



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# NIS INVESTMENTS 2025

Survey data companion document

DECEMBER 2025

# About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: [www.enisa.europa.eu](http://www.enisa.europa.eu).

## CONTACT

To contact the authors, please send an email to [nis360@enisa.europa.eu](mailto:nis360@enisa.europa.eu).  
For media enquiries about this report, please email [press@enisa.europa.eu](mailto:press@enisa.europa.eu).

## AUTHORS

Eleni Philippou, Ugne Komzaite-Kraujale, Jurgita Skritaite, ENISA

## ACKNOWLEDGEMENTS

The authors would like to thank the following contributors for the insights, feedback, and value they have provided to this effort: Patrick Abel, François Gratiolet, Edwin Maaskant, Gartner, members of the NIS Cooperation Group, NLOs Group, and colleagues from the European Commission and ENISA.

## LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

## COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025

This publication is licenced under CC-BY 4.0 “Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated”. Copyright for the image on the cover © ShutterstockFor any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-776-4, DOI 10.2824/6446718

# Table of Contents

<b>About ENISA</b>	<b>1</b>
<b>1. About this document</b>	<b>5</b>
<b>2. Member State view</b>	<b>7</b>
2.1 IT spending	7
2.2 IT spending as a share of revenues	8
2.3 IS spending	9
2.4 Outcomes attained via cybersecurity investment in 2024	10
2.5 Key cybersecurity investment drivers for 2024	10
2.6 Targeted outcomes of cybersecurity investment in the coming year	11
2.7 IT FTEs	13
2.8 IS FTEs	14
2.9 IS FTEs as a share of IT FTEs	15
2.10 Proportion of women in IS FTEs	16
2.11 Challenges to attracting cybersecurity talent	17
2.12 Challenges to retaining cybersecurity personnel	18
2.13 Cybersecurity staffing strategy	19
2.14 Cost reduction measures affecting cybersecurity staffing	20
2.15 Most in-demand cybersecurity skills currently	21
2.16 Most challenging NIS2 requirements to implement	22
2.17 Main obstacle to implementing NIS2 requirements	23
2.18 Cybersecurity assessments	24
2.19 Average time to patch critical vulnerabilities on critical systems	25
2.20 Supply chain risk management practices implemented	26
2.21 Characteristics of preferred suppliers of digital products	27
2.22 Information Sharing	28
2.23 Attacks with the greatest operational impact on day-to-day operations	29
2.24 Cybersecurity threats of most concern looking ahead	30
2.25 Preparedness against scenarios	31
<b>3. Sector view</b>	<b>35</b>

<b>3.1</b>	<b>IT spending</b>	<b>35</b>
<b>3.2</b>	<b>IT spending as a share of revenues</b>	<b>36</b>
<b>3.3</b>	<b>IS spending</b>	<b>37</b>
<b>3.4</b>	<b>IS spending as a share of IT spending</b>	<b>38</b>
<b>3.5</b>	<b>Outcomes attained via cybersecurity investment in 2024</b>	<b>39</b>
<b>3.6</b>	<b>Key cybersecurity investment drivers for 2024</b>	<b>40</b>
<b>3.7</b>	<b>Targeted outcomes of cybersecurity investment in the coming year</b>	<b>41</b>
<b>3.8</b>	<b>IT FTEs</b>	<b>42</b>
<b>3.9</b>	<b>IS FTEs</b>	<b>43</b>
<b>3.10</b>	<b>IS FTEs as a share of IT FTEs</b>	<b>44</b>
<b>3.11</b>	<b>Proportion of women in IS FTEs</b>	<b>45</b>
<b>3.12</b>	<b>Challenges to attracting cybersecurity talent</b>	<b>46</b>
<b>3.13</b>	<b>Challenges to retaining cybersecurity personnel</b>	<b>47</b>
<b>3.14</b>	<b>Cybersecurity staffing strategy</b>	<b>48</b>
<b>3.15</b>	<b>Cost reduction measures affecting cybersecurity staffing</b>	<b>49</b>
<b>3.16</b>	<b>Most in-demand cybersecurity skills currently</b>	<b>50</b>
<b>3.17</b>	<b>Most challenging NIS2 requirements to implement</b>	<b>51</b>
<b>3.18</b>	<b>Main obstacles to implementing NIS2 requirements</b>	<b>53</b>
<b>3.19</b>	<b>Cybersecurity assessments</b>	<b>55</b>
<b>3.20</b>	<b>Average time to patch critical vulnerabilities on critical systems</b>	<b>56</b>
<b>3.21</b>	<b>Supply chain risk management practices implemented</b>	<b>58</b>
<b>3.22</b>	<b>Characteristics of preferred suppliers of digital products</b>	<b>59</b>
<b>3.23</b>	<b>Information Sharing</b>	<b>60</b>
<b>3.24</b>	<b>Attacks with the greatest operational impact on day-to-day operations</b>	<b>61</b>
<b>3.25</b>	<b>Cybersecurity threats of most concern looking ahead</b>	<b>62</b>
<b>3.26</b>	<b>Preparedness against scenarios</b>	<b>63</b>
<b>4.</b>	<b>Survey demographics</b>	<b>67</b>
<b>5.</b>	<b>Definitions</b>	<b>71</b>
<b>5.1</b>	<b>Median and average definitions</b>	<b>71</b>
<b>5.2</b>	<b>SME definition</b>	<b>71</b>

## SECTION 1

# About this document

# 1. About this document

This companion document accompanies the main NIS Investments 2025 report and presents **all responses collected through the study's survey**. It is designed to complement the report's analytical findings by providing a detailed, visual overview of the underlying data.

Through a series of charts, this companion document enables readers to explore **how the broader insights highlighted in the main report manifest across the organisations surveyed** — both within individual **Member States** and across the **different sectors** covered by the study.

By offering this level of granularity, this document allows readers to **examine patterns and variations** in cybersecurity practices, challenges, and levels of preparedness in greater depth. It is intended as a resource for policymakers, regulators, and practitioners seeking to better understand the context behind the study's findings and to support evidence-based decision-making

## SECTION 2

# Member State view

## 2. Member State view

### 2.1 IT spending

**Survey Question:** What was your organisation's estimated IT budget or spending in Euros for 2024 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

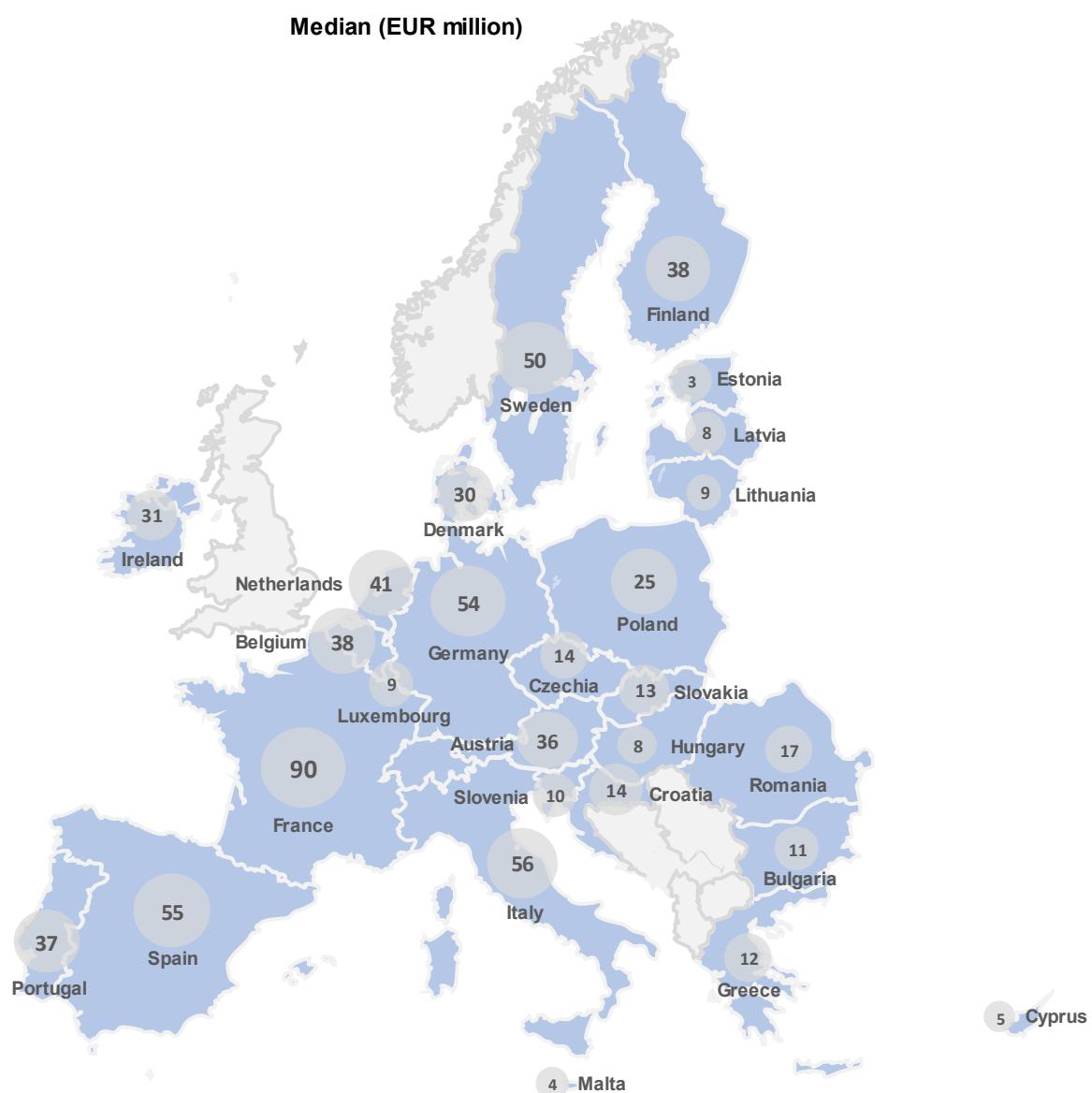


Figure 1 - IT spending per Member State (median values)

## 2.2 IT spending as a share of revenues

**Calculated field:** This metric is a calculated field that expresses the proportion (or percentage) of an organisation's revenue that is allocated to IT.

