R&D activities in the EU. The report and associated dataset cover the period between 1995 to 2016, providing a long-term analysis of the European Union (EU) ICT sector and its R&D. The statistical information provided by the figures allows the comparison between ICT sector and the total economy. Update frequency: irregularly (expected to be updated once in two years). Latest update: January 2019.
3.	Study on the development of statistical data on the European security technological and industrial base [ECORYS]	The final report of the study on the development of statistical data on the European security technological and industrial base represents estimated market size data for EU security industry, including cybersecurity. Data is based on representative surveys conducted.

No	Data source	Description
	Data used: cybersecurity market size data for EU.	Update frequency: no (one-time calculation). Date: June 2015
4.	ITU Global Cybersecurity Index (GCI) 2018 report [ITUGCI] Data used: countries cybersecurity advancement index data.	The GCI is a composite index, which measures commitment of countries to cybersecurity. It quantifies legal, technical, organisational, capacity building, and cooperation measures. Update frequency: once in two years. Latest update: 2019
5.	Gartner IT Key Metrics Data 2018 [GARKMD] Data used: IT spending as a percentage of operating expenses; by industry for midsize enterprises. Data used: sectorial cybersecurity spending representation as a percentage from ICT spending.	The Gartner IT Key Metrics Data research series contains more than 3,000 IT investment, cost, staff, and performance metrics, including for cybersecurity. Update frequency: yearly. Latest update: December 2019

5.3. The ICRI tool

The Consultants developed the Identification of Cybersecurity Related Investment tool (the ICRI), which implements the methodology described in section 5.1 of this document. The tool is developed using Microsoft Excel and calculates cybersecurity investment values in a semi-automated and traceable way. The ICRI tool was applied on select EIB projects to validate the methodology and the cybersecurity investment estimates it produced. The findings are discussed in Chapter 6, "Validation of default values of cybersecurity related investments using the developed approach" of this report.

Mtd. step	Description	Values
1	Select project (accomplished, ongoing or investment	
	- Project name	**VHH HAMBURG E-MOBILITY PROGRAMME**
	- Reference ID	**20180665**
	- Release date	**12/Sep/2019**
	- Promoter	**ERKEHRSBETRIEBE HAMBURG-HOLSTEIN GMBH**
	- Total project cost (Approximate amount)	**EUR 142 million**
	- Proposed EIB finance (Approximate amount), EUR, million	**EUR 60 million**
	- Link	link
2	Is ICT component present? (Information and communication technology, abbreviated as ICT, covers all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software)	**Yes**
3	Is ICT component value known?	**No**
	- Defined total ICT budget, EUR, million	
	- Defined EIB financed ICT budget, EUR, million	
	- Investment in ICT intensity factor as a part of total investment (qualitative)(when ICT component value not known)	**Very low**
	- Investment in ICT intensity factor value	**0.32**
	- Estimated total ICT budget, EUR, million	**EUR 5.5 million**
	- Estimated EIB financed ICT budget, EUR, million	**EUR 2.32 million**
4B	Project investment into cybersecurity will be calculated as:	**generalised statistical % from total EIB investment into project**
	- Selected index (specific country or EU as a whole)	**Germany**
	- Applied default index value	**0.50%**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 0.23 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 0.10 million**
5	Apply **country's** cybersecurity development multiplier for calculated cybersecurity budget	
	- Selected index (automatically)	**ITU Global Cybersecurity Index (GCI) 2018**
	- Source for multiplier selection	**Germany**
	- Normalised multiplier value used for calculation	**1.09**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 0.25 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 0.11 million**
6	Apply **sector's cyber-threat exposure** multiplier for calculated cybersecurity budget	
	- Select sector (in a form of market segment)	**Transport**
	- Normalised multiplier value used for calculation	**0.83**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 0.21 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 0.09 million**
7	Is it a new investment potential?	**No**
8	Apply quantified NISD value to investment potential	
	- Select sector investment potential belongs to (NISD)	**Other than defined in NIS**
	- Sector's criticality multiplier (NISD) to be applied for new investment potential	**0.0%**
9A	*Human Labour costs (innovation cost) within cybersecurity finance by EIB, EUR, million*	**EUR 0.00 million**
9B	Adjusted to context project specific cybersecurity investment (quantified value), **total**, EUR, million	**EUR 0.21 million**
	Adjusted to context project specific cybersecurity investment (quantified value), **EIB-related**, EUR, million	**EUR 0.09 million**

Figure 2. Cybersecurity values calculation example using ICRI tool

6. CALCULATION OF DEFAULT VALUES OF CYBERSECURITY RELATED INVESTMENTS UNDER THE ESI

6.1. Calculation and default values of step 4A of the methodology – Apply generalised cybersecurity investment ratio (% from ICT budget)

When investment into ICT component is known in the project, the approximate cybersecurity investment can be extracted from the total investment into ICT by applying a generalized multiplier, calculated using the proportion of the EU cybersecurity market size to ICT market size. This section explains in detail how the default value for the cybersecurity investment is calculated as a percentage of the ICT budget.

The formula for step 4A is:

$$Cybersecurity\ investment\ ratio\ in\ project\ (as\ \%\ from\ ICT\ budget) = (Investment\ into\ ICT\ value)\ x\ (Generalised\ cybersecurity\ to\ ICT\ percentage)$$

Where

$$Generalised\ cybersecurity\ to\ ICT\ percentage = \frac{Cybersecurity\ market\ size\ in\ EU}{ICT\ market\ size\ in\ EU}\ x\ 100$$

Table 3 represents the calculation of default generalised cybersecurity to ICT percentage value.

Table 3. Calculation of generalised cybersecurity to ICT percentage value

No	Component	Value
1.	Size of EU cybersecurity market, 2015 [ECORYS]	EUR 26 billion
2.	Size of ICT market in EU, 2015 [ECPREDICT]	EUR 628 billion
3.	**Generalised cybersecurity ratio to ICT** (Size of EU cybersecurity market divided into Size of EU ICT (EU28))	4.14 %

Even though there is a possibility for deviation when applying the calculated ratio to an individual project, the deviation narrows when the ratio is applied to a larger sample space of projects, which also provides a better representation of the market. In addition, the latest statistical data set found on cybersecurity market size in EU is dated for year 2015.

As a result, this calculated generalised cybersecurity percentage value is applied once the ICT value is known and inserted into the ICRI tool. Later, calculated cybersecurity investment ratio will be adjusted with multipliers reflecting country's cybersecurity development maturity and sector's criticality.

3	Is ICT component value known?	**Yes**
	*- Defined **total** ICT budget, EUR, million*	**EUR 100 million**
	*- Defined **EIB financed** ICT budget, EUR, million*	**EUR 50 million**
4A	Project investment into cybersecurity will be calculated as:	**% from project's ICT budget**
	- Selected index (specific country or EU as a whole)	**Germany**
	- Applied default index value	**4.3%**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 4.3 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 2.1 million**

Figure 3. Cybersecurity component calculation example with ICRI when the project ICT value is known.

6.2. Calculation and default values of step 4B of the methodology – Extract generalised ICT and cybersecurity investment values (% from investment)

This step is used when ICT component value is not known in the project and needs to be extracted by using statistical approach. This step is based on the following formula:

$$Cybersecurity\ investment\ ratio\ in\ project\ (as\ \%\ of\ investment) =$$

$$(Investment\ value)\ x\ (ICT\ percentage\ in\ GFCF)\ x\ (Investment\ in\ ICT\ intensity\ ratio)\ x\ Generalised\ cybersecurity\ to\ ICT\ percentage$$

For default values of ICT percentage in GFCF, the OECD Gross fixed capital formation (GFCF) statistical data [ODGFCF] has been used, which is a proxy for extracting CAPEX

value from total investment). One of GFCF data subsets presents capital investments into ICT as a percentage of total GFCF.

Table 4. ICT percentage in GFCF

No	Country	Value
1.	Austria	14.5 %
2.	Czech Republic	16.0 %
3.	Denmark	13.3 %
4.	Estonia	8.5 %
5.	Finland	8.4 %
6.	France	16.1 %
7.	Hungary	7.3 %
8.	Italy	12.3 %
9.	Latvia	8.2 %
10.	Lithuania	14.9 %
11.	Luxembourg	8.9 %
12.	Netherlands	18.1 %
13.	Slovakia	4.8 %
14.	Slovenia	10.6 %
15.	Spain	13.5 %
16.	Sweden	18.7 %
17.	EU27 average	12.1 %

Investment in ICT intensity factor is a qualitative relative adjustment, developed from data representing ICT spending as a percentage of total operational spending data, as provided by Gartner IT Key Metrics Data 2018 [GARKMD].

Table 5 represents exact figures for the ICT intensity factor.

Table 5. Investment in ICT intensity factor

No	Intensity	Value	Calculation	When to apply?
1.	Very low	0.3	Minimum index (relative) value divided to arithmetic index average value.	Field / industrial works with indirect exposure to ICT. Best fitting: field works (transportation, pipelines, like roads with associated infrastructure, depots, natural resources, chemicals.
2.	Low	0.5	First quartile (25th percentile) index (relative) value.	Activities with limited exposure to ICT. Best fitting industries: construction (like houses, industrial buildings), industrial manufacturing, transportation (except field works), energy.
3.	Medium (standard)	1.0	Median (average) index (relative) value converted to default value.	Average. Direct or indirect exposure to ICT in project as a part of project activities. Best fitting industries: government, utilities.
4.	High	1.3	Third quartile (75th percentile) index (relative) value.	Activities with direct exposure to ICT. Best fitting industries: telecommunications, insurance, healthcare, if construction component is not present or is minimal
5.	Very high	2.5	Maximum index (relative) value divided to	Projects with heavy exposure to ICT and cybersecurity, related to

No	Intensity	Value	Calculation	When to apply?
			arithmetic index average value.	digitalization and/or automation, monitoring, log collection and several ICT systems integration, productivity and effectiveness enhancement as a dedicated part of project activities. Best fitting industries: financial services (excluding financing/refinancing activities).

These calculated multipliers are applied into the ICRI tool.

4B	Project investment into cybersecurity will be calculated as:	**generalised statistical % from total EIB investment into project**
	- Selected index (specific country or EU as a whole)	**Croatia**
	- Applied default index value	**0.50%**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 0.8 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 0.8 million**

Figure 4. Cybersecurity component calculation example with ICRI when the project ICT value is not defined.

6.3. Calculation and default values of step 5 of the methodology – Apply country's cybersecurity development multiplier for calculated cybersecurity budget

Different countries have different cybersecurity development maturity. Thus, projects in some countries may have more demanding requirements and standards for implementing cybersecurity compared to projects in some others, primarily due to a country's regulatory and legal environment, technical guidelines and digital

infrastructures to which integrations need to be established and maintained. The ITU Global Cybersecurity Index (ITU GCI) evaluates and reflects in its score (i) legal, (ii) technical, (iii) organisational, (iv) capacity building, and (v) cooperation parameters. As a result, countries' cybersecurity development maturity is represented as a specific ITU GCI score.