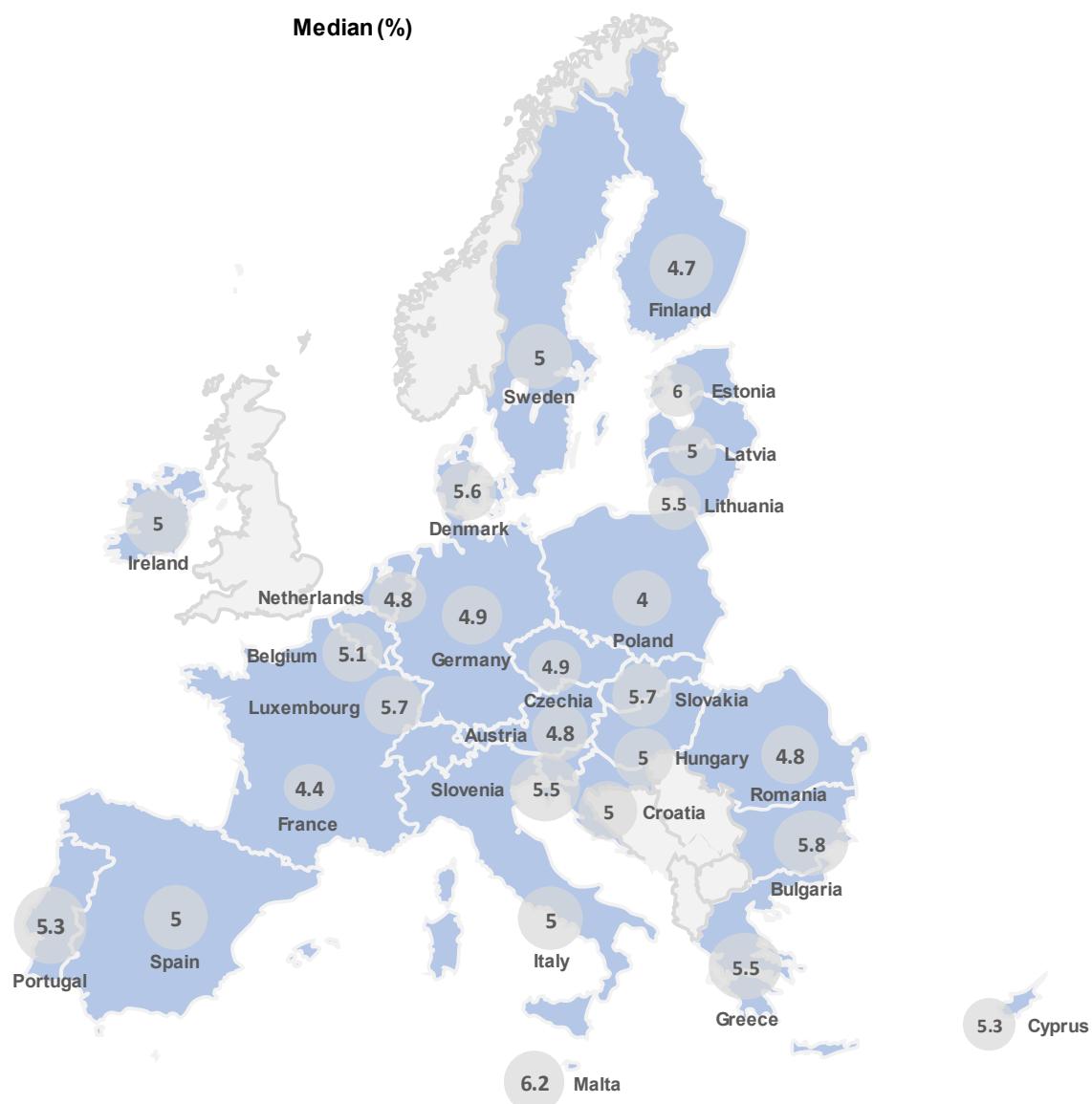
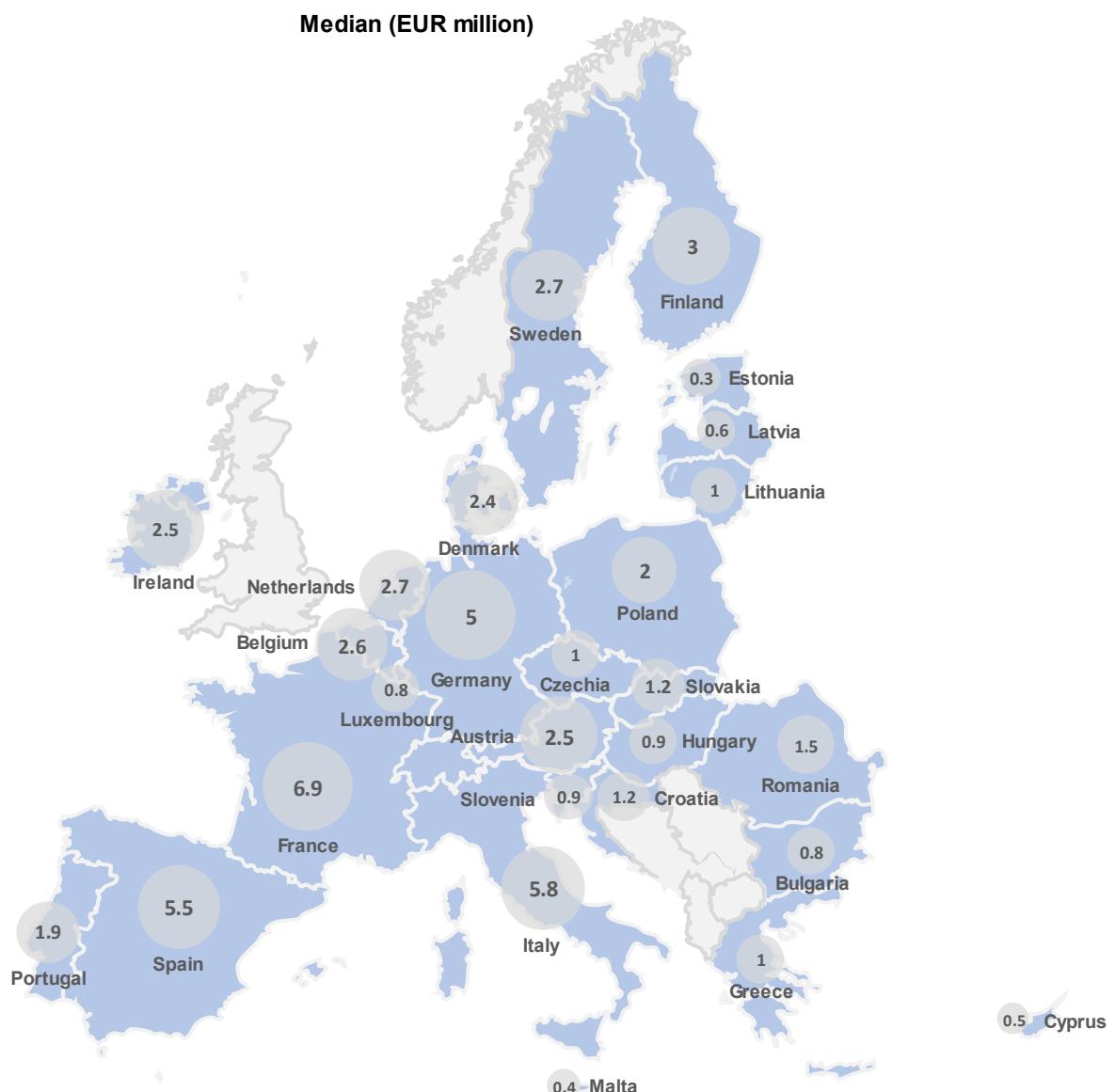


Figure 2 - IT spending as a share of revenues

## 2.3 IS spending

**Survey Question:** What was your organisation's estimated Information Security budget or spending in Euros for 2024 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

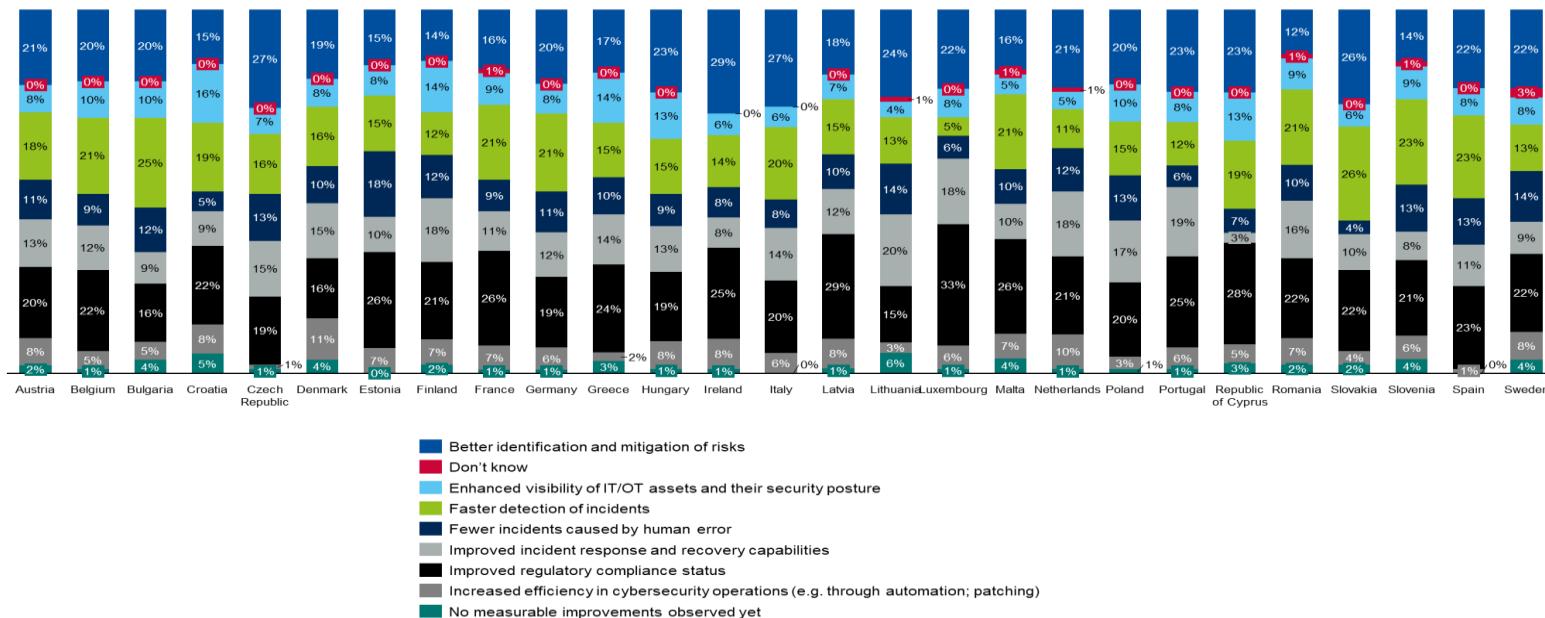


*Figure 3 - IS spending per Member State (median values)*

## 2.4 Outcomes attained via cybersecurity investment in 2024

**Survey Question:** Which of the following outcomes has your organisation achieved as a result of its cybersecurity investments in the past year?  
 (Select up to three)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

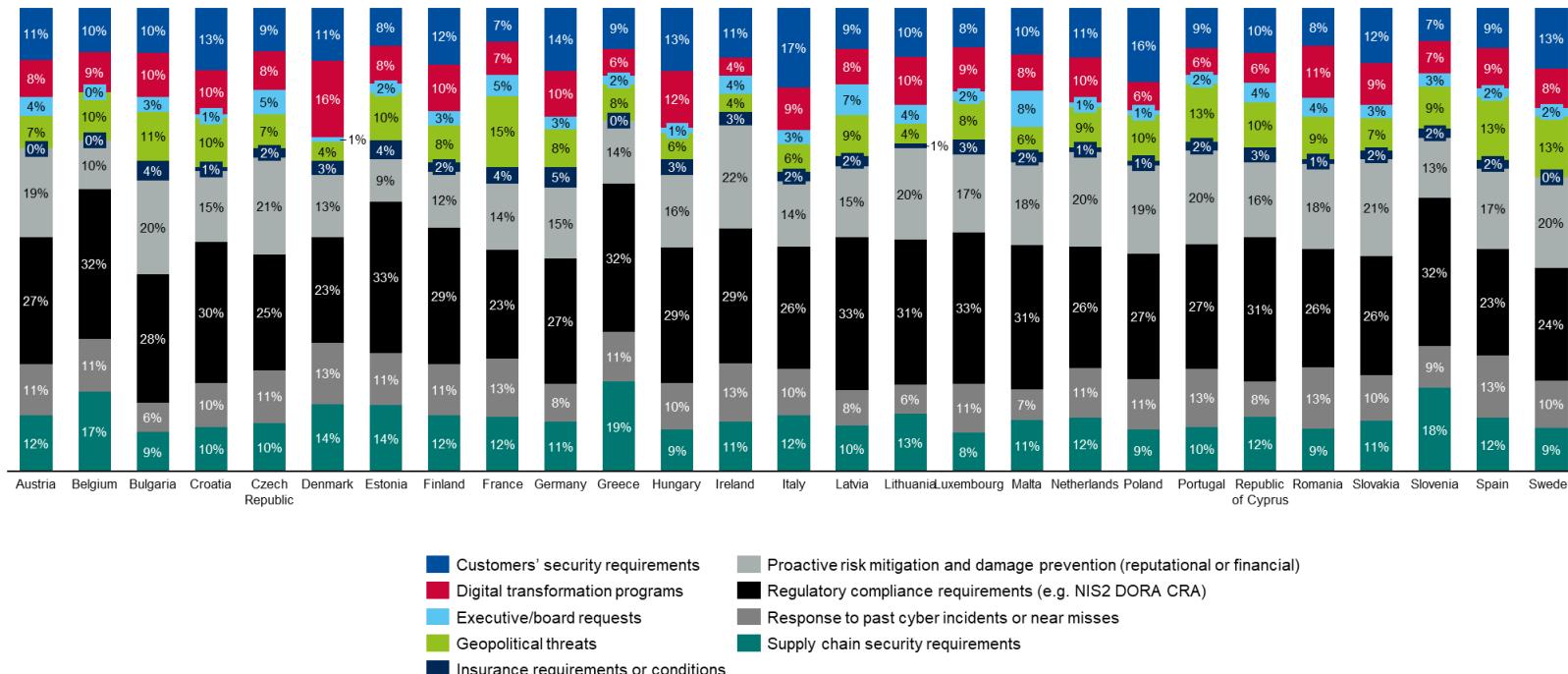


**Figure 4 - Outcomes attained via cybersecurity investment in 2024, per Member State**

## 2.5 Key cybersecurity investment drivers for 2024

**Survey Question:** In the past year, which of the following has most significantly driven cybersecurity investment in your organisation? (Select up to 3)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