Due to the fact that the majority of the EIB projects are concentrated in EU27, the country's cybersecurity development multiplier is being calculated with the following formula:

$$Country's\ cybersecurity\ development\ multiplier = \frac{Country's\ ITU\ GCI\ value}{EU27\ average\ of\ ITU\ GCI\ value}\ x\ 100$$

As a result of applying this formula, the default values for EU27 cybersecurity development multipliers are:

Table 6. EU27 cybersecurity development multipliers

No	Component	Country's cybersecurity development multiplier value	ITU GCI value
	Austria	106%	0.826
	Belgium	105%	0.814
	Bulgaria	93%	0.721
	Croatia	108%	0.840
	Cyprus	84%	0.652
	Czech Republic	73%	0.569
	Denmark	110%	0.852
	Estonia	117%	0.905
	Finland	110%	0.856
	France	118%	0.918
	Germany	109%	0.849
	Greece	68%	0.527
	Hungary	105%	0.812
	Ireland	101%	0.784

No	Component	Country's cybersecurity development multiplier value	ITU GCI value
	Italy	108%	0.837
	Latvia	96%	0.748
	Lithuania	117%	0.908
	Luxembourg	114%	0.886
	Malta	62%	0.479
	Netherlands	114%	0.885
	Poland	105%	0.815
	Portugal	98%	0.758
	Romania	73%	0.568
	Slovakia	94%	0.729
	Slovenia	90%	0.701
	Spain	116%	0.896
	Sweden	104%	0.810
	EU27 average of ITU GCI value		0.776

These calculated multipliers are applied into the ICRI tool.

5	Apply **country's** cybersecurity development multiplier for calculated cybersecurity budget	
	- Selected index (automatically)	**ITU Global Cybersecurity Index (GCI) 2018**
	- Source for multiplier selection	**Germany**
	- Normalised multiplier value used for calculation	**1.09**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 4.8 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 2.4 million**

Figure 5. Cybersecurity component calculation example by applying country's cybersecurity development multiplier in ICRI tool.

6.4. Calculation and default values of step 6 of the methodology – Apply sector's cyber-threat exposure multiplier for calculated cybersecurity budget

Cyber-threats affect economic sectors differently. Cyber-threat actors have various motivations for carrying out cyber-attacks. However, two major trends emerge. One trend is to attack sectors where higher possibility to monetise malicious activities exists, the financial incentive being the motivation. For example, the finance industry is a target of professional malicious actors, which are forming malicious groups with profit sharing agreements. The second trend is to attack the most vital national assets (Critical Information Infrastructures (CIIs)) with two motivations: to illegally access sensitive data to support state level intelligence operations (for example – tax records of citizens); or to weaponize vulnerabilities found and exploit them to make damage to society (for example – industrial control systems managing electricity supply or cyberwarfare). This is a focus of malicious state actors or professional groups hired by malicious state actors.

On the other hand, sectors which face greater cyber-threat exposure, tend to invest more in cybersecurity in order to manage cyber risks. As a result, investments in cybersecurity differ from sector to sector.

The report on Gartner IT key metrics data for 2018 [GARKMD] was examined by EIB for sectorial multiplier development in a form of "IT Security spending as percent from total IT spending". Since generalised cybersecurity investment values are already calculated, using this data, sectorial differences were identified, using Cross-Industry Average as default cyber investment multiplier equal to 1 and calculating sectorial differences from this average.

$$Sectorial\ cybersecurity\ multiplier = \frac{Gartner\ sectorial\ value}{Garner\ Cross\ Industry\ Average}$$

Table 7. Gartner sectorial cybersecurity investment percentages and calculated sectorial multiplier

No	Industry	Security spending as % from IT spending	Multiplier
1.	Cross-Industry Average	6.0%	1.0
2.	Software publishing and internet services	8.7%	1.45
3.	Banking and financial services	7.3%	1.22
4.	Government - National/International	6.7%	1.12
5.	Retail and wholesale	6.1%	1.02
6.	Industrial electronics and electrical equipment	5.9%	0.98
7.	Pharmaceuticals, life sciences and medical products	5.8%	0.97
8.	Professional services	5.7%	0.95
9.	Insurance	5.7%	0.95
10.	Education	5.1%	0.85
11.	Energy	5.0%	0.83
12.	Healthcare providers	5.0%	0.83
13.	Industrial manufacturing	4.5%	0.75
14.	Government - Local	4.4%	0.73

Gartner data [GARKMD] represents economy sectors, not consistent with European classification NACE2 (used to designate the various statistical classifications of economic activities developed since 1970 in the European Union) and is not always applicable to the economic sectors classification, used by EIB. The mapping table was developed to simplify the Gartner sector data applicability to EIB investments. For sectors, where no direct mapping is present, Cross-Industry Average was used. For investments, when investment description is pointing to cross-sectorial investment, Cross-Industry Average is recommended to be used.

Table 8 Sectorial cyber-threat exposure multipliers calculated from Gartner data

EIB classification	Gartner Classification	Gartner value	Multiplier
Cross-Industry Average	Cross-Industry Average	6.0%	1.00
Agriculture, fisheries, forestry	-	6.0%	1.00
Composite infrastructure	-	6.0%	1.00

Credit lines	Banking and financial services	7.3%	1.22
Education	Education	5.1%	0.85
Energy	Energy	5.0%	0.83
Health	Healthcare providers	5.0%	0.83
Industry	Industrial manufacturing	4.5%	0.75
Industrial electronics	Industrial electronics and electrical equipment	5.9%	0.98
Services	Professional services	5.7%	0.95
Solid waste	-	6.0%	1.00
Telecom	Software publishing and internet services	8.7%	1.45
Transport	-	6.0%	1.00
Urban development	Government - Local	4.4%	0.73
Water, sewerage	-	6.0%	1.00

These calculated multipliers are applied into the ICRI tool.

6	Apply **sector's cyber-threat exposure** multiplier for calculated cybersecurity budget	**Sectorial cybersecurity multiplier**
	- Select sector (in a form of market segment)	**Industry**
	- Normalised multiplier value used for calculation	**0.75**
	- Calculated total cybersecurity budget in Project, EUR, million	**EUR 3.6 million**
	- Calculated EIB cybersecurity budget in Project, EUR, million	**EUR 1.8 million**

Figure 6. Cybersecurity component calculation example by applying the sectoral cyber-threat exposure multiplier in ICRI tool.

6.5. Calculation and default values of step 8 of the methodology – Apply sector's criticality multiplier for calculated cybersecurity budget (NIS)

EU promotes single digital market to enhance EU's position as a world leader in the digital economy. Cybersecurity is an integral component of this strategy. The Directive on Security of Network and Information Systems (NIS Directive) sets a benchmark for what constitutes a desirable level of institutional, policy and regulatory capacity to minimise the impact of cyber-threats and lays down measures with a view of achieving a high common level of security of networks and information

systems within the Union. The NIS Directive defines specific sectors and subsectors which provide services that are essential for the maintenance of critical and societal and economic activities, and which require a higher level of protection from cyber-threats and harmonized approach to cybersecurity across the EU.

The formula was developed to indicate the difference between a specific country and top 5 most cybersecurity advanced countries, in order to indicate what amount could be invested additionally to boost cybersecurity readiness in future investment projects that fall under the NIS defined critical sectors.

A list of cybersecurity measures, their purpose and their average costs are included in the Final Report to facilitate Project Promoters to evaluate and include a wide spectrum of cybersecurity measures into future projects to enhance cybersecurity and contribute directly to the European Security Initiative (ESI).

7. VALIDATION OF APPLIED METHODOLOGY FOR ESTIMATION OF CYBERSECURITY RELATED INVESTMENTS

This chapter presents the results of the validation of the methodology applied to estimate cybersecurity investment values in projects.

The quantification methodology developed combines statistical data sets available through OECD, Eurostat, and others, together with market research data from credible sources such as Gartner. It additionally calibrates cybersecurity investments based on available data on the project such as overall investment, specific investments towards ICT infrastructure, the presence of cybersecurity components, criticality of the sector and other sectoral multipliers. The table below lists the multipliers that are validated under this Chapter.

Table 9. Selected multipliers for cybersecurity investment calculations

No	Multiplier	Value
1.	ICT investment percentage in GFCF (Gross fixed capital formation) EU27 average, OECD data	12.1 %
2.	Sectorial investment into ICT intensity ratio, Gartner	0.32 – 2.45
3.	Cybersecurity investment ratio (% from ICT budget)	4.14%
5.	Security spending from IT spending: Sectorial multipliers	0.73 – 1.45

7.1. Validation of ICT investment percentage in GFCF multiplier

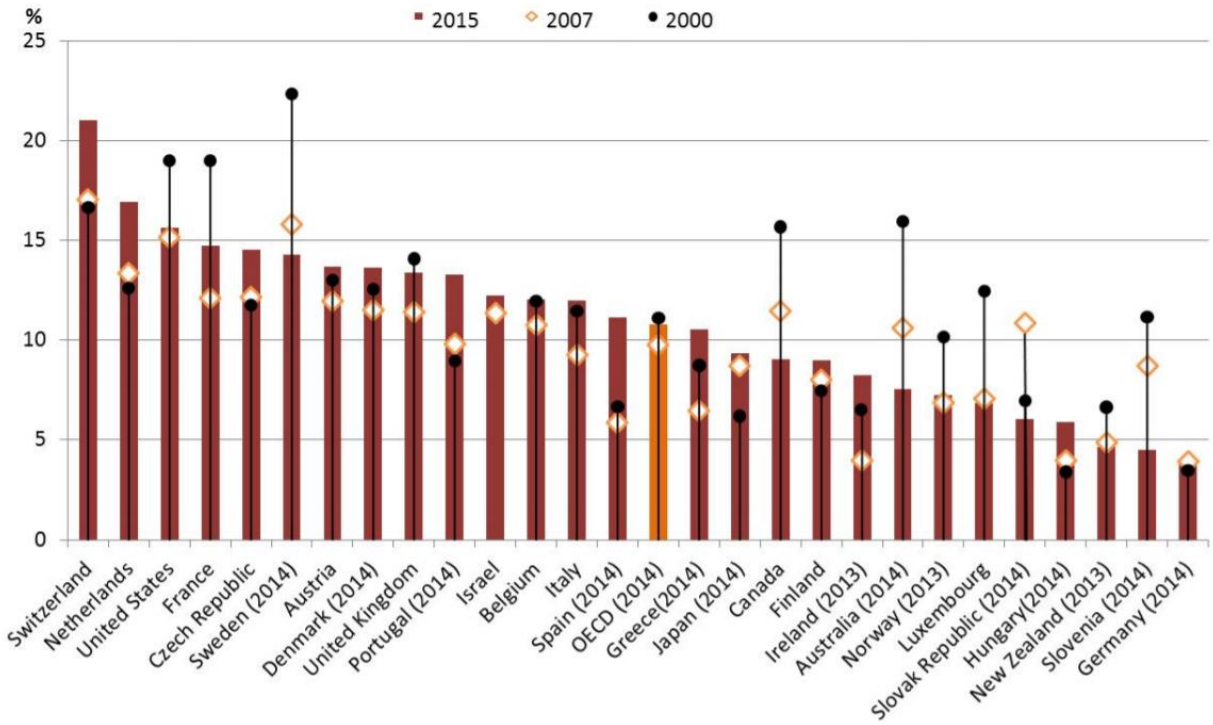
To verify and validate the accuracy of the value used for this multiplier, which represents the EU27 average for capital investments into ICT as a percentage of total Gross Fixed Capital Formation (GFCF), the following sources have been used.

7.1.1. Bank of France ICT investment data

Banque de France (BoF) has presented data on the investment in ICT in OECD countries as part of a working paper published in July of 2018 [BoFICTI] titled "Measuring "Indirect" Investments in ICT in OECD Countries". This document quotes "*…within global investment nominal spending, the ICT share seems stable over the 2000-2015 period, on average among OECD countries, but with differences between countries…*[1]"

The document includes data on ICT investment as a percentage of total investment, calculated by the authors of document. The authors estimate the average ICT investment value for the OECD countries to be around 12% for 2015. (Figure 7. BoF calculated ICT investment as a percentage of investment - 2000, 2007 and 2015). [BoFICTI] data is provided as reference but not used in calculations.

[1] Banque de France working paper "Measuring "Indirect" Investments in ICT in OECD Countries". https://publications.banque-france.fr/sites/default/files/medias/documents/wp-686.pdf



Source: Authors' calculations, 2017.

Figure 7. BoF calculated ICT investment as a percentage of investment – 2000, 2007 and 2015

7.1.2. World Bank ICT investment data

Data from the World Bank that calculates the ICT investment as a percentage of total non-residential gross fixed capital formation for 2009-2010 [WBICTI] can be examined[2] to further verify the "ICT investment percentage in GFCF" multiplier. range.

[2] https://tcdata360.worldbank.org/indicators/ict.inv?country=CAN&indicator=28&countries=BRA&viz=line_chart&years=2008,2010

Table 10. Word bank estimated ICT investment % for EU countries in 2009- 2010

No	Country	Year
1	Finland	2010
2	France	2009
3	Germany	2010
4	Ireland	2010
5	Italy	2010
6	Spain	2010
7	Sweden	2009
8	**Average**	**2010**

Basis the data available for only select EU27 countries listed above, the estimated average of ICT investment as a percentage of total non-residential gross fixed capital formation is – 15.21%. Although higher than the 12.1% that is used for this multiplier, when following the regional median within Europe (represented by the dotted-line below), a general trend towards a lowering median can be observed with the median dropping to around 13% in 2010. If data were available for additional countries and for more recent years, it is expected that the average for the ICT investment as a percentage of total non-residential gross fixed capital formation should be comparable to the 12.1% used in the methodology.

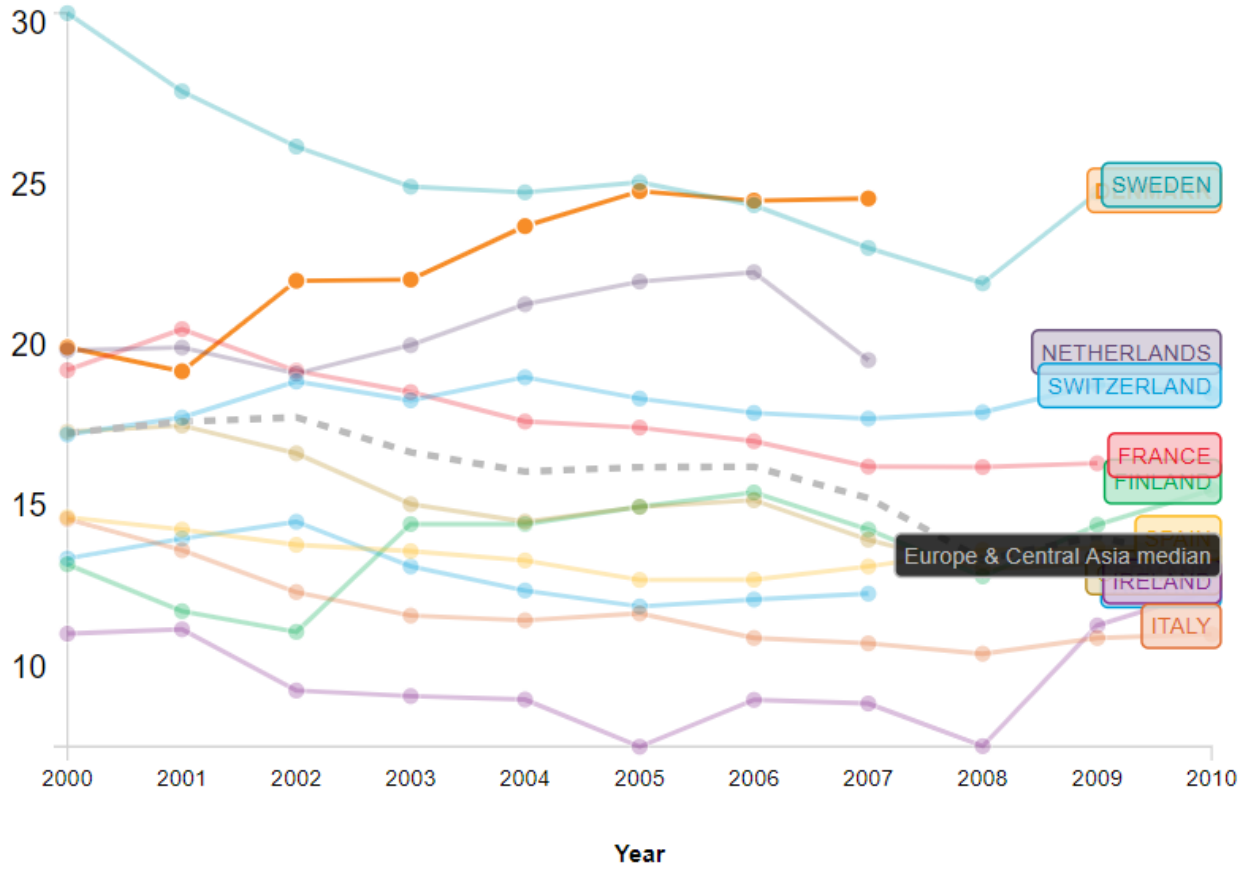


Figure 8. ICT investment as a percentage of total non-residential gross fixed capital formation from 2000-2010

7.1.3. EIB ICT investment data

EIB investment survey data [EIBICTI] for EU was verified for large and medium size enterprises[3], which indicated an EU ICT investment average of 11% for medium and 10% for large companies, which is again comparable to the multiplier value used.

[3] EIB Investment Survey – Tracking investment needs and constraints across Europe. https://data.eib.org/eibis/download

Table 11. EIB investment survey data for investments into ICT component

No	Country	Year	Sector	Size	Software, data, IT networks and website activities	Size	Software, data, IT networks and website activities
1	Austria	2017	All	Medium	0.11	Large	0.08
2	Belgium	2017	All	Medium	0.13	Large	0.1
3	Bulgaria	2017	All	Medium	0.08	Large	0.08
4	Croatia	2017	All	Medium	0.08	Large	0.07
5	Cyprus	2017	All	Medium	0.08	Large	-
6	Czechia	2017	All	Medium	0.16	Large	0.06
7	Denmark	2017	All	Medium	0.16	Large	0.17
8	Estonia	2017	All	Medium	0.09	Large	-
9	Finland	2017	All	Medium	0.14	Large	0.12
10	France	2017	All	Medium	0.11	Large	0.08
11	Germany	2017	All	Medium	0.14	Large	0.1
12	Greece	2017	All	Medium	0.11	Large	0.09
13	Hungary	2017	All	Medium	0.11	Large	0.09
14	Ireland	2017	All	Medium	0.1	Large	-
15	Italy	2017	All	Medium	0.12	Large	0.12
16	Latvia	2017	All	Medium	0.11	Large	0.18
17	Lithuania	2017	All	Medium	0.11	Large	0.12
18	Luxembourg	2017	All	Medium	0.11	Large	-
19	Malta	2017	All	Medium	0.12	Large	-
20	Netherlands	2017	All	Medium	0.14	Large	0.19
21	Poland	2017	All	Medium	0.12	Large	0.04

22	Portugal	2017	All	Medium	0.13	Large	0.09
23	Romania	2017	All	Medium	0.07	Large	0.12
24	Slovakia	2017	All	Medium	0.06	Large	0.07
25	Slovenia	2017	All	Medium	0.06	Large	0.06
26	Spain	2017	All	Medium	0.1	Large	0.09
27	Sweden	2017	All	Medium	0.1	Large	0.13
Calculated EU Average		**2017**	**All**	**Medium**	**0.11**	**Large**	**0.10**

7.2. Verification of sectorial investment intensity into ICT

Besides Gartner data, an article on Deloitte insights [4] [DEI] that presents the analysis of data collected for Deloitte's 2016-2017 Global CIO Survey showing the IT budget as percentage of revenue was further evaluated to extract sectorial ICT differences.

[4] Deloitte insights article: https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/technology-investments-value-creation.html

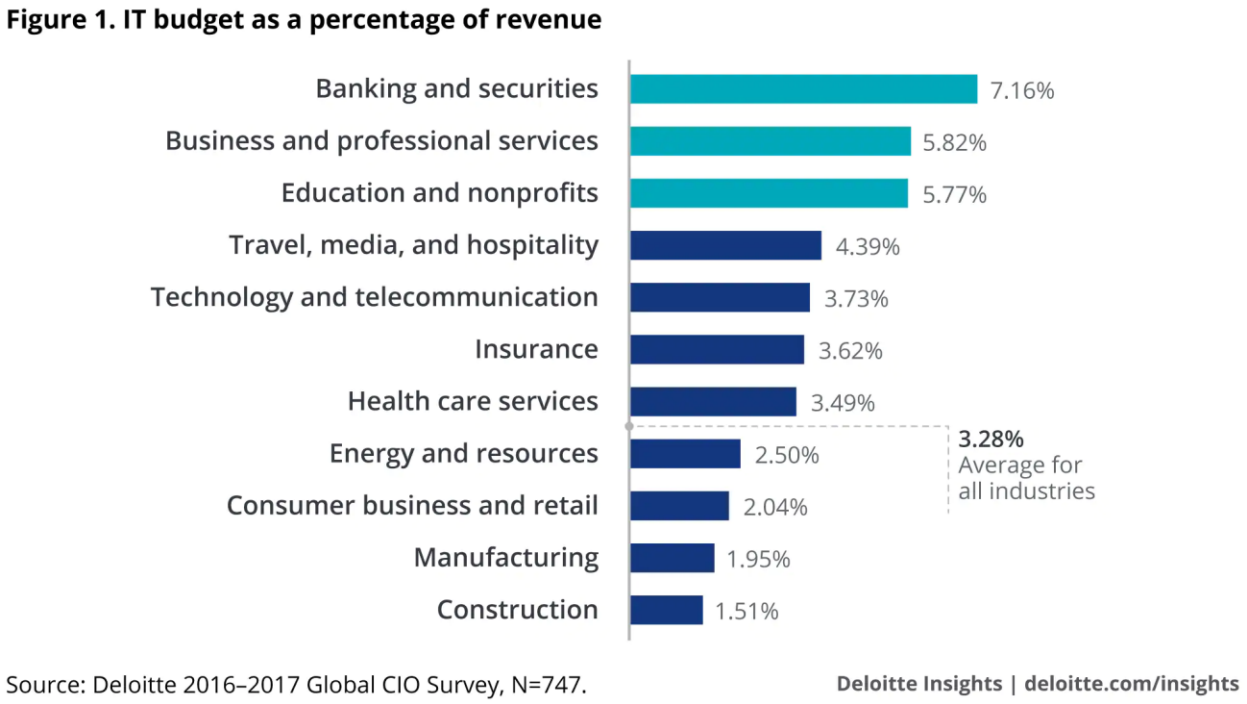


Figure 9. Deloitte data on IT budget as of percentage of revenue

[DEI] percentage values, recalculated to intensity ratios, gives following numbers (Table 12. Deloitte insights-based intensity ratios):

Table 12. Deloitte insights-based intensity ratios

No	Intensity	Value	Calculation
1.	Very low	0.3	Minimum index (relative) value divided to arithmetic index average value.
2.	Low	0.5	First quartile (25th percentile) index (relative) value.
3.	Medium (standard)	1	Median (average) index (relative) value converted to default value.
4.	High	1.1	Third quartile (75th percentile) index (relative) value.
5.	Very high	1.5	Maximum index (relative) value divided to arithmetic index average value.