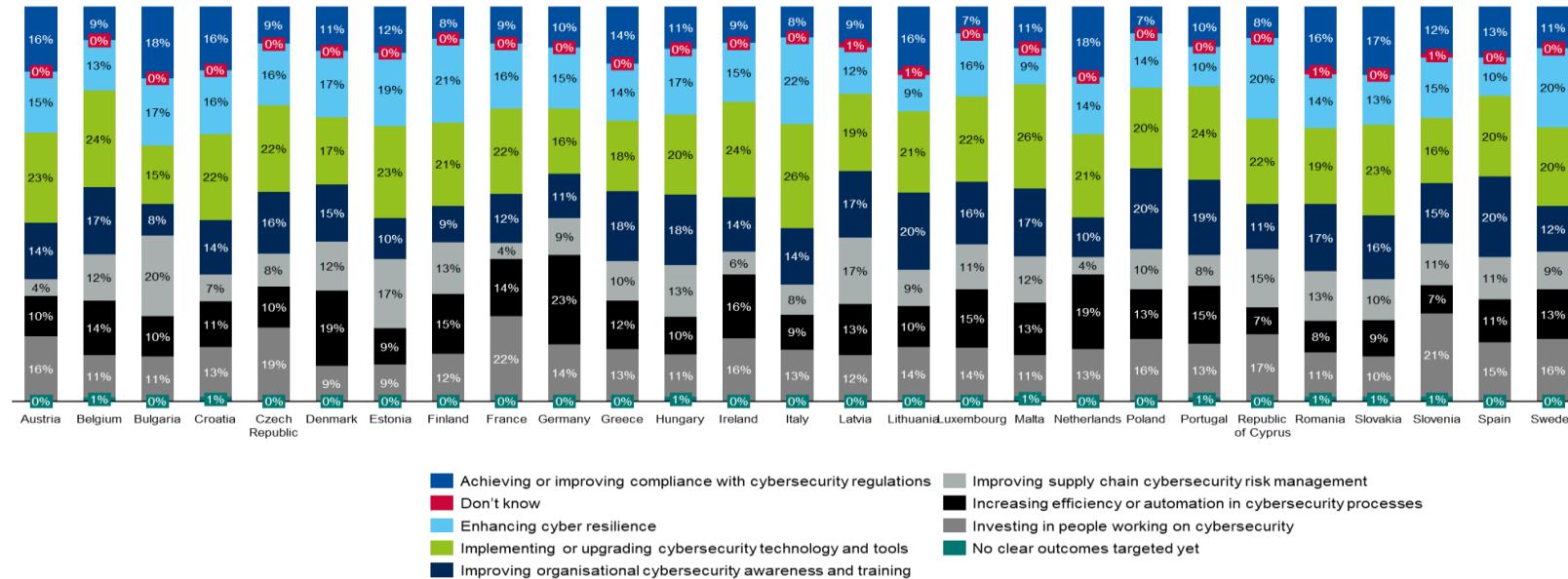


**Figure 5 - Key cybersecurity investment drivers for 2024, per Member State**

## 2.6 Targeted outcomes of cybersecurity investment in the coming year

**Survey Question:** Which of the following outcomes are you primarily targeting with your cybersecurity investments in the coming year? (Select up to three)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.



**Figure 6 - Targeted outcomes of cybersecurity investment in the coming year, per Member State**

## 2.7 IT FTEs

**Survey Question:** What was your organisation's estimated number of IT FTEs for 2024 including internal staff and contractors?



Figure 7 - IT FTEs per Member State (median values)

## 2.8 IS FTEs

**Survey Question:** What was your organisation's estimated number of Information Security FTEs for 2024 including internal staff and contractors?



Figure 8 - IS FTEs per Member State (median values)

## 2.9 IS FTEs as a share of IT FTEs

**Calculated field:** This metric is a calculated field that expresses the proportion (or percentage) of an organisation's IS FTEs over IT FTEs.

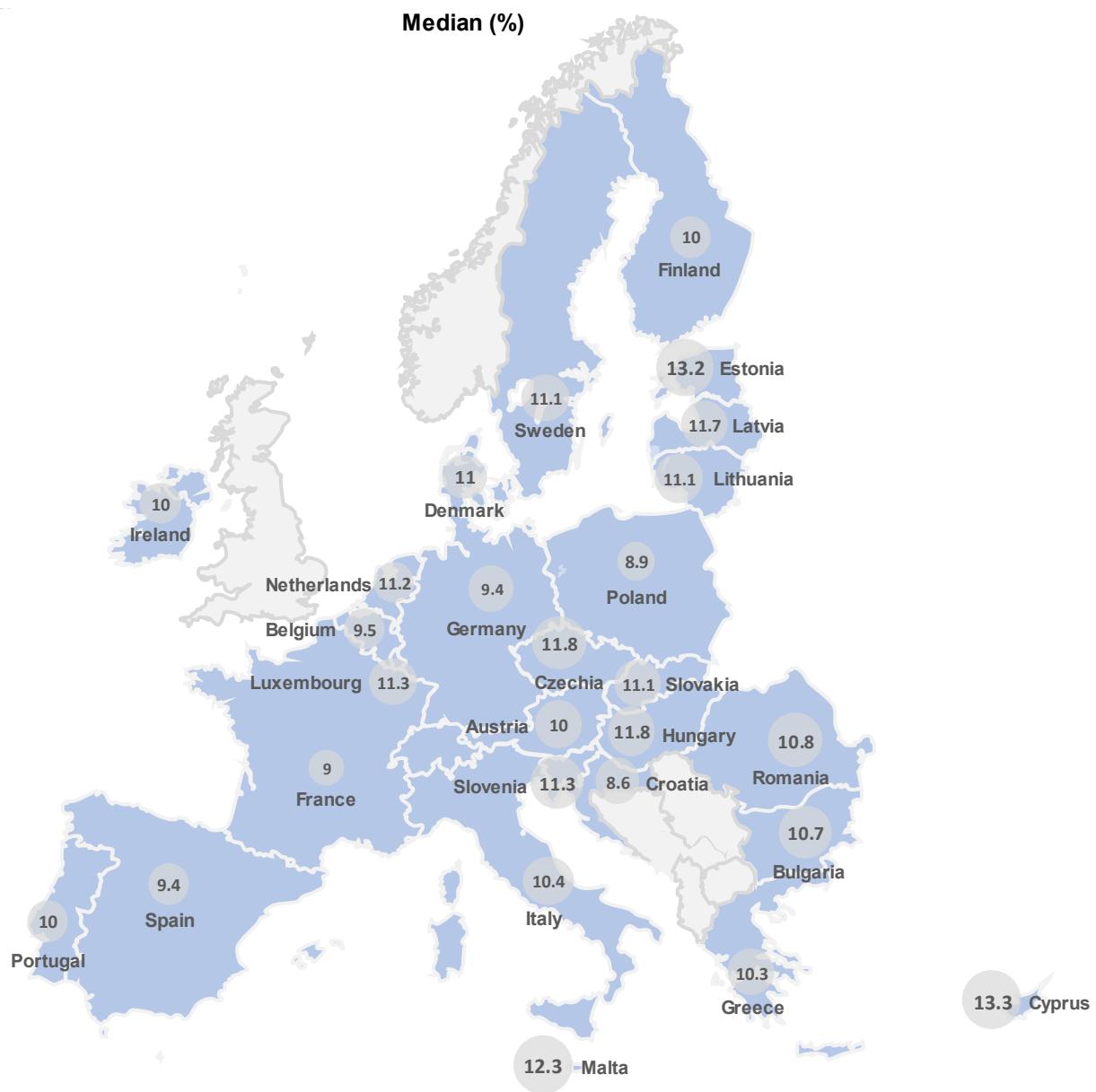
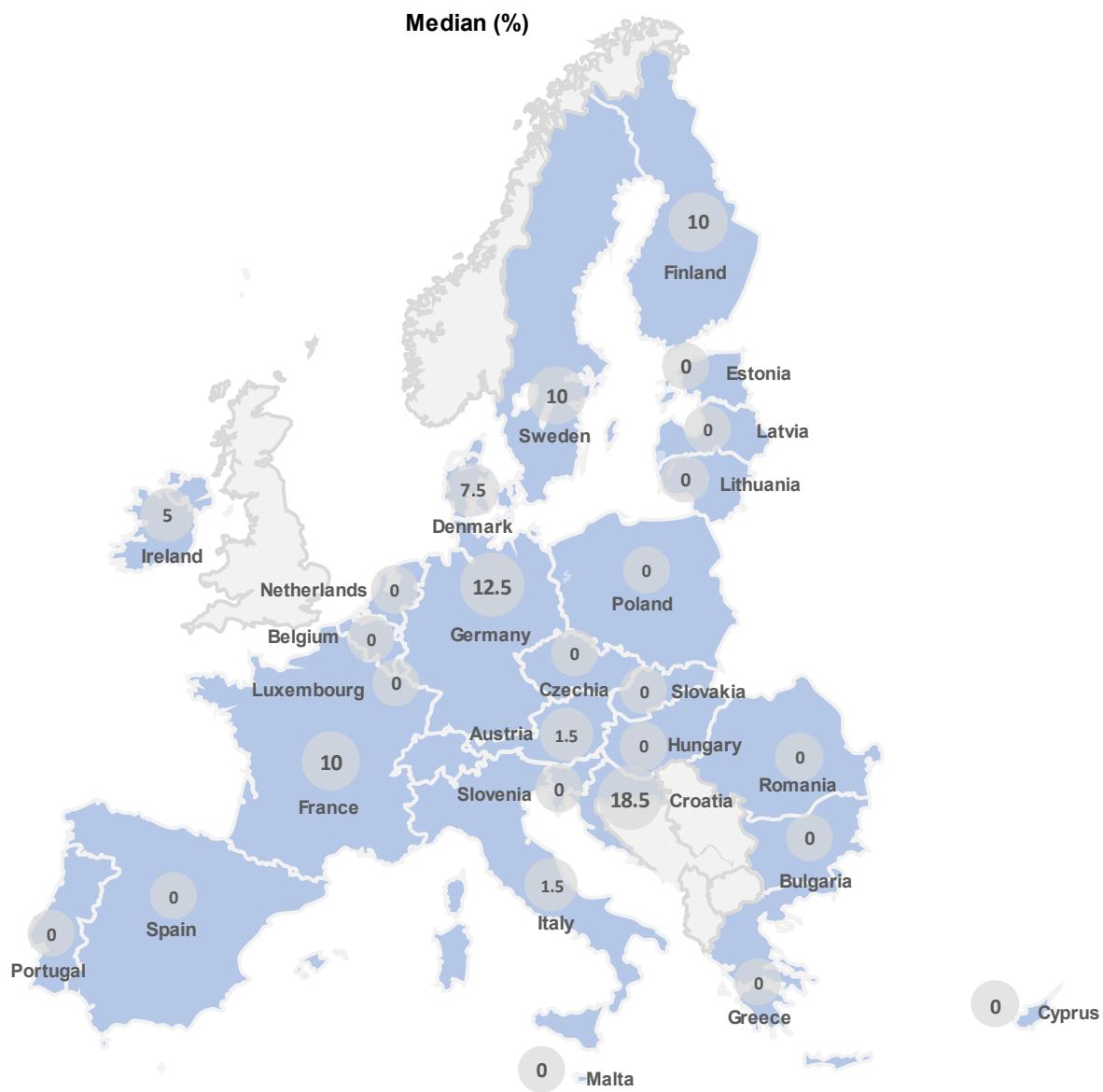


Figure 9 - IS FTEs as a share of IT FTEs per Member State (median values)

## 2.10 Proportion of women in IS FTEs

**Survey Question:** Please share what percentage of your IS FTEs are women?



**Figure 10 - Proportion of women in IS FTEs (median values)**

## 2.11 Challenges to attracting cybersecurity talent

**Survey Question:** Which barriers does your organisation face in attracting cybersecurity personnel? (Select up to three)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

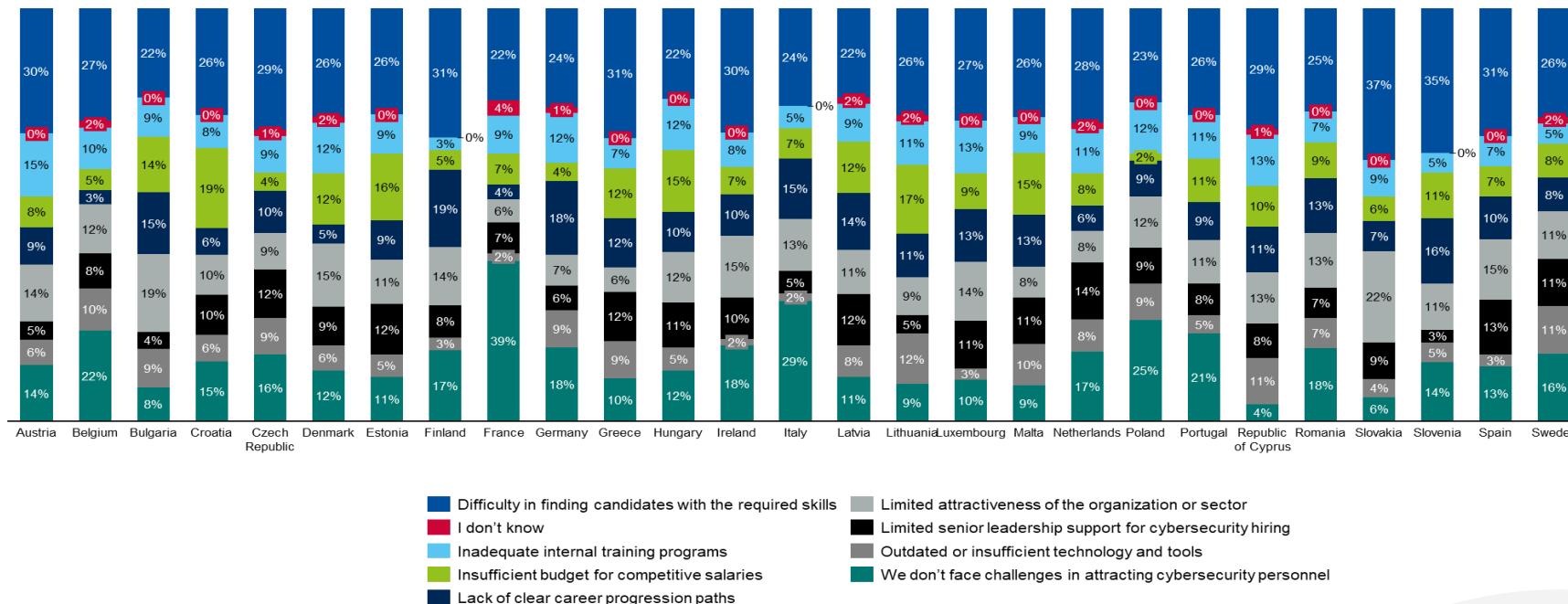


Figure 11 - Challenges to attracting cybersecurity talent, per Member State

## 2.12 Challenges to retaining cybersecurity personnel

**Survey Question:** What are the main challenges your organisation faces in retaining cybersecurity personnel? (Select up to three)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

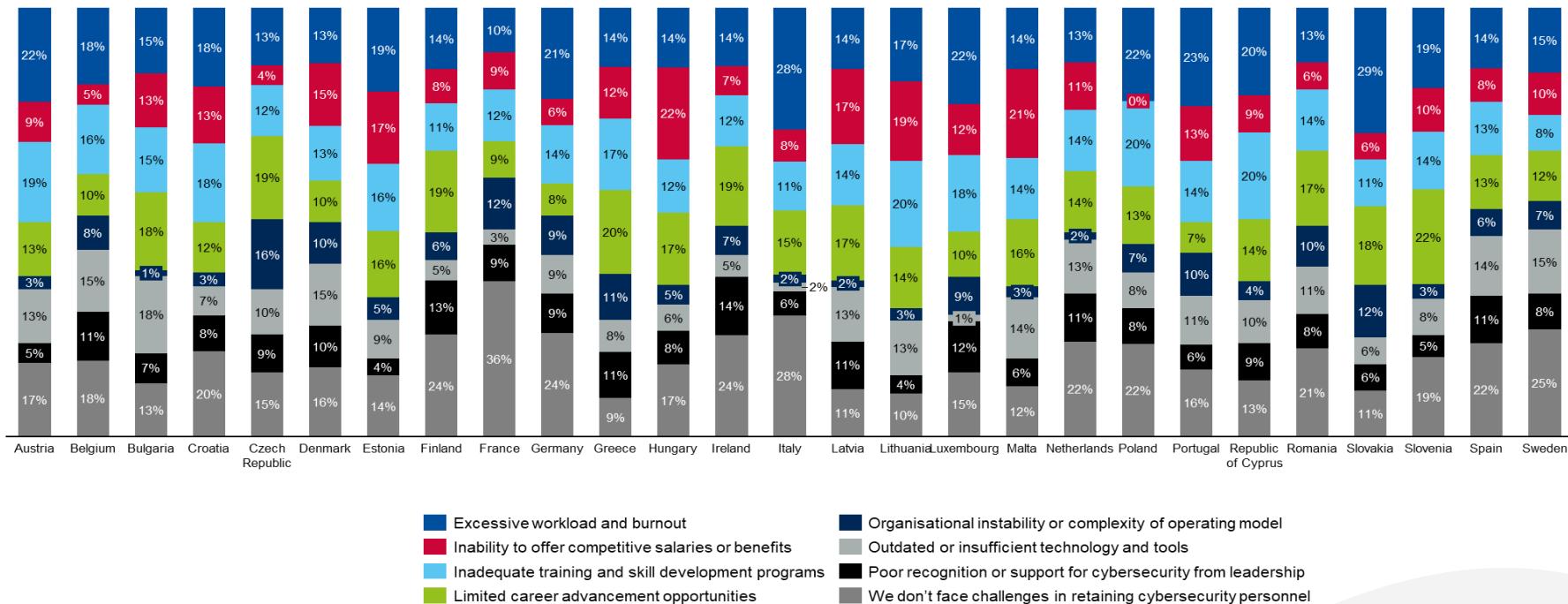


Figure 12 - Challenges to retaining cybersecurity personnel, per Member State

## 2.13 Cybersecurity staffing strategy

**Survey Question:** What best describes your organisation's cybersecurity staffing plan for the next 12 months?

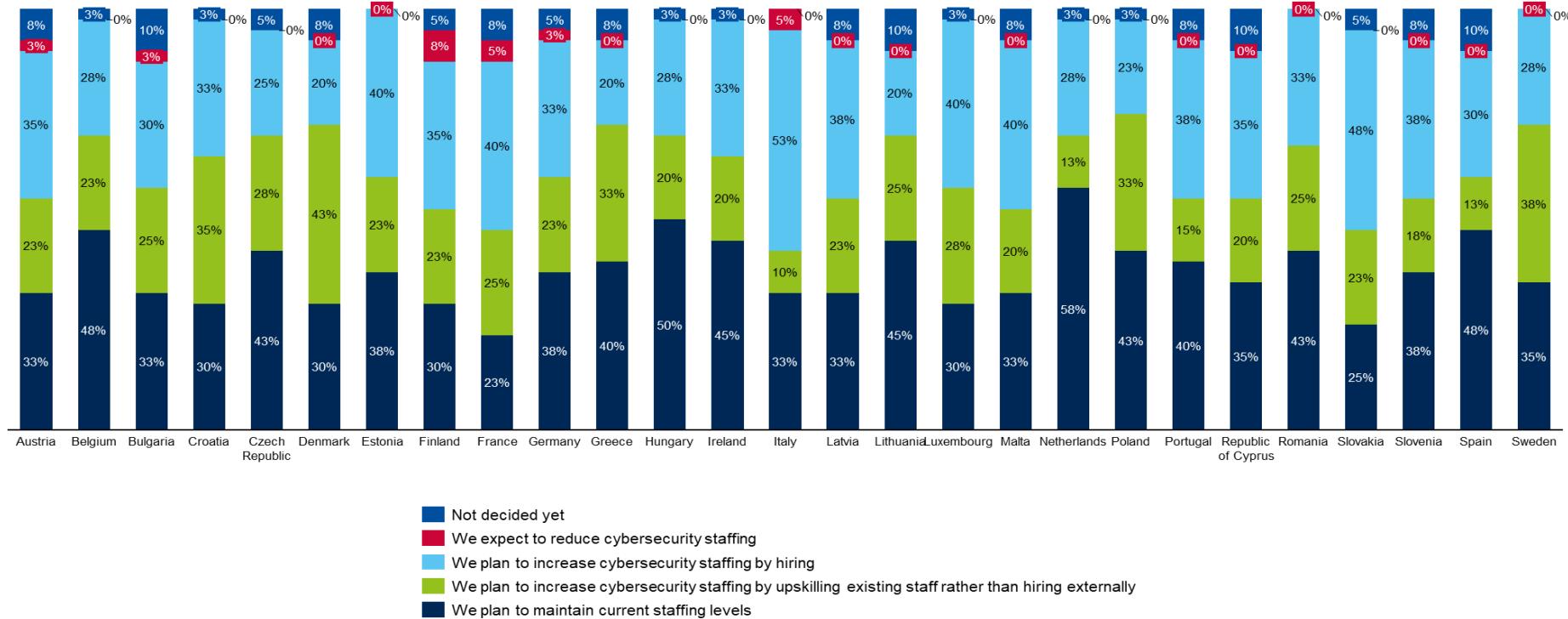


Figure 13 - Cybersecurity staffing strategy, per Member State

## 2.14 Cost reduction measures affecting cybersecurity staffing

**Survey Question:** In the past year, did your organisation take any of the following cost reduction measures affecting cybersecurity staffing?