Deloitte data shows a very good match to Gartner data, except for the Very high Intensity ratio, giving notably a lower value of 1.52 compared to Gartner's 2.5. This

difference can be explained by the data and the methodological differences between the two studies. Gartner data is split into 21 sectors compared to the 11 sectors used by Deloitte. Furthermore, Deloitte data is missing key sectors like the public sector which can be characterised by higher IT investments compared to the sectors in the lower quartile.

Looking at additional publicly available sources such as Computer economic research[5] [CER], it is observed that IT spending as a percentage of revenue in the financial services industry ranges between 4.4% at the 25th percentile to 11.4% at the 75th percentile, discrete manufacturing companies spend 1.4% and 3.2% at the 25th and 75th quartiles, respectively. This additional data matches with the sectoral IT spending data provided by both Gartner and Deloitte.

7.3. Verification of cybersecurity investment ratio in ICT

7.3.1. ECORYS Study

ECORYS Study on the development of statistical data on the European security technological and industrial base [ECORYS] estimates EU cybersecurity market size in EU for 2015 to be EUR 26 Billion. Using this data together with ICT market size of EUR 628 Billion [ECPREDICT], we estimated the Cybersecurity investment ratio (as a % of ICT budget) to be 4.14%.

7.3.2. BCG Article on Cybersecurity spending

An article[6] by BCG discussing the spending on Cybersecurity, compares the benchmark provided by two independent studies by PwC and Gartner that estimate the average security spending as a percentage of IT spending to be 3.7% and 5.9% respectively. The multiplier value of 4.14% used in the methodology falls in between these estimates.

[5] Computer economic research
https://www.computereconomics.com/article.cfm?id=2626
[6] Are you spending enough on Cybersecurity (BCG),
https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity

7.3.3. ENTERPRISE IRELAND data

Ireland government organisation "Enterprise Ireland", responsible for the development and growth of Irish enterprises in world markets, has published "The European Cybersecurity Market" study[7] [EIECM], covering Belgium, France, Germany, Italy, The Netherlands, Poland, and Spain. ICT and cybersecurity markets are estimated as follows (Table 13. [EIECM] ICT and cybersecurity market sizes and proportions):

Table 13. [EIECM] ICT and cybersecurity market sizes and proportions

No	Country	GDP, billions	ICT market, billions	ICT/GPD	Cyber market, billions	Cyber/ICT
1	Belgium	495	16.6	3.35%	0.4	2.41%
2	France	2591	60	2.32%	2.5	4.17%
3	Germany	3664	85	2.32%	5.7	6.71%
4	Italy	1950	61	3.13%	1.1	1.80%
5	Netherlands	833	33	3.96%	3.8	11.52%
6	Poland	526	9.9	1.88%	1.2	12.12%
7	Spain	1317	36	2.73%	1.3	3.61%
8	Total	11376	97	2.65%	16	5.3%

[EIECM] EU countries average gives estimated 5.3% Cybersecurity to ICT investment ratio, comparable to the multiplier value used in the methodology.

7.3.4. GARTNER data

[GARKMD] data estimates average cybersecurity to ICT investment ratio of 6%. Gartner further provides security spending breakdown by asset class (See Figure 10. Gartner security spending breakdown by asset class).

[7] "THE EUROPEAN CYBERSECURITY MARKET" study, https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Full-Report.pdf

No	Asset class	Spending %
1	Hardware	19
2	Software	23
3	Facilities	6
4	Personnel cost	27
5	Consulting	9
6	Managed services, cloud	8
7	Outsourcing services	8

Figure 10. Gartner security spending breakdown by asset class

As personnel cost in most circumstances is not eligible cost of investment and has to be excluded, Gartner cybersecurity to ICT investment ratio is estimated at 4.38%, after personnel cost exclusion.

Once again, we see the 4.14% value comparable to the Gartner data.

7.4. Verification of Sectorial multipliers of cyber security spending

[ECORYS] dataset provides estimated turnover for cybersecurity products and services for different sectors and employment in EU related to cybersecurity products and services. These two datasets can be used to validate the sectoral multiplier for cybersecurity spending.

Table 14. [ECORYS] employment based sectorial multipliers

Industry	Employment based sectorial multiplier
Defence	1.20
Public security service providers	1.02
Public administration	1.83
Health and education	**0.76**
Transport	**0.80**
Energy and water	**0.77**
Communications and information services	**1.14**
Financial services	**1.67**

Primary sectors	0.40
Manufacturing	1.25
Construction	0.75
Real estate and property management	0.82
Wholesale and retail distribution	1.16
Hotels, restaurants, and leisure	0.84
Other market services	0.63
Private individuals and households	1.54
Other	1.00

Table 15. [ECORYS] turnover based sectorial multipliers

Industry	Turnover based sectorial multiplier
Defence	0.78
Public security service providers	0.91
Public administration	1.54
Health and education	**0.61**
Transport	**0.62**
Energy and water	**0.60**
Communications and information services	**0.84**
Financial services	**1.39**
Primary sectors	0.33
Manufacturing	1.11
Construction	0.64
Real estate and property management	0.68
Wholesale and retail distribution	1.04
Hotels, restaurants, and leisure	0.73
Other market services	0.50
Private individuals and households	1.32
Other	0.26

Considering NIS directive and 5 EU critical sectors, following comparison table can be built to evaluate data:

Table 16. Sectorial cybersecurity spending multipliers comparison for critical sectors

Sector	Gartner multiplier	ECORYS employment-based multiplier	ECORYS turnover-based multiplier
Health and education	0.83	0.76	0.61
Transport	-	0.80	0.62
Energy and water	0.83	0.77	0.60
Communications and information services	1.45	1.14	0.84
Financial services	1.22	1.67	1.39

Gartner data was selected as primary source as having fewer extreme values. As Gartner data was missing Transport sector multiplier and [ECORYS] values show that Health, Transport and Energy sectors have relatively similar sectorial multipliers, estimated 0.83 value for transport sector is recommended to be used to fill the Gartner data gap.

8. REVIEW OF ELIGIBLE COST ITEMS FOR CYBERSECURITY PROJECTS

This section represents results of review of eligible cost items for cybersecurity projects and suggests improvement opportunities backed by best practices.

The EIB document named Eligibility Costs for Cybersecurity projects – for Adopters (bank groups, major companies, …), dated December 2017 was reviewed against the European Cyber Security Organisation's cybersecurity products and services action-oriented taxonomy defined in the ECSO Cybersecurity Market Radar [ECSOMR]. In general, ECSO Cybersecurity Market Radar provides the following cybersecurity products and services taxonomy:

Table 17. ECSO Cybersecurity Market Radar taxonomy

No	Solution category	Product/service group
1.	Asset management (The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy)	• IT Service Management • Software & Security Lifecycle Management
2.	Business environment (The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions)	• Business Impact Analysis
3.	Governance & Risk Management	• Governance, Risk & Compliance (GRC)

No	Solution category	Product/service group
	(The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk)	• Security Certification
4.	Risk assessment (The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals)	
5.	Risk management strategy (The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions)	
6.	Supply chain risk management (The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks)	
7.	Identity Management & Access Control (Access to physical and logical assets and associated facilities is limited to authorized users, processes, and	• Access Management • Authentication • Authorisation • Identity Management

No	Solution category	Product/service group
	devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions)	
8.	Awareness and Training (The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements)	• Awareness Trainings • Cyber Ranges
9.	Data Security (Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information)	• PKI / Digital Certificates • Data Leakage Prevention • Encryption • Cloud Access Security Brokers • Hardware Security Modules (HSM) • Digital Signature
10.	Information Protection Processes and Procedures (Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets)	• Static Application Security Testing (SAST) • Application Security
11.	Maintenance (Maintenance and repairs of industrial control and information system	• Patch Management • Vulnerability Management • Penetration Testing / Red Teaming

No	Solution category	Product/service group
	components are performed consistent with policies and procedures.)	
12.	Protective Technology (Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements)	• Wireless Security • Remote Access / VPN • IoT Security • PC/Mobile/End Point Security • Mobile Security /Device management • Sandboxing • Content Filtering & Monitoring • Firewalls / NextGen Firewalls • Unified Threat Management (UTM) • Anti-Spam • Anti-Virus/Worm/Malware • Backup / Storage Security
13.	Anomalies and Events (Anomalous activity is detected and the potential impact of events is understood)	• Fraud Management • Intrusion Detection
14.	Security Continuous Monitoring (The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures)	• SIEM / Event Correlation Solutions • Cyber Threat Intelligence • Security Operations Center (SOC)
15.	Detection Processes (Detection processes and procedures are maintained and tested to ensure awareness of anomalous events)	• Underground/Darkweb investigation • Honeypots / Cybertraps • Social Media & Brand Monitoring
16.	Planning Response	• Incident Management • Crisis Management

No	Solution category	Product/service group
	(Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents)	
17.	Communications (Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies))	• Crisis Communication
18.	Analysis (Analysis is conducted to ensure effective response and support recovery activities)	• Fraud Investigation • Forensics
19.	Mitigation (Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident)	• Takedown services • Services (CSRIT aaS) Incident Response • Data Recovery • DDoS Protection • Cyber Security Insurance
20.	Improvements (Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities)	
21.	Recovery planning (Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents)	• Business Continuity/ Recovery Planning • System Recovery

Description of each solution category defined in the table is taken from the NIST Cyber Cybersecurity Framework [NISTCSF].

The eligible EIB cybersecurity cost items reviewed against ECSO categories and product/service groups are defined in Table 17 of this document, and the following improvements are suggested to the EIB document Eligibility Costs for Cybersecurity projects:

1. To add new eligible categories into the list:
    i. Governance, Risk & Compliance (GRC) consulting/management activities/services;
    ii. Cyber threat intelligence HW/SW/services;
    iii. Digital forensics.
2. Expand a set of protective technology HW/SW items with:
    i. Wireless security;
    ii. Remote access / VPN;
    iii. IoT security;
    iv. PC/mobile/end point security;
    v. Mobile security/ device management;
    vi. Sandboxing;
    vii. Unified Threat Management (UTM);
    viii. Anti-spam;
    ix. Backup / storage security.
3. To update data security subcategories with:
    i. PKI/digital certificates;
    ii. Encryption HW/SW;
    iii. Hardware Security Modules (HSM).