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

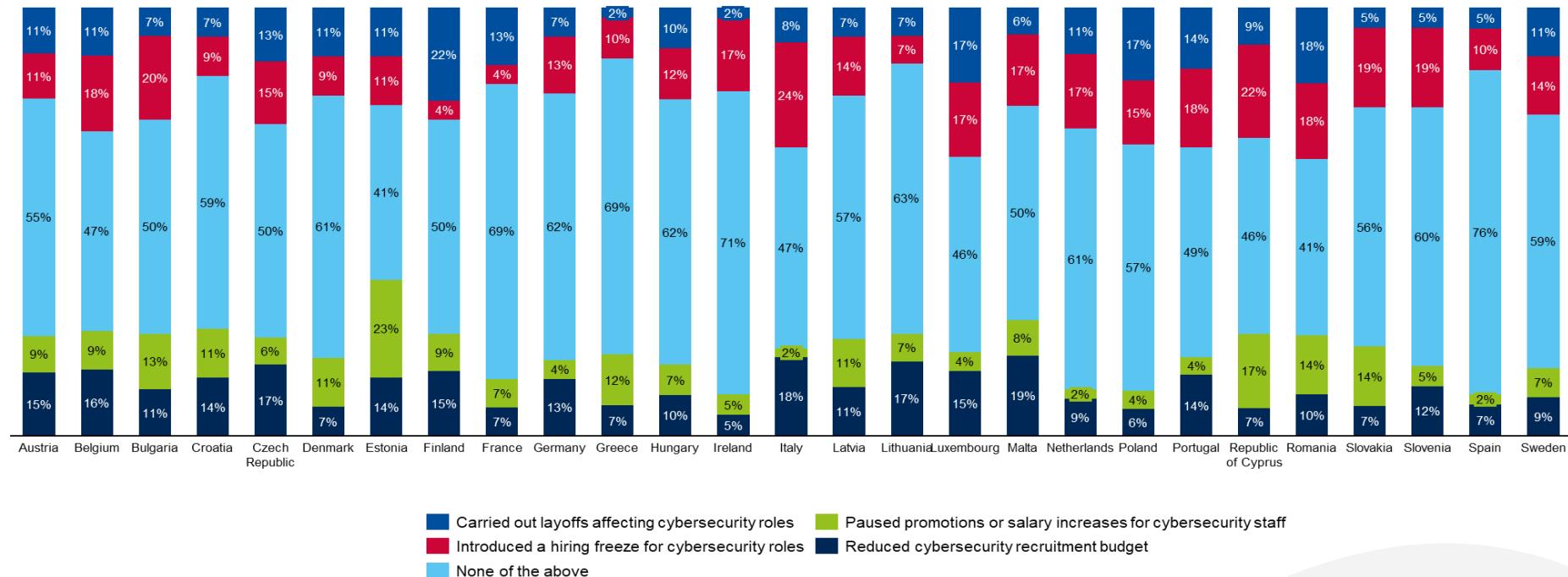


Figure 14 - Cost reduction measures affecting cybersecurity staffing, per Member State

## 2.15 Most in-demand cybersecurity skills currently

**Survey Question:** Which of the following are the most in-demand cybersecurity skills in your organisation right now? (Select up to 3)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

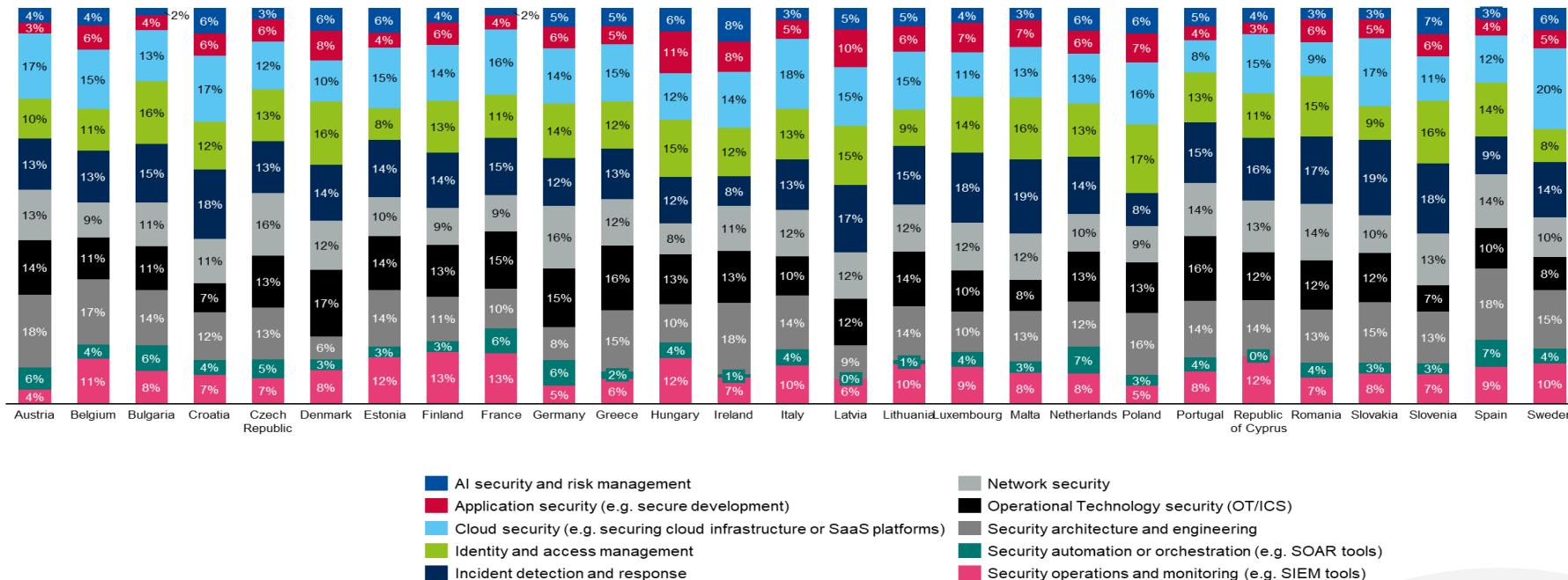


Figure 15 - Most in demand cybersecurity skills currently, per Member State

## 2.16 Most challenging NIS2 requirements to implement

**Survey Question:** Which of the following NIS2 areas is the most challenging for your organisation to implement? (Select up to three)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

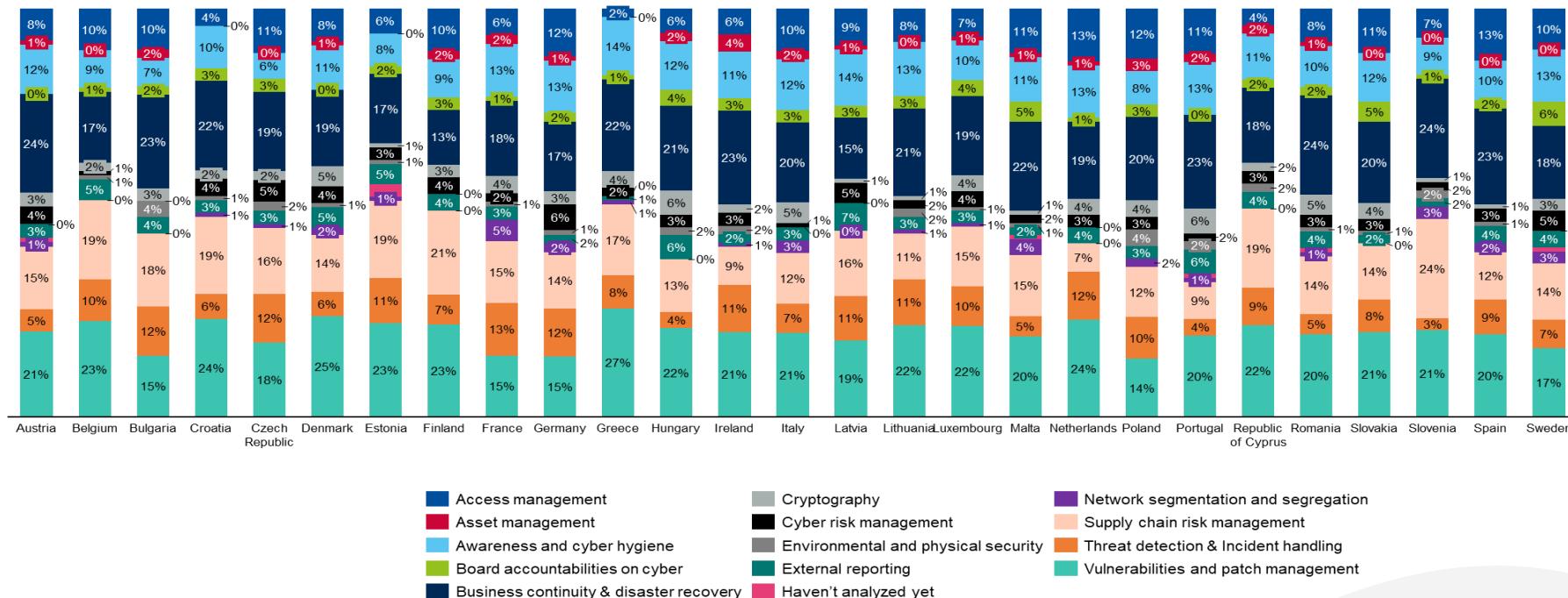


Figure 16 - Most challenging NIS2 requirements, per Member State

## 2.17 Main obstacle to implementing NIS2 requirements

**Survey Question:** What is the main obstacle to implementing these controls effectively?

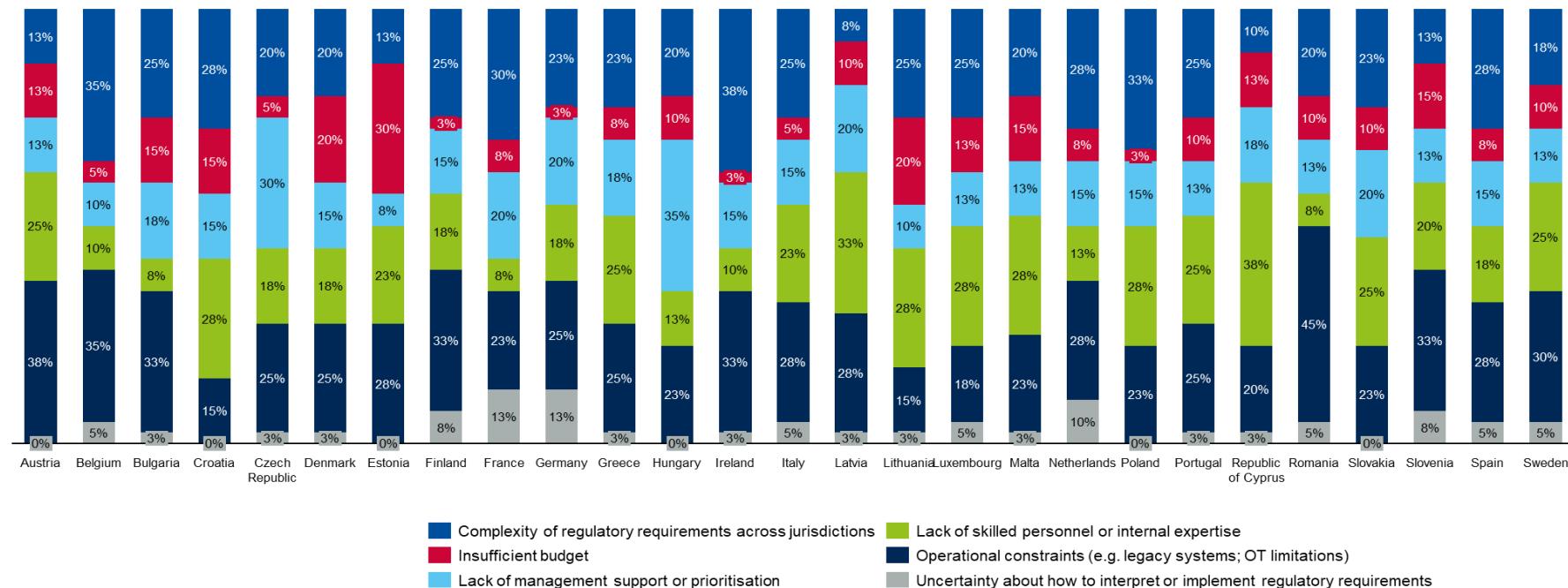


Figure 17 - Main obstacle to implementing NIS2 requirements, per Member State

## 2.18 Cybersecurity assessments

**Survey Question:** Has your organisation conducted any form of cybersecurity assessment or testing (e.g. technical audit, penetration test, red team exercise, maturity assessment) within the past 12 months?