9. SWOT ANALYSIS OF DEVELOPED METHODOLOGY

While various methodologies can be applied for estimating the cybersecurity investment in particular projects (detailed information is provided in the inception [EIBASFIR] and 1st Interim [EIBASIR] reports), the proposed statistical approach is the only one feasible due to various limitations related to the availability and granularity of the project-level data of EIB financed projects. During 2018-2020 financial years, the bank is expected to accomplish more than two thousand investment projects. When a statistical approach is applied to a large sample space such as this, it is known to produce reliable results, as projects' investment fluctuations will average out. The approach has several advantages and disadvantages to be considered when applying the methodology. Therefore, the following SWOT table has been prepared to represent these findings in detail.

Table 18. SWOT analysis of developed methodology

Strengths (S)	Weaknesses (W)
• Simple to use: made in stepped, human-readable, and easy-to-follow approach. • Out-of-the-box usage: input for EIB calculation is taken from data "as-is" and does not require detailed projects' breakdown (which is difficult to get for a large number of projects). • Applicable at an early project stage, many details are not known / identified. • Allows quick calculations at large scale. • Calculates investment (CAPEX) part of cybersecurity budget. • Produces reliable results while using at scale (applied to more than >50 projects to have better representation of GDP and investments in economies). • Calibrated for EU economies/countries with associated statistical datasets.	• Might have larger deviation when applied at medium scale (up to 50 projects) • Can lead to deviations if reliable data is not being used for multipliers (which is not the case for the methodology provided as it builds on reliable primary data sources). • Does not address sub-sectorial multipliers as only very fragmented data was identified for it (several publicly and commercially available data sets and reports were investigated). • EU cybersecurity market size value is found for year 2015 only and there are no additional/similar studies to validate data provided in the respective study.
Opportunities (O)	**Threats (T)**
• Easily extendable and adjustable when more specific data is available. • Easily adoptable/changeable for future needs as parameters are not locked (e.g., for other regions). • Open for (re-)validation with future datasets (e.g., from EUROSTAT, project breakdowns, dedicated specific market studies).	• Significant deviation possible, if applied at a single project level.

9.1. Recommendations for further development and improvement of methodology

At the current juncture, with the available data on the EIB financed projects and the literature on cybersecurity, ICRI has been developed with the most optimal set of parameters to perform calculations required to extract cybersecurity investment within the EIB financed projects. However, the following improvements and its update aspects need to be considered in the future:

1. EU cybersecurity market size data needs to be updated when a new representative study with exposure to EU will be conducted.
2. Exact figure of the ICT percentage in GFCF is known for only half of the EU member states. Associated calculation table needs to be updated when more data will be available.
3. Associated data sets need to be updated every year (starting from 2021) to reflect the most recent data in associated statistical data sets.
4. If additional dimensions or factors influencing cybersecurity investments are learnt in the future, ICRI should be modified to introduce or replace multipliers that can further improve the accuracy of the estimates produced by the methodology.

ACRONYMS

Acronym	Meaning
BYOD	Bring Your Own Device
BoF	Bank of France
CAPEX	Capital expenditures
CII	Critical Information Infrastructure
EC	European Commission
ECSO	European Cyber Security Organisation
EHR	Electronic Health Records
EIB	European Investment Bank
ESB	Erste & Steiermaerkische Bank
ESI	European Security Initiative
ETD	Environment and Sustainable Territorial Development Department
EU	European Union
FTE	Full time employee
JRC	Joint Research Centre
GCI	Global Cybersecurity Index
GDP	Gross Domestic Product
GFCF	Gross fixed capital formation
ICRI	Identification of Cybersecurity Related Investment tool
ICT	Information and Communications Technologies
INCO	Innovation and Competitiveness Department
ITU	International Telecommunication Union
NIS	Networks and Information Systems
NIS Directive	Directive on Security of Networks and Information Systems
OECD	Organisation for Economic Co-operation and Development
OPEX	Operational expenditures
PaaS	Platform as a Service
PCI	Public Common Interest
R&D	Research and Development
RDI	Research, Development, Innovation
SaaS	Software as a Service
SME	Small and Medium Enterprises
SIEM	Security Information and Event Management
SWOT	Strengths, Weaknesses, Opportunities, and Threats

BIBLIOGRAPHY

There are no sources in the current document.

REFERENCES

[ATEADC]	European Investment Bank. (2018). *ATEA DC expansion*. Retrieved from https://www.eib.org/en/projects/pipelines/all/20170547
[BoFICTI]	Banque de France, July 2018. Measuring "Indirect" Investments in ICT in OECD Countries. https://publications.banque-france.fr/en/measuring-indirect-investments-ict-oecd-countries
[CIDSUEA]	Beissel, S. (2016). *Cybersecurity Investments Decision Support Under Economic Aspects*. Switzerland: Springer.
[CER]	Computer economic research. https://www.computereconomics.com/article.cfm?id=2626
[DEI]	Deloitte insights. https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/technology-investments-value-creation.html
[DSMSE]	European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region on the Mid-Term Review on the Implementation of the Digital Single Market Strategy: A connected digital single market for all", COM(2017) 228 final, Brussels, 10 May 2017.
[DSNIS]	Directive (EU) 2016/1148 of the European Parliament and of the Council of July 2016 concerning measures of a high common level of security of network and information systems across the Union.
[ECPREDICT]	Joint Research Centre (European Commission), "The 2019 PREDICT Key Facts Report. An Analysis of ICT R&D in the EU and Beyond", 11 June 2019. Luxembourg. ISSN 1831-9424. https://op.europa.eu/s/n22G Link to the dataset for download: https://ec.europa.eu/jrc/en/predict/ict-sector-analysis-2019/data-metadata
ECPREDICT2020]	Joint Research Centre (European Commission), "The 2020 PREDICT

	Key Facts Report. An Analysis of ICT R&D in the EU and Beyond", 06 August 2020. Luxembourg. ISBN 978-92-76-20790-0. https://op.europa.eu/en/publication-detail/-/publication/1f4d0e0e-d853-11ea-adf7-01aa75ed71a1
[EIBASFIR]	FIRST INTERIM REPORT
[EIBASIR]	INCEPTION REPORT
[EIBICTI]	EIB investment survey- "Tracking investment needs and constraints across Europe". https://data.eib.org/eibis/download
[EIECM]	Enterprise Ireland. The European cybersecurity market. Mapping the opportunities and route to market for Irish SMEs. Retrieved from https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Full-Report.pdf
[ECORYS]	European Commission DG Migration and Home Affairs. (2015). Study on the development of statistical data on the European security technological and industrial base. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/security_statistics_-_final_report_en.pdf
[ECSOMR]	European Cyber Security Organisation. (2018). The ECSO Cybersecurity Market Radar. Retrieved from https://www.ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-brochure.pdf and https://ecs-org.eu/working-groups/news/the-ecso-cyber-security-market-radar
[ESTGDP]	EUROSTAT, GDP and main components (output, expenditure and income). Retrieved from https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_gdp&lang=en
[ECSOCMR]	European Cyber Security Organisation. (2019). *The ECSO cybersecurity market radar*. Retrieved from https://www.ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-brochure_20190911_10_14_26.pdf
[EICTIDX]	Organisation for Economic Cooperation and Development. (2017). *Evolution of ICT investments, as a percentage of total*

	investments. Retrieved from https://www.oecd.org/sti/broadband/oecdkeyictindicators.htm
[EUCSA]	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No. 5216/2013 (Cyber Security.
[EUCSS]	Council of the European Union, "Council Conclusions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 22 July 2013 (doc. 12109/13).
[EUSTAR]	European Commission, "Communication from the Commission to the European Parliament and the Council – The EU approach to resilience: Learning from security crisis", COM(2012) 568 final, Brussels, 3 October 2012.
[GARKMD]	Gartner, IT Key Metrics Data 2018: Index of Published Documents and Metrics, 11 December 2017. Retrieved from https://www.gartner.com/en/documents/3830144/it-key-metrics-data-2018-index-of-published-documents-an
[GARTPI]	Gartner Peer Insights. Retrieved from: https://www.gartner.com/reviews/markets
[ISO27001]	ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements International Organization for Standardization, Geneva, Switzerland. https://www.iso.org/standard/54534.html
[ITUGCI]	ITU. (2018). Global Cybersecurity Index (GCI) 2018 report. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[NISTCSF]	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 National Institute of Standards and Technology 16 April 2018. https://www.nist.gov/cyberframework

[ODGFCF]	OECD. (2020). Investment by asset (indicator). doi: 10.1787/8e5d47e6-en (Accessed on 26 May 2020). Retrieved from: https://data.oecd.org/gdp/investment-by-asset.htm#indicator-chart
[WIKI]	Wikipedia The Free Encyclopaedia. Retrieved from: https://www.wikipedia.org/
[WBICTI]	World bank calculated dataset of economy indicators https://tcdata360.worldbank.org/indicators/ict.inv?country=CAN&indicator=28&countries=BRA&viz=line_chart&years=2008,2010

ANNEXES

Annex A: List of data sources evaluated but not selected

The following table presents a list of data sources evaluated while developing the methodology for estimating cybersecurity investments in projects.

Table 19. List of data sources evaluated but not incorporated in the methodology

No	Data source
1.	Directorate-General for Communications Networks, Content and Technology (European Commission), Leaders in security (LSEC), PwC. (2018). Cybersecurity industry market analysis. Final report. Retrieved from: https://op.europa.eu/s/n7eE
2.	Hughes, Barry & Bohl, David & Irfan, Teuku & Margolese-Malin, Eli & Solórzano, José. (2016). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. Technological Forecasting and Social Change. 10.1016/j.techfore.2016.09.027.
3.	Eurostat. (2020). ICT security in enterprises in 2019. ISSN 2443-8219. Retrieved from: https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises
4.	Accenture. (2020). Third annual report on state of cyber resilience. Retrieved from: https://www.accenture.com/ae-en/insights/security/invest-cyber-resilience
5.	Boston consulting group (BCG). (2019). Are You Spending Enough on Cybersecurity? Retrieved from: https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity.aspx
6.	UK Department for Digital, Culture, Media & Sport. (2019). Official Statistics. Cyber Security Breaches Survey 2019. Retrieved from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019
7.	The Lisbon Council for Economic Competitiveness and Social Renewal, International Data Corporation (IDC). (2019). The European data market monitoring tool: key facts & figures, first policy conclusions, data landscape and quantified stories. Retrieved from: http://datalandscape.eu/study-reports
8.	Energy expert cyber security platform. (2017). Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector. Retrieved from: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

No	Data source
9.	TNS Opinion & Social. (2015). Special Eurobarometer 423. Cyber security report. Retrieved from: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf
10.	TNS Opinion & Social. (2017). Special Eurobarometer 464a. Europeans' attitudes towards cyber security report. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/special-eurobarometer-europeans-attitudes-towards-cyber-security
11.	Dark reading. (2018). How Enterprises Are Attacking the Cybersecurity Problem. Retrieved from: https://www.darkreading.com/archives.asp?section_id=315&
12.	International monetary fund. (2018). World Economic and Financial Surveys. Fiscal Monitor. Capitalizing on Good Times. Retrieved from: https://www.imf.org/en/Publications/FM/Issues/2018/04/06/fiscal-monitor-april-2018
13.	The Hague Centre for Strategic Studies. (2016). Dutch investments in ICT and cybersecurity. Putting it in perspective. Retrieved from: https://www.thehaguesecuritydelta.com/media/com_hsd/report/123/document/HCSS-Dutch-Investments-in-ICT.pdf
14.	Nasdaq Global information services. (2018). Cybersecurity Industry Report & Investment Case. Retrieved from: https://www.nasdaq.com/articles/cybersecurity-industry-report-investment-case-2018-06-25
15.	Directorate-General for Communications Networks, Content and Technology (European Commission). (2015). Monitoring the Digital Economy & Society 2016 – 2021. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/new-monitoring-framework-digital-economy-and-society
16.	Enterprise Ireland. (2019). The European cybersecurity market mapping and route for Irish SMES. Key takeouts. Retrieved from: https://globalambition.ie/cybersecurity-report-and-conference/
17.	Spiceworks. (2019). Details on the data of survey conducted within business technology buyers from organizations across North America and Europe. Retrieved from: https://www.spiceworks.com/marketing/state-of-it/report/
18.	Ernst & Young (EY). (2018). Global Information Security Survey 2018-19. Retrieved from: https://www.ey.com/en_lu/advisory/global-information-security-survey-2018-2019

Annex B: Essential information on cybersecurity product/service groups

This annex represents essential information about cybersecurity product/service groups. The baseline for product/service groups' description is taken from Gartner Peer Insights [GARTPI] and Wikipedia [WKPD] webpages. Indicative prices provided for each product/service category is estimated for medium-large size enterprise (250 – 500 employees) with 3 years of support. Defined price ranges are indicative and might vary significantly, depending on the context and maturity of technology and the organisation providing the technology.

Table 20. Detailed description of cyber security product/service groups

No	Product/service group	Description
1.	IT Service Management	Set of methods and best IT management practices supported and implemented within a solution that enables an organisation to maximise business value from the use of ICT. Usually purchased as service desk software with deployment services. Expected cost variations: EUR 20000 – 200000. Indicative product examples: ServiceNow, JIRA Service Desk Alternative: cloud SaaS subscription. Open source: available.
2.	Business Impact Analysis	Systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. Usually is purchased as a consulting service. Expected cost variations: EUR 10000 – 100000.
3.	Governance, Risk & Compliance (GRC)	Integrated collection of capabilities that enable an organisation to reliably achieve objectives, address uncertainty and act with integrity.

No	Product/service group	Description
		Usually purchased as software with deployment services. Expected cost variations: EUR 200000 – 1000000. Indicative product example: RSA archer suite. Alternative: cloud SaaS subscription.
4.	Security Certification	Assessment and certification of organisation's information security management system's conformance to international (like ISO/IEC 27001:2013) or applicable local standards by authorised accredited body. Usually purchased in two phases: i) as a consulting service for implementation of information management system and ii) certification. Expected cost variations for implementation: EUR 30000 – 100000. Expected cost variations for certification: EUR 10000 – 30000. Indicative service providers: Bureau Veritas, TUV.
5.	Access Management	Access management applies to technologies that use access control engines to provide centralized authentication, single sign-on (SSO), session management and authorisation enforcement for target applications in multiple use cases. Typically is combined with or acts as Identity management solutions. Usually purchased as a software with integration services or as a cloud service. Expected cost variations: EUR 10000 – 500000. Indicative product example: Microsoft Active Directory.
6.	Authentication	Products and services that provide user authentication for the enterprise's workforce and

No	Product/service group	Description
		various counterparties, like customers. This supports their access to electronic or digital assets owned or managed by, or provided on behalf of, the enterprise. User authentication is the real-time corroboration (with an implied or notional confidence or level of trust) of a person's claim to an identity previously established to enable his or her access to an electronic or digital asset. Usually is purchased as a software (can include dedicated hardware / server) or as a cloud SaaS. Expected cost variations: EUR 5000 – 100000. Indicative product example: Microsoft Multi-Factor Authentication, Yubico YubiKey.
7.	Authorisation	Refer to product/service group: Authentication.
8.	Identity Management	Identity governance and administration solutions manage identity and access life cycles across multiple systems. These products automate provisioning of accounts, fulfil access requests, manage passwords, and govern user access and access certification processes. Usually is combined with or acts as Access management solutions. Usually purchased as a software with integration services or as a cloud SaaS. Expected cost variations: EUR 100000 – 500000. Indicative product example: Microsoft Identity Manager, Oracle Identity Manager.
9.	Awareness Trainings	Cybersecurity awareness raising and training activities. Can be supported by dedicated awareness portals (software) and computer-based testing tools. Usually purchased as an online or on-premise training activity (OPEX).

No	Product/service group	Description
		In case of on-premises platform deployment (CAPEX), expected cost variations: EUR 20000 – 100000. Indicative product example: Lucysecurity, Phishingbox, Hoxhunt.
10.	Cyber Ranges	A controlled virtual hands-on environment for simulating and learning essential and specific skillset for incident detection, management, and response. In some cases can involve offensive skills development. Usually is purchased as a SaaS subscription or dedicated event for a cybersecurity team (with cost variations: EUR 5000 – 50000). Alternative approach for large enterprises: deployment on premise (EUR 200000 – 500000). Indicative product example: Cyberbit cloud cyber range, Check point cyber range.
11.	PKI / Digital Certificates	Set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. Expected cost variations: EUR 10000 – 100000. Indicative product example: Microsoft Active Directory Certificate Services. Alternative approach: cloud PaaS.
12.	Data Leakage Prevention	Provides visibility into data usage across an organisation for a broad set of use cases and the dynamic application of policies based on the content and context at the time of an operation. DLP seeks to address data related threats including the risks of inadvertent or accidental data loss, and the exposure

No	Product/service group	Description
		of sensitive data using monitoring, filtering, blocking and other remediation features. Usually purchased as a software or an appliance (software with dedicated hardware) with deployment services. Expected cost variations: EUR 50000 – 150000. Indicative product example: Symantec DLP, Safetica DLP, McAfee DLP.
13.	Encryption	Solutions that encrypt data at-rest on endpoint devices like computers, smartphones, and tablets, including BYOD. Usually is purchased as a software or cloud SaaS for managing BYOD. Expected cost variations: EUR 10000-100000. Indicative product example: Microsoft BitLocker, Sophos SafeGuard, IBM MaaS360. Also check category PC/Mobile/End Point Security.
14.	Cloud Access Security Brokers	Solution that sits between cloud service users and cloud applications and monitors all activity and enforces security policies. Can offer a variety of services such as monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware. Usually is purchased as an on-premises or cloud SaaS. Expected cost variations: EUR 10000 – 100000. Indicative product example: Proofpoint Cloud App Security Broker, Netskope Security Cloud.
15.	Hardware Security Modules (HSM)	Physical computing device that safeguards and manages digital keys, performs encryption and

No	Product/service group	Description
		decryption functions for digital signatures, strong authentication, and other cryptographic functions. Usually is purchased as an on-premises or cloud platform with dedicated hardware. Expected cost variations: EUR 10000 – 50000. Indicative product example: Thales HSM, Azure Dedicated HSM.
16.	Digital Signature	A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity. Usually is purchased as a cloud SaaS. Expected cost variations: EUR 10000 – 50000. Indicative product example: Adobe Sign, DocuSign.
17.	Static Application Security Testing (SAST)	A set of technologies designed to analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyse an application from the "inside out" in a non-running state. Usually is purchased as a software. Expected cost variations: EUR 5000 – 20000. Indicative product example: Veracode Static Analysis, SonarQube.
18.	Application Security	Consulting service incorporation broad list of services associated to application security. Usually based on risk assessment and/or threat modelling. Usually is purchased as a consulting service. Expected cost variations: EUR 10000 – 50000. Check references in: Business Impact Analysis, Governance, Risk & Compliance (GRC), Encryption,

No	Product/service group	Description
		Static Application Security Testing (SAST), Patch Management, Vulnerability Management, Penetration Testing / Red Teaming, Backup / Storage Security, DDoS Protection, System Recovery and related.
19.	Patch Management	Server and endpoint management tools that support or automate management tasks like OS deployment, software inventory and distribution, patch management and configuration management. Usually is purchased as a software. Expected cost variations: EUR 5000 – 20000. Indicative product example: Windows Server Update Services (WSUS), ManageEngine Patch Manager.
20.	Vulnerability Management	Solutions that provide capabilities to identify, categorize and manage vulnerabilities. These include unsecure system configurations or missing patches, as well as other security-related updates in the systems connected to the enterprise network directly, remotely or in the cloud. Usually is purchased as a software. Expected cost variations: EUR 3000 – 50000. Alternative approach: cloud SaaS subscription. Indicative product example: Tenable Nessus, Qualys Vulnerability Management.
21.	Penetration Testing / Red Teaming	Authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. Usually is combined with vulnerability assessment. Usually is purchased as a consulting service. also, can be understood as purchasing dedicated tools / software. Expected cost variations for consulting: EUR 5000 – 30000.

No	Product/service group	Description
		Expected cost variations for software: EUR 5000 – 50000. Indicative product example: Metaspolit, Burpsuite. Open source: available.
22.	Wireless Security	Prevention of unauthorized access or damage to computers or data using wireless networks and hardware. Enables cyber situational visibility at wireless networks. Usually is purchased as an additional subscription-based software layer to network-related hardware implementing wireless networks (like routers). Expected cost variations: EUR 1000 – 50000. Indicative product example: Cisco DNA Software for Wireless.
23.	Remote Access / VPN	Extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection. Usually extends capabilities of core network devises or can be a separate hardware or software. Alternative approach: open source solutions. Expected cost variations: EUR 10000 – 50000. Indicative product example: Cisco Any connect, Fortinet FortiClient.
24.	IoT Security	Incident detection capability and cyber security situational awareness across and in IoT networks.

No	Product/service group	Description
		Usually is purchased as a software or an appliance (software with dedicated hardware) with deployment services. Expected cost variations: EUR 20000 – 100000. Indicative product example: CyberX, Claroty.
25.	PC/Mobile/End Point Security	Approach to the protection of computer networks that are remotely bridged to client devices. The connection of laptops, tablets, mobile phones, and other wireless devices to corporate networks creates attack paths for security threats. Endpoint security attempts to ensure that such devices follow a definite level of compliance to standards. Usually is purchased as a software or cloud SaaS for managing BYOD. Expected cost variations: EUR 10000-100000. Indicative product example: Microsoft BitLocker, Sophos SafeGuard, IBM MaaS360.
26.	Mobile Security /Device management	Administration of mobile devices, such as smartphones, tablet computers and laptops. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices. Usually is purchased as a software or cloud SaaS for managing BYOD. Expected cost variations: EUR 10000-100000. Indicative product example: Sophos SafeGuard, IBM MaaS360.
27.	Sandboxing	Used to execute untested or untrusted programs or code from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system.