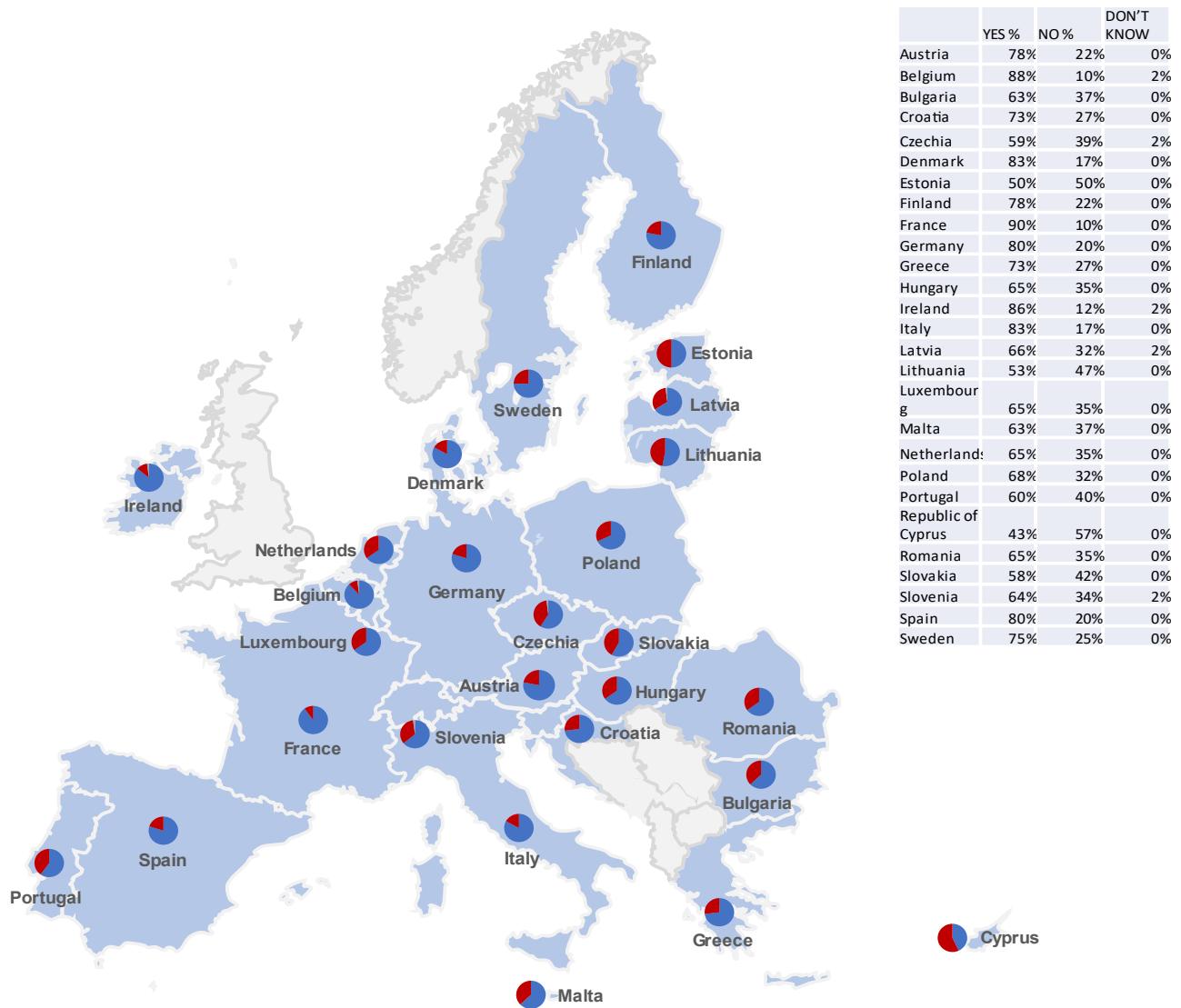


Figure 18 - Proportion of entities having conducted any form of cybersecurity assessment in the past 12 months

## 2.19 Average time to patch critical vulnerabilities on critical systems

**Survey Question:** What is the average time to patch critical vulnerabilities on your organisation's critical assets (IT and OT)?

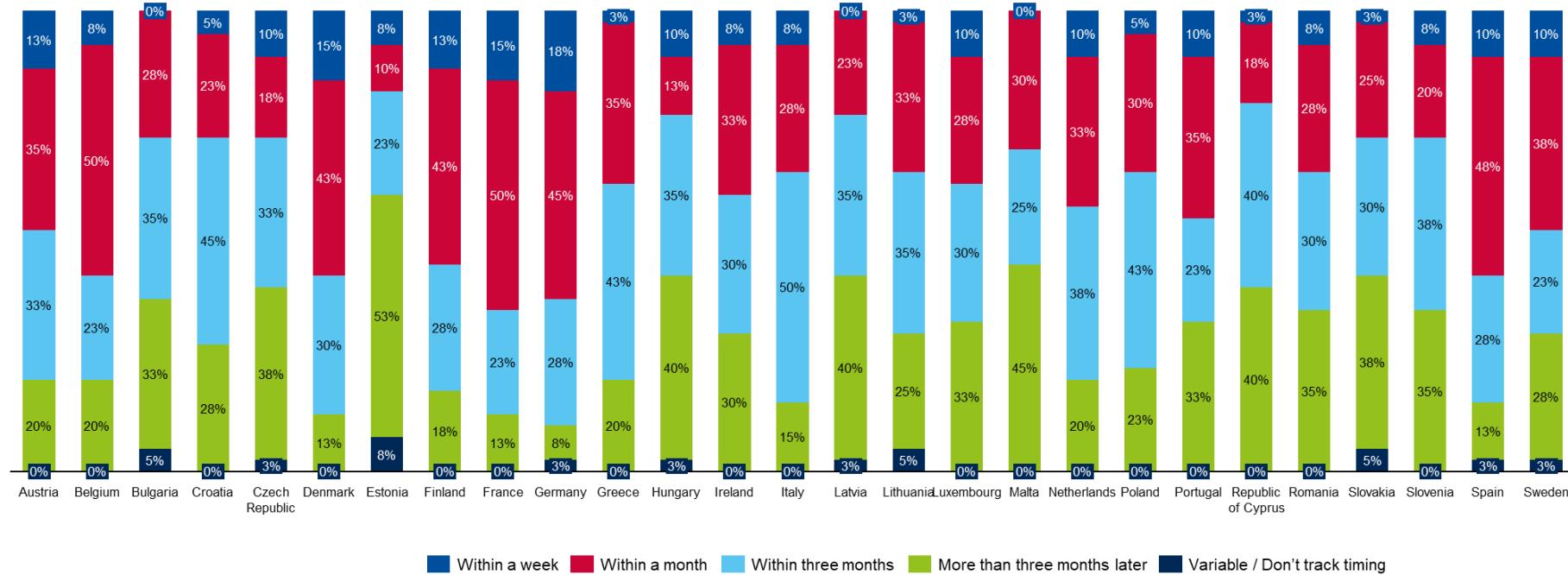


Figure 19 - Average time to patch critical vulnerabilities on critical systems, per Member State

## 2.20 Supply chain risk management practices implemented

**Survey Question:** Which of the following supply chain risk management practices are currently in place in your organisation? (Multiple choices possible)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

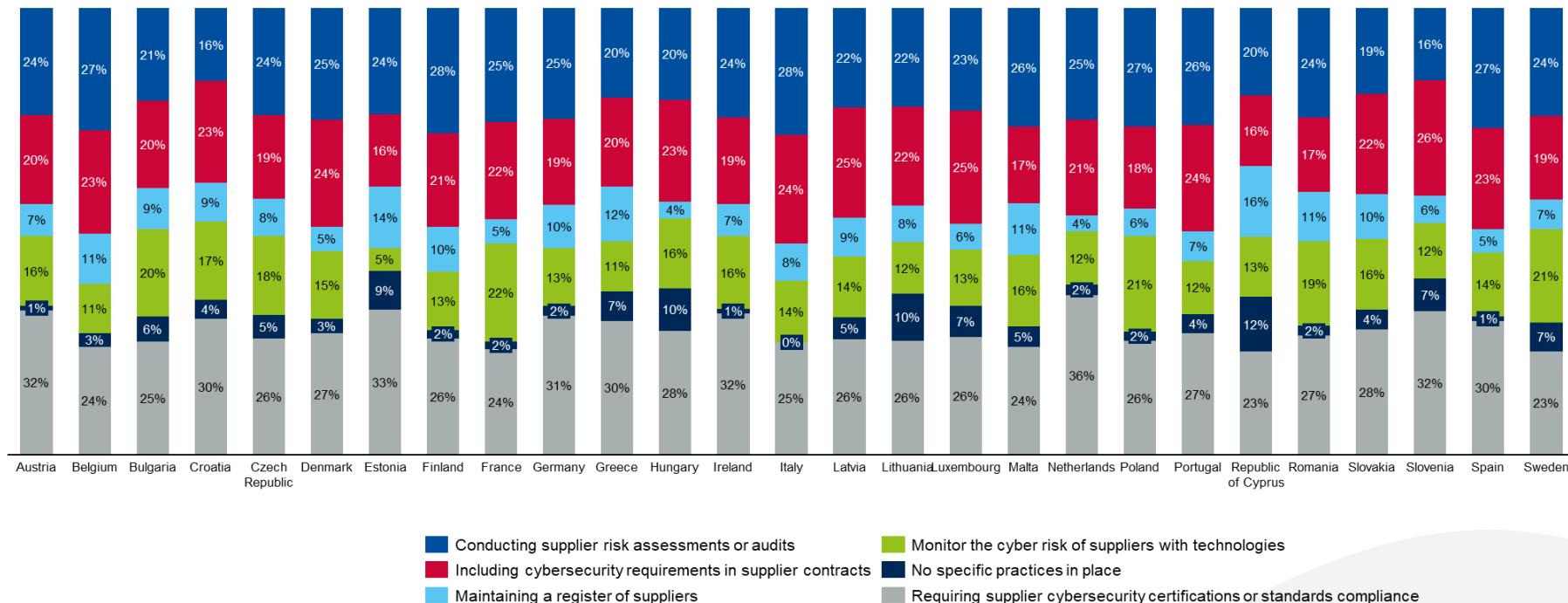


Figure 20 - Supply chain risk management practices implemented, per Member State

## 2.21 Characteristics of preferred suppliers of digital products

**Survey Question:** When procuring products with digital elements (hardware or software), which supplier categories do you commonly use?  
 (Select all that apply)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

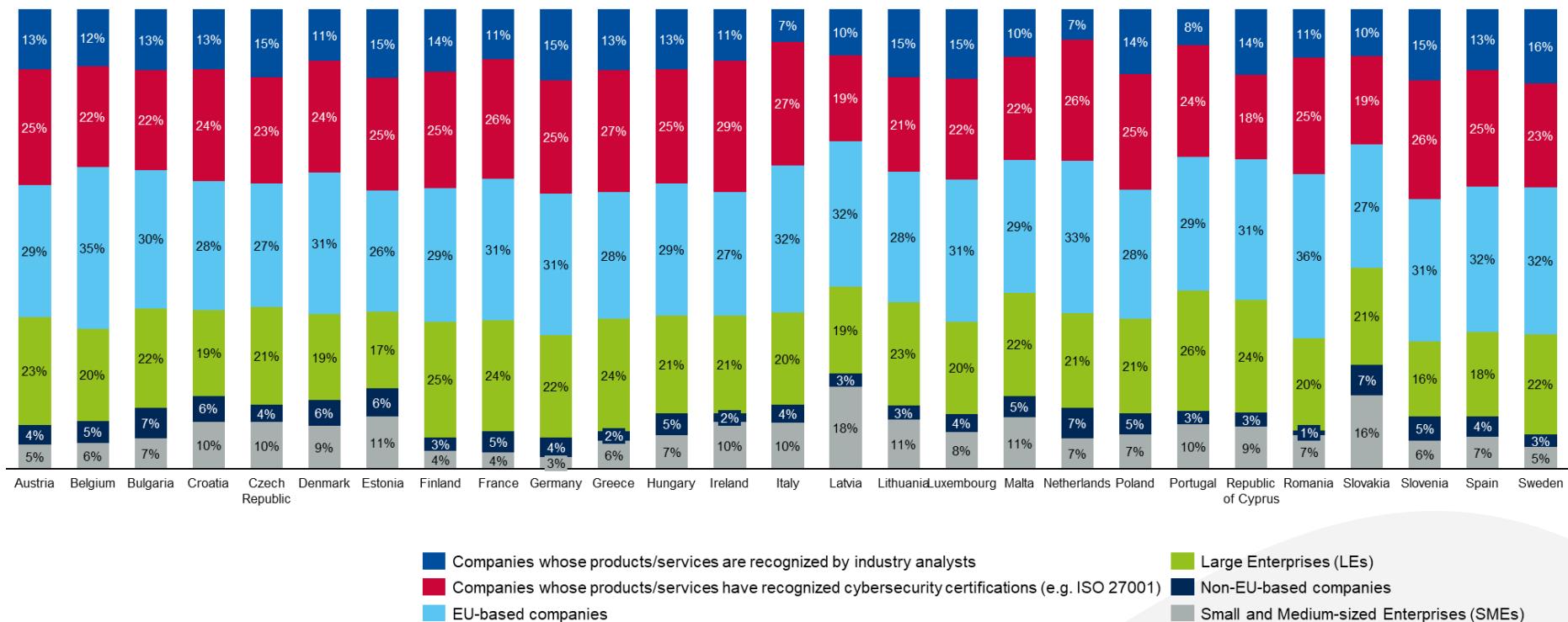


Figure 21 - Characteristics of preferred suppliers of products with digital elements, per Member State