No	Product/service group	Description
		Usually is purchased as a software or solution (software with dedicated hardware). Expected cost variations: EUR 5000-30000. Indicative product example: Cuckoo Sandbox, FortiSandbox. Open source: available.
28.	Content Filtering & Monitoring	Provides URL filtering, advanced threat defense and legacy malware protection to defend users from internet-borne threats, and to help enterprises enforce internet policy compliance. Sometimes named as Secure web gateways (SWGs). Usually is purchased a as on-premises appliances (hardware and virtual) or cloud-based services, or in hybrid mode (combined on-premises appliances and cloud-based services). Expected cost variations: EUR 10000-30000. Indicative product example: McAfee Web Gateway, Cisco Umbrella.
29.	Firewalls / NextGen Firewalls	Composed primarily of purpose-built appliances for securing enterprise corporate networks, although virtual appliances across public and private cloud and heavily virtualized data centers are becoming more important. Products in this segment must be able to support single-enterprise firewall deployments and large and/or complex deployments. These include traditional “big firewall” data center placements, branch offices, multi-tiered demilitarized zones, and, increasingly, virtual versions for the data center and various cloud environments. Usually is purchased a as on-premises appliances (hardware) or cloud-based services, or in hybrid

No	Product/service group	Description
		mode (combined on-premises appliances and cloud-based services). Expected cost variations: EUR 20000-150000. Indicative product example: Fortinet FortiGate, CheckPoint Next Generation Firewalls (NGFW).
30.	Unified Threat Management (UTM)	Approach to information security where a single hardware or software installation provides multiple security functions. This contrasts with the traditional method of having point solutions for each security function. UTM simplifies information-security management by providing a single management and reporting point for the security administrator rather than managing multiple products from different vendors. Usually is purchased a as on-premises appliances (hardware), but can be deployed as an application (software) too. Expected cost variations: EUR 5000-30000. Indicative product example: Sophos SG UTM, Juniper UTM.
31.	Anti-Spam	Prediction, prevention, detection and response framework used to provide general or targeted attack protection for email. Usually is purchased as a cloud SaaS, on premises software or solution (software with dedicated hardware). Expected cost variations: EUR 5000-30000. Indicative product example: Fortinet FortiMail, Microsoft Exchange Online Protection (EOP).

No	Product/service group	Description
32.	Anti-Virus/Worm/Malware	Solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts. Purchased as a software. Expected cost variations: EUR 15000-50000. Indicative product example: Symantec Endpoint Protection, ESET Endpoint Security.
33.	Backup / Storage Security	Backup and recovery software products provide features such as traditional backup to tape, backup to conventional random-access media (such as a hard disk or solid-state drives) or devices that emulate the previous backup targets (such as virtual tape library), data reduction (such as compression, deduplication or single instancing), array and/or server-based snapshot, heterogeneous replication, and continuous data protection. Usually is purchased as a solution (software with dedicated hardware). Expected cost variations: EUR 10000-30000. Indicative product example: Veeam Backup & Replication, Dell EMC Avamar.
34.	Fraud Management	Products or services that help an organization detect fraud that occurs over the web, mobile or other telephony channels (i.e., call center, interactive voice recognition. Other solutions detect online fraud as transactions and interactions occur, in real time or

No	Product/service group	Description
		near-real time. They provide solutions for web, mobile or telephony channels. Usually is purchased as a cloud-based SaaS. Expected cost variations: EUR 5000-20000. Indicative product example: Experian fraud shield.
35.	Intrusion Detection	Network intrusion detection and prevention system (IDPS) market is composed of stand-alone physical and virtual appliances that inspect defined network traffic either on-premises or in the cloud. They are often located in the network to inspect traffic that has passed through perimeter security devices, such as firewalls, secure Web gateways and secure email gateways. IDPS devices are deployed in-line and perform full-stream reassembly of network traffic. They provide detection via several methods. When deployed in-line, IDPSs can also use various techniques to detect and block attacks that are identified with high confidence. Usually is purchased a as on-premises appliances (hardware) or cloud-based services, or in hybrid mode (combined on-premises appliances and cloud SaaS). Expected cost variations: EUR 50000-200000. Indicative product example: Darktrace, FireEye Network Security (NX). Open source: available.
36.	SIEM / Event Correlation Solutions	Event data aggregation and analysis in real time for early detection of attacks (including targeted) and data breaches, and to collect, store, investigate and report on log data for incident response, forensics

No	Product/service group	Description
		and regulatory compliance. SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data, such as network telemetry. Event data is combined with contextual information about users, assets, threats and vulnerabilities. The data may be normalized, so that events, data and contextual information from disparate sources can be analysed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time analysis of events for security monitoring, query and long-range analytics for historical analysis. Usually is purchased a as on-premises appliances (hardware), software, or cloud SaaS. Expected cost variations: EUR 50000-200000. Indicative product example: IBM QRadar, Splunk, LogRhythm SIEM. Open source: available.
37.	Cyber Threat Intelligence	Threat intelligence is evidence-based knowledge - including context, mechanisms, indicators, implications and actionable advice - about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard. Usually is purchased as a software or cloud SaaS subscription. Expected cost variations: EUR 10000-50000.

No	Product/service group	Description
		Indicative product example: Recorded Future Intelligence Services, Anomali Threat Platform.
38.	Security Operations Center (SOC)	Incident detection establishment and management services covering broad range for organisation's assets, like network, applications, servers, endpoints and data. Usually is deployed with technology, integration services and intensive trainings. Can be outsourced. Usually is purchased as managed security service provider (MSSP) services. Alternative approach: establish on premises by purchasing associated consulting services. Expected cost variations: EUR 100000-400000.
39.	Underground/Darkweb investigation	Darkweb monitoring platforms, combine intelligence with search capabilities to identify, analyse and proactively monitor for an organization's compromised or stolen employee and customer data. Usually, can be a part of Cyber Threat Intelligence products category. Usually is purchased as a cloud SaaS subscription. Expected cost variations: EUR 5000-20000. Indicative product example: DarkOwl Vision, Network box dark web monitoring.
40.	Honeypots / Cybertraps	Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Usually is purchased as on-premises appliances (hardware) or software. Expected cost variations: EUR 1000-10000.

No	Product/service group	Description
		Indicative product example: Thinkst Canary. Open source: available.
41.	Social Media & Brand Monitoring	Defined as online reputation management. It focuses on the management of product and service search results within the digital space. Usually is purchased as a cloud SaaS subscription. Expected cost variations: EUR 5000-20000. Indicative product example: Brandwatch, Brand24.
42.	Incident Management	Check categories: Services (CSRIT aaS) Incident Response; Forensics.
43.	Crisis Management	Solutions that help organizations consistently orchestrate and manage the data, resources, expenditures, communications and tasks used for response, recovery and restoration activities during and after a crisis. Such solutions securely store and share emergency operating procedures and response plans used by facility staff and first responders to effectively prepare for, respond to and recover from any emergency. Is used in wider context than cybersecurity only. Usually is purchased as a solution with deployment services. Expected cost variations: EUR 100000-250000. Indicative product example: Rapid Responder.
44.	Crisis Communication	Check category: Crisis Management.
45.	Fraud Investigation	Check category: Forensics.
46.	Forensics	Refer to a set of advisory services and/or solutions that help clients collecting digital evidence (during or after an incident) in a forensically sound manner, to be used as part of an investigation.

No	Product/service group	Description
		Usually is purchased as a service. Expected cost variations: EUR 10000-50000. Indicative product example: Secureworks Digital Forensic Investigation Services, NCC Digital Forensics & Incident Response. Alternative approach: establish digital forensics lab. Expected cost variations: EUR 100000-800000. Indicative product example: EnCase Forensic Software, FTK, Oxygen Forensic Suite.
47.	Takedown services	Check category: Services (CSRIT aaS) Incident Response.
48.	Services (CSRIT aaS) Incident Response	Understood as a part of managed security services (MSS) or managed detection and response (MDR). MSS/MDR is defined as the remote monitoring or management of IT security functions delivered via shared services from remote security operations centers. MSSs/MDRs include monitored/managed firewalls or intrusion prevention/detection systems; managed multifunction firewalls; unified threat management technology; managed security gateways for messaging or web traffic; security analysis and reporting of events collected from IT infrastructure logs; reporting associated with monitored/managed devices and incident response; managed vulnerability scanning of networks, servers, databases or applications; distributed denial of service protection; monitoring/management of customer-deployed security information, event management technologies; and monitoring/management of advanced threat defense technologies, or the provision of those capabilities as a service.

No	Product/service group	Description
		Usually is purchased as a medium-long term subscription service. Expected cost variations: EUR 100000-400000. Indicative service example: IBM MDR, NCC MDR.
49.	Data Recovery	Check category: Backup / Storage Security.
50.	DDoS Protection	Includes vendors that deliver services for detecting and mitigating DDoS attacks. Usually is purchased as a cloud SaaS service. Alternative approach: purchasing dedicated solution on premise. Expected cost variations: EUR 5000-50000. Indicative service example: Cloudflare DDoS mitigation services, Akamai DDoS protection.
51.	Cyber Security Insurance	Insurance product intended to protect businesses, and individuals providing services for such businesses, from Internet-based risks, and more generally from risks relating to information technology infrastructure, information privacy, information governance liability, and activities related thereto. Usually is purchased as a sub-item to broader insurance policy. Expected cost variations: EUR 1000-10000. Indicative service example: AIG Cyber Insurance for Businesses, Allianz Cyber Insurance.
52.	Business Continuity/ Recovery Planning	Software-integrated infrastructure that applies a modular approach to compute, network and storage on standard hardware, leveraging distributed, horizontal building blocks under unified management. Vendors either build their own

No	Product/service group	Description
		appliances using common, off-the-shelf infrastructure (hardware, virtualization, operating system), or they engage with systems vendors that package infrastructure vendor's software stack as an appliance. Usually is purchased as a dedicated solution (hardware and software. Alternative approach: utilizing public cloud services / hybrid cloud. Expected cost variations: EUR 200000-800000. Indicative product example: HPE SimpliVity, Dell EMC VxRail.
53.	System Recovery	Check category: Business Continuity/ Recovery Planning.

Annex C: Guide to using the ICRI tool

To extract and quantity the cybersecurity component from the total investment value, the ICRI tool was developed to assist EIB investment officers in actual calculations. This Annex presents a step-by-step guide how to use this tool.

Step 1 – Select Project

- Provide information related to the project such as the Project name, Reference ID, Release date, Project Promoter, Total project cost, and the portion of the project cost that was financed by the EIB, and finally a link to the project if available.

Step 2 – Is ICT Component present?

- Select "Yes" from the dropdown menu if it is known or can be judged that the project has some Information and Communication Technology (ICT) components. ICT covers all technical means used to access, store, transmit, and manipulate information. This includes telecommunication equipment, computers, network hardware, as well as their software.
- Select "No" if it is known or can be judged that there are no ICT components in the project.

  NOTE: Construction of roads or railroads, energy grid extension, etc. are projects that may typically not include ICT components.

Step 3 – Is ICT component value known?

- If in Step 2 it is established that there is an ICT component in the project, select "Yes" if the specific investment within ICT in the project is known. Fill in the total ICT budget and the EIB financed ICT budget in the subsequent fields.
- However, if the specific ICT investment is unknown then select "No" and skip the subsequent fields for the total ICT budget and the EIB financed ICT budget. The drop-down field "investment in the ICT intensity ratio as a part of total investment" has 5 values ranging from Very Low to Very High. Select the appropriate ICT intensity level based on the guidance presented below. Once the intensity is chosen, it will automatically generate an appropriate "Investment in ICT intensity multiplier value" in the next field.

Intensity	When to apply?
Very low	Field / industrial works with indirect exposure to ICT. Best fitting for construction projects related to transportation (rail, roads, ports), pipelines, chemicals, etc.
Low	Activities with limited exposure to ICT. Best fitting industries: construction (like houses, industrial buildings), industrial manufacturing, transportation (other than construction), energy.
Medium (standard)	Average. Direct or indirect exposure to ICT in project as a part of project activities. Best fitting industries: government, utilities.
High	Activities with direct exposure to ICT. Best fitting industries: telecommunications, insurance, healthcare.
Very high	Projects with heavy exposure to ICT, related to digitalization and/or automation, productivity, and effectiveness enhancement as a dedicated part of project activities. Best fitting industries: financial services (excluding financing/ refinancing activities).

Step 4 – Project investment into cybersecurity

NOTE: In Step 3, for "Is ICT component value known?", if the selected value is "Yes" then the sheet automatically loads Step 4A which calculates the cybersecurity investment as a % of ICT budget. If the selected value is "No" then the sheet loads Step 4B which calculates the cybersecurity investment as a % from the total EIB investment into project.

(Either) Step 4A – Project investment into cybersecurity will be calculated as: % from project's ICT budget

- Select the country in which the project is being implemented.
- A standard "Applied default index value" of 4.14% is used for all countries within EU. This index is calculated from using data on the size of the cybersecurity products and services market in EU compared to the total ICT market size in EU.

- Based on the total ICT budget and the EIB financed part that was mentioned in Step 3, and the "Applied default index value", the corresponding Cybersecurity budget is estimated in the fields.

(Or) Step 4B – Project investment into cybersecurity will be calculated as: generalised statistical % from total EIB investment into project

- Select the country in which the project is being implemented.
- An "Applied default index value" is generated based on the selected country. This value differs from one country to another and is calculated based on a country's Gross fixed capital formation (GFCF) in ICT.
- Based on the total Project Cost and the EIB financed part of this in Step 1, and the "Applied default index value", the corresponding Cybersecurity budget is estimated in the fields.

Step 5 – Apply country's cybersecurity development multiplier for calculated cybersecurity budget

NOTE: In this step, the cybersecurity budget within a project that is estimated in Step 4 is further adjusted based on the cybersecurity maturity (as per the ITU Global Cybersecurity Index, 2018) of the country where the project is implemented.

- Select the country where the project is implemented under "Source for multiplier selection".
- Based on the selection, a "Normalised multiplier value used for calculation" is automatically generated. This multiplier either reduces or boosts the estimated cybersecurity spending in a project based on the cybersecurity maturity of a country as per the ITU Global Cybersecurity Index. The updated cybersecurity budget is presented in the fields.

Step 6 – Apply sector's cyber-threat exposure multiplier for calculated cybersecurity budget

NOTE: A sector's cyber-threat exposure multiplier value is calculated using data from a Gartner Report that provides IT Security spending as a percentage of total IT spending for different sectors. Higher the threat-exposure, higher the investment within cybersecurity and therefore higher the value for the multiplier.

- Select the most appropriate sector for the project from the drop-down list. The list includes sectors such as Telecom, Energy, Solid Waste, Services, Health, Education, Agriculture, etc.
- Based on the selected sector, a "Normalised multiplier value used for calculation" is automatically generated based on a sector's exposure to cyber-threats.
- Further adjusted cybersecurity budgets are presented in the fields.

Step 7 – Is it a new investment potential?

NOTE: This step has been introduced to guide EIB investment officers in the process of reviewing new investment projects. When ICRI is used for new investment projects, it can provide an estimate on the cybersecurity investment that can be expected based on the specified project parameters (such as investment size, country of investment, sector, etc.) which the investment officers can use to guide the dialogue with project promoters to understand if investments within cybersecurity are adequate or can be further boosted.

- Select "Yes" or "No" from the dropdown-menu to differentiate between a new investment and a completed ESI investment. The estimated cybersecurity investment will be fine-tuned further in the next Step for new investments which are expected to comply with emerging EU cybersecurity policies and enforce higher cybersecurity standards, particularly in NIS sectors.

Step 8 – Apply quantified NISD value to investment potential

- If in Step 7 the investment is classified as a new investment potential with a "Yes", in Step 8 select the closest sector to which the investment belongs and a "Sector's criticality multiplier (NISD) to be applied for new investment potential" is automatically used to adjust (boost) the estimated cybersecurity investment if it is in one of the critical sectors covered under the NIS Directive (NISD).

Step 9 – Adjusted to context project specific cybersecurity investment

NOTE: ICRI does not account for spending on human labour within the cybersecurity in projects in its estimates. In specific cases, the EIB considers these investment costs as being eligible under their financing guidelines. The "*Human Labour costs within cybersecurity*" field has therefore been introduced to capture the costs for human

labour within cybersecurity that the EIB has agreed to finance as part of the agreement with Project Promoters.

(Optional and used on a case-by-case basis) Step 9A – Human Labour costs within cybersecurity (cybersecurity innovation cost)

- Specify the Human Labour costs within cybersecurity. This value is project specific and the EIB Staff/investment officer will need to have prior knowledge of it. Not all projects finance human labour costs. Therefore, this field is optional, only used on a case-by-case basis and the field must be filled manually with the exact investment made towards human labour within cybersecurity.

The final, adjusted and project-context specific cybersecurity investment is presented in Step 9B, including the EIB share of this investment for ESI reporting.

Annex D: Guide to updating the ICRI tool

This annex is a brief guide on how the ICRI tool should be updated when new statistical data is released.

Updating ICT and cybersecurity percentages based on investment_in_GFCF

To extract the estimated ICT investment value, when only total project investment value is known, OECD published data on ICT investment percentage in GFCF is used. "ICT_investment_in_GFCF" sheet within the excel document (ICRI) must be selected to update relevant data:

a) National ICT investment % in GFCF must be extracted from the OECD website and written to the table, replacing previous national investment percentage value. The actual table with OECD field names and values is present in Figure 11. ICT% in GFCF data table

b)

Original data : ICT % in GFCF

LOCATION	INDICATOR	SUBJECT	MEASURE	FREQUENCY	TIME	Value
FIN	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	8.398430058
GRC	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2015	15.08183995
DNK	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2016	13.33869207
LUX	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	8.85867495
ESP	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	13.45197797
SVN	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	10.59091629
SVK	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	4.792642211
EST	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2015	8.520854633
AUT	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	14.47470889
PRT	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	11.97639254
IRL	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2016	4.085970953
NLD	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	18.0560974
HUN	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	7.338099791
CZE	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	16.00148127
FRA	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	16.12363013
ITA	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	12.33752095
SWE	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	18.66095653
LVA	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2016	8.228142036
LTU	GFCFASSET	OTHMACHINEQT	PC_GFCF	A	2017	14.84509329

Figure 11. ICT% in GFCF data table

c) Cybersecurity investment % is calculated as a proportion of EU's Cybersecurity market size to EU's ICT market size. EU ICT market size is published as part of the PREDICT data set. Dataset has to be downloaded and data filtered out by filter: "Unit" as "Millions of current euros", "countrycode" as "EU",

"Description" as "A. ICT Total (A=B+SER), "year" – as a year, for which the EU Cybersecurity market size is available.

variablecode	unit	dataset_type	countrycod	country	classification	classificationcode	definition	sectorcode	description	year	value
BERDEUR	Millions of current euros	PREDICT 2019 Dataset	EU	European Union	NACE Rev.2.	261-264, 268, 465, 582, 61, 62, 631, 951	a) ICT sector (comprehensive definition)	A=B+SER	A. ICT Total [A=B+SER]	2015	31537.01
GOEUR	Millions of current euros	PREDICT 2019 Dataset	EU	European Union	NACE Rev.2.	261-264, 268, 465, 582, 61, 62, 631, 951	a) ICT sector (comprehensive definition)	A=B+SER	A. ICT Total [A=B+SER]	2015	1315255.217
GVAEUR	Millions of current euros	PREDICT 2019 Dataset	EU	European Union	NACE Rev.2.	261-264, 268, 465, 582, 61, 62, 631, 951	a) ICT sector (comprehensive definition)	A=B+SER	A. ICT Total [A=B+SER]	2015	628574.9255

Figure 12. PREDICT dataset, filtered to total ICT value in 2015

Actual multiplier used in calculations is calculated in Column "Cyber to GFCF ratio".

Updating ICT_Intensity multipliers

ICT intensity multipliers are calculated using Gartner IT Key Metrics Data 2018 [GARKMD] report. The table "IT spending as a percentage of Operating Expense by Industry for Midsize Enterprise" is used in establishing the IT spending percentages for each sector. These values are then used in the excel formula "QUARTILE.INC" to calculate 5 quartiles to be used as five intensity adjustment multipliers. Actual data and formula are present in Figure 13. ICT intensity values calculation. This Gartner report is published in regular periods. When more recent IT Key Metrics Data is available, they can replace the data from 2018 that is used in this methodology.

Function Library Defi

=QUARTILE.INC($C$18:$C$38, 1)

	IDX value (deviation from standard value)	Quartiles
Very low	0.32	1.5
Low	0.53	2.5
Medium (standard)	1	4.7
High	1.26	5.9
Very high	2.45	11.5
Not applicable	-	

Figure 13. ICT intensity values calculation

Updating cybersecurity development multiplier

Every country's cybersecurity development index is published by ITU in the "Global Cybersecurity Index" report. The EU27 average development index is calculated from this. A country's cybersecurity development value proportional to the EU27 average development index is used to develop the cybersecurity development multiplier.

To update data, a more recent ITU report must be reviewed, when available, and the EU27 cybersecurity development index should be updated in the "ITU_development" sheet of the excel document (ICRI).

Updating sectorial cybersecurity multipliers

Sectorial cybersecurity multipliers are calculated in the sheet "Sectorial_cyber_multipliers" of the excel document (ICRI) as a proportion of specific sector values to the cross-industry average. The "Sectorial cybersecurity spending representation as a percentage from ICT spending" table from Gartner IT Key Metrics Data report is used for this multiplier. Gartner's economic activity sectors are mapped into EU's economic activity classifier NACE2. For the sectorial cybersecurity multiplier, sectorial spending to the cross-industry average is calculated for each sector for which sectorial data is available. Where sectoral spending data is not available, cross-industry average is used for this multiplier.