## 2.22 Information Sharing

**Survey Question:** Does your organisation engage in collaboration and information sharing with others? (Multiple choices possible)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

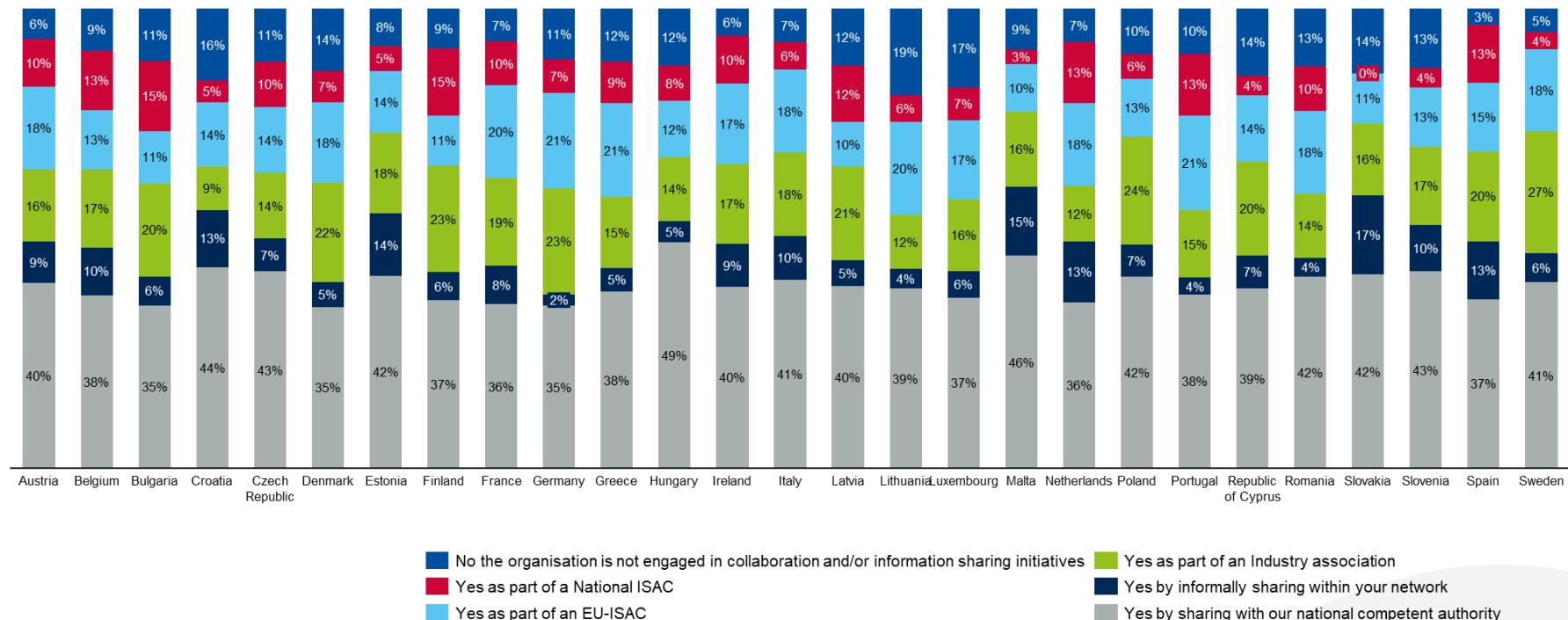


Figure 22 - Participation in information sharing, per Member State

## 2.23 Attacks with the greatest operational impact on day-to-day operations

**Survey Question:** In the past 12 months, which type of cyberattack had the greatest impact on your day-to-day operations?

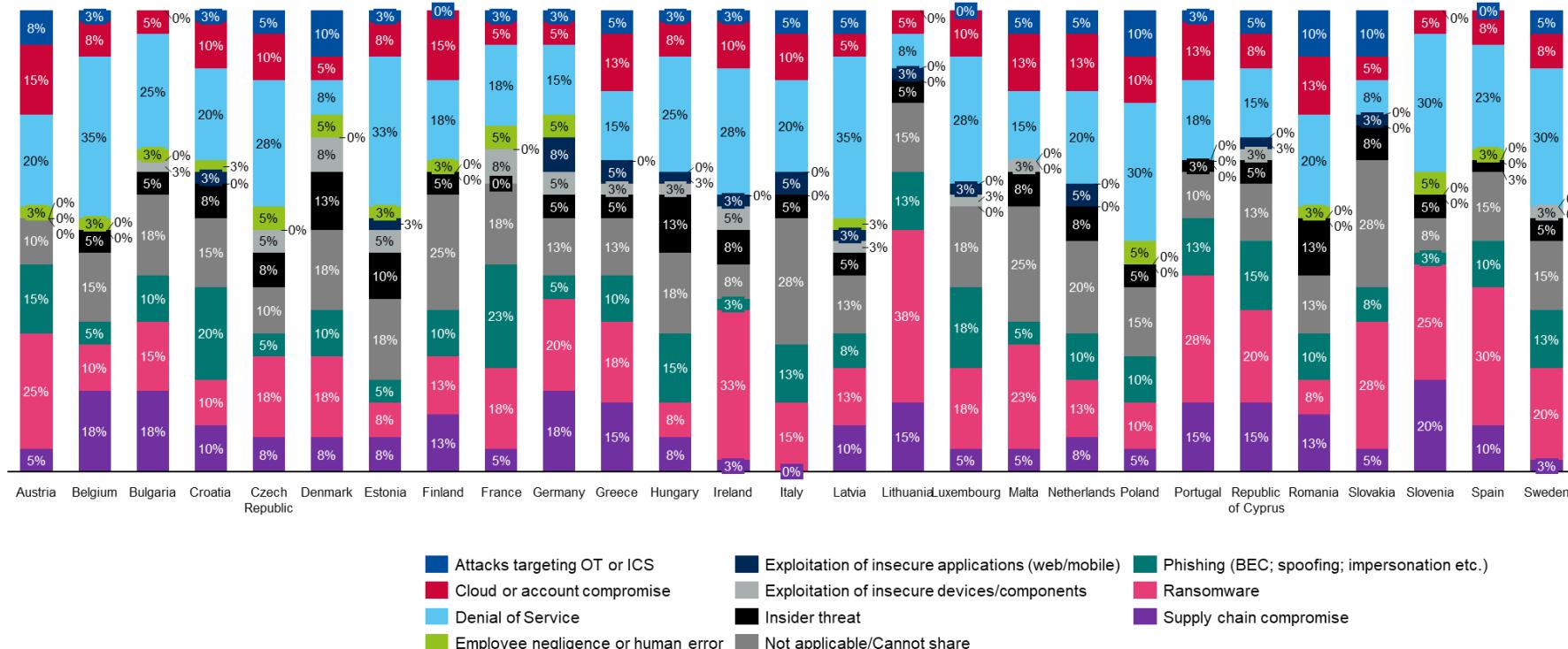


Figure 23 - Attacks with the greatest operational impact on day-to-day operations, per Member State

## 2.24 Cybersecurity threats of most concern looking ahead

**Survey Question:** Which of the following cybersecurity risks or attack types concern you the most looking ahead? (Select up to 3)

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective Member State. Not the proportion of entities within the respective Member State, having provided that answer.

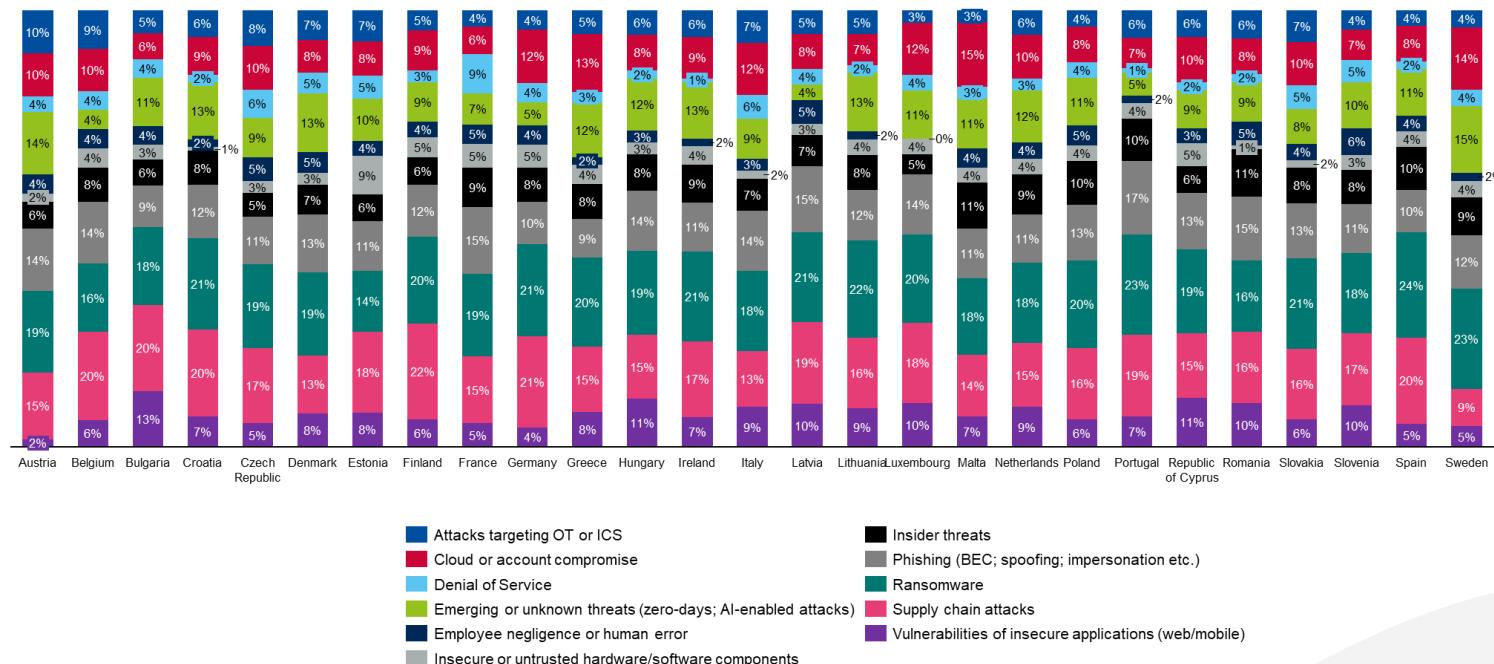


Figure 24 - Cybersecurity threats of most concern looking ahead, per Member State

## 2.25 Preparedness against scenarios

**Survey Question:** For each of the following scenarios, would you categorize your organization's current stance as predominantly prepared or unprepared? –

(Cybersecurity preparedness refers to your organisation's ability to anticipate, prevent, respond to, and recover from cyber incidents effectively)

### A ransomware attack that encrypts critical systems

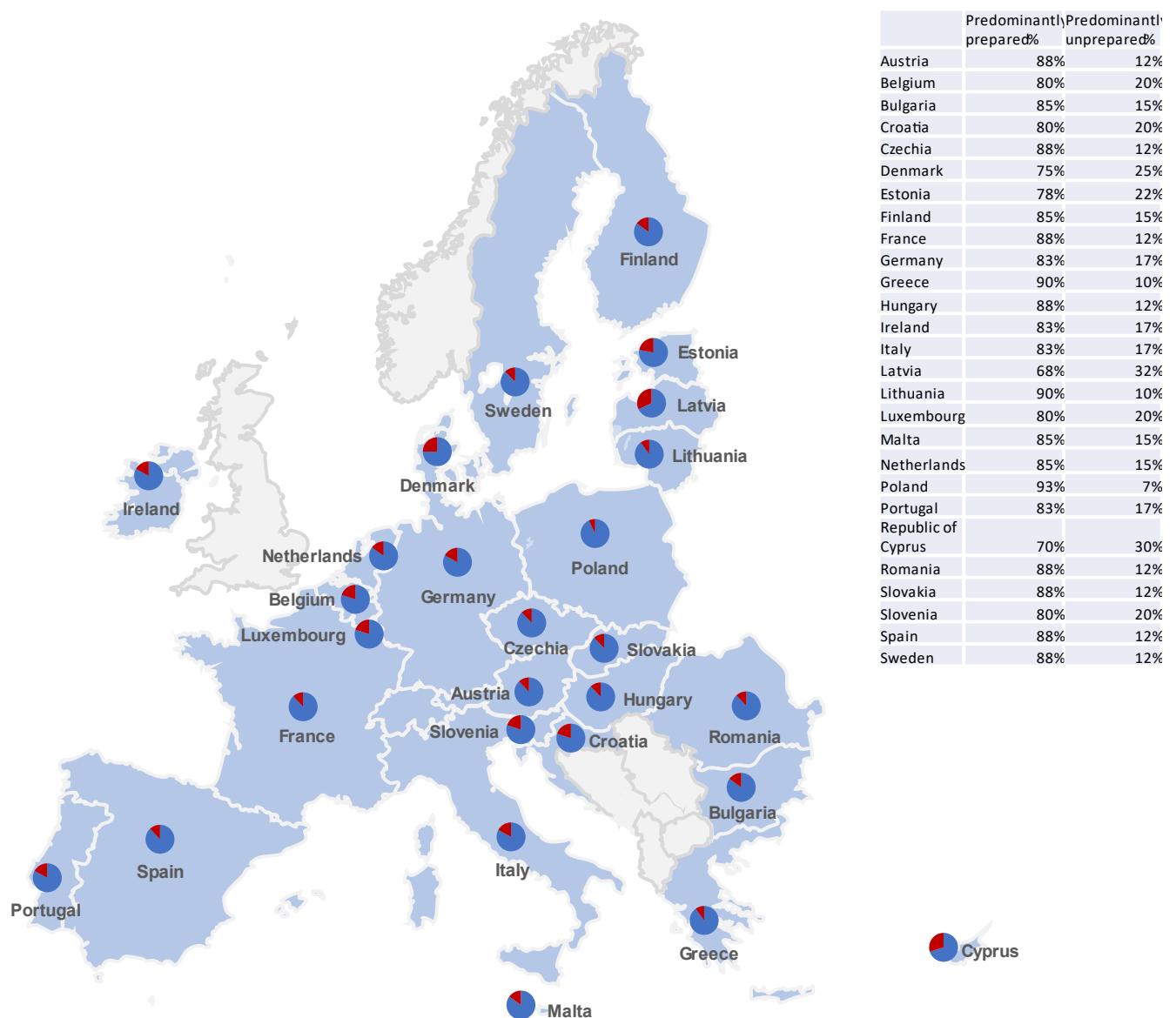


Figure 25 - Preparedness against ransomware

**Survey Question:** For each of the following scenarios, would you categorize your organization's current stance as predominantly prepared or unprepared? –

#### A supply chain attack or compromise to a third-party service

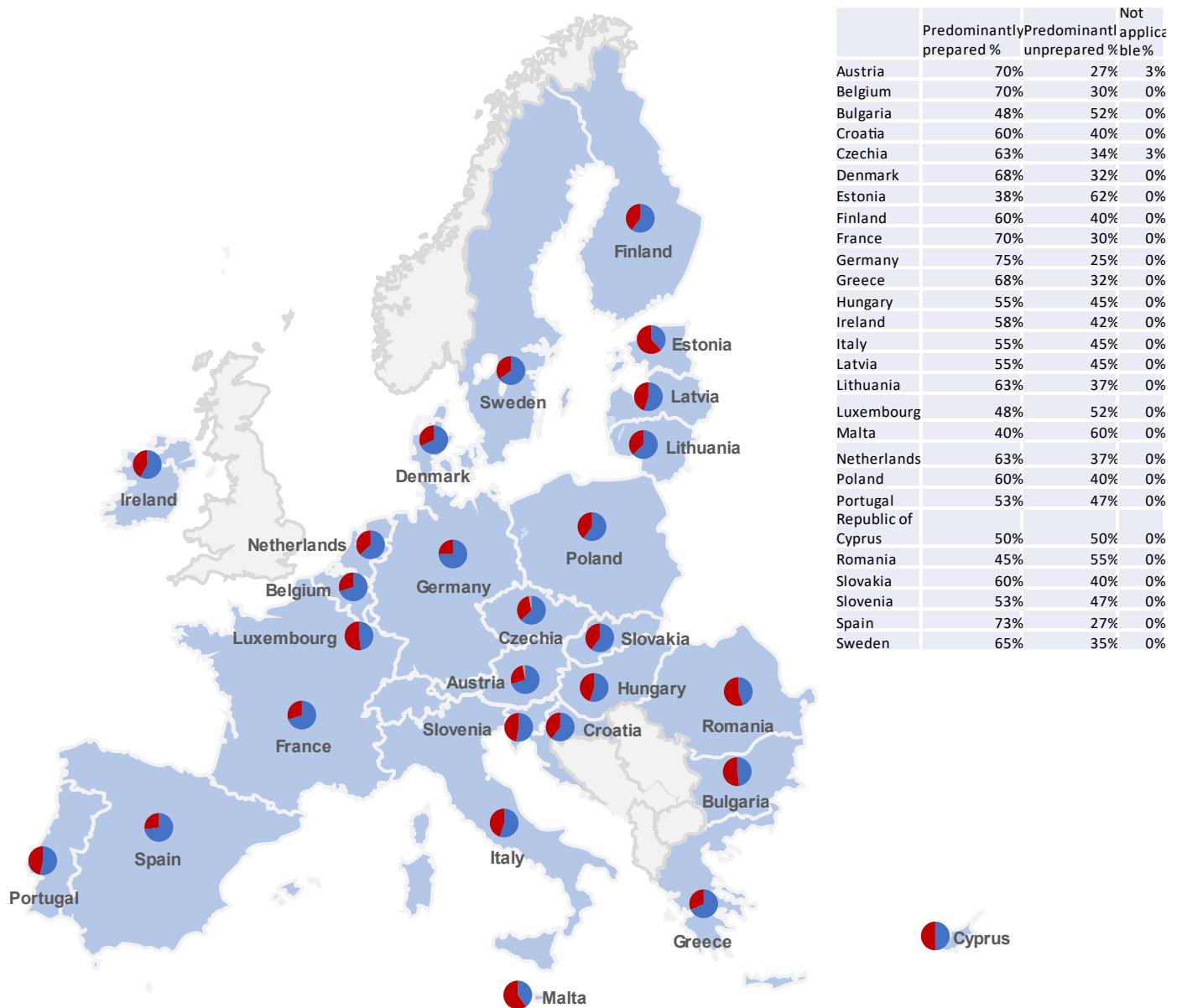


Figure 26 - Preparedness against supply chain attack or third-party compromise

**Survey Question:** For each of the following scenarios, would you categorize your organization's current stance as predominantly prepared or unprepared? –

#### A cyberattack causes IT/OT infrastructure outage or degradation

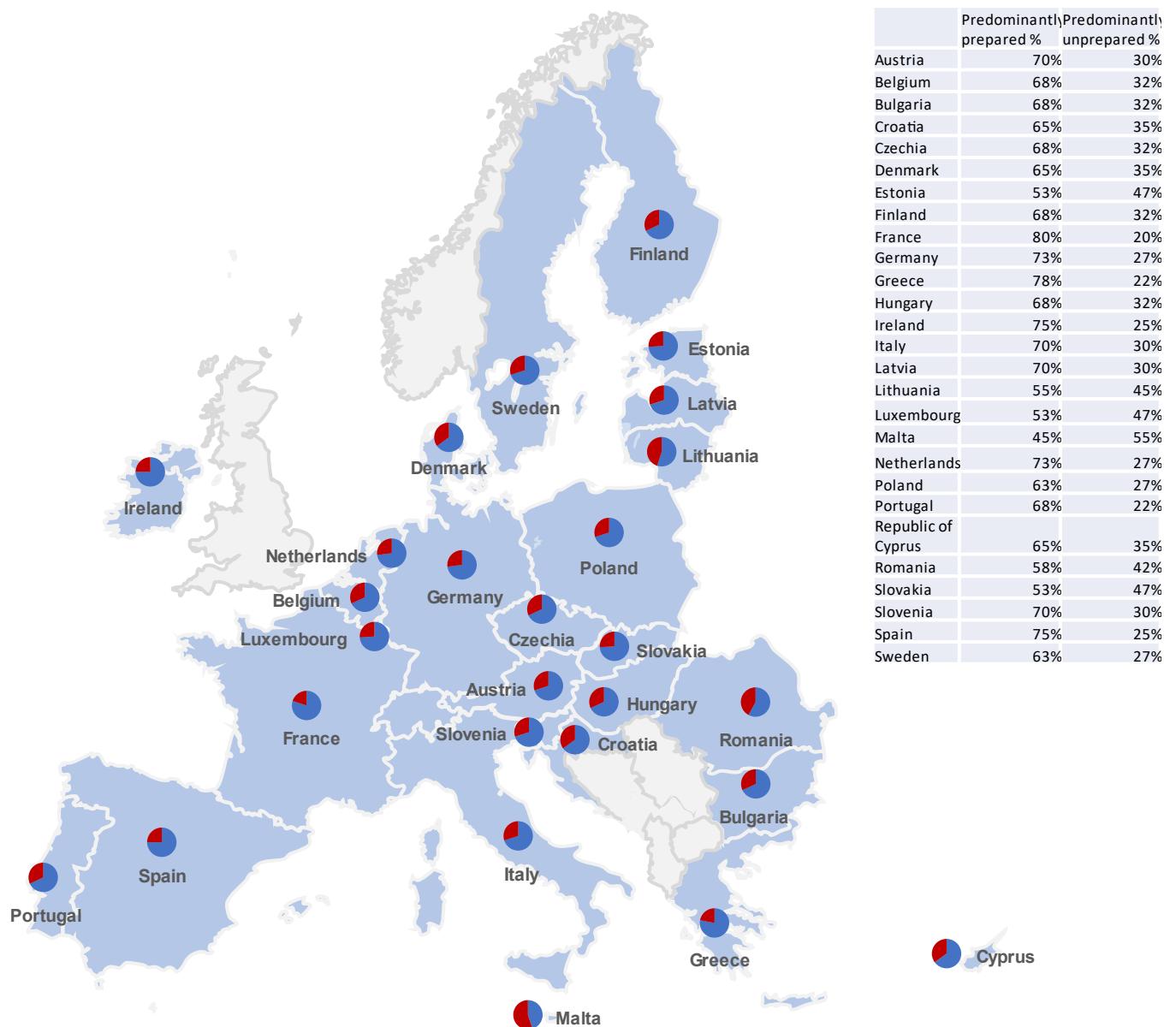


Figure 27 - Preparedness against attacks causing IT/OT infra outages or degradation

## SECTION 3

# Sector view

## 3. Sector view<sup>1</sup>

### 3.1 IT spending

**Survey Question:** What was your organisation's estimated IT budget or spending in Euros for 2024 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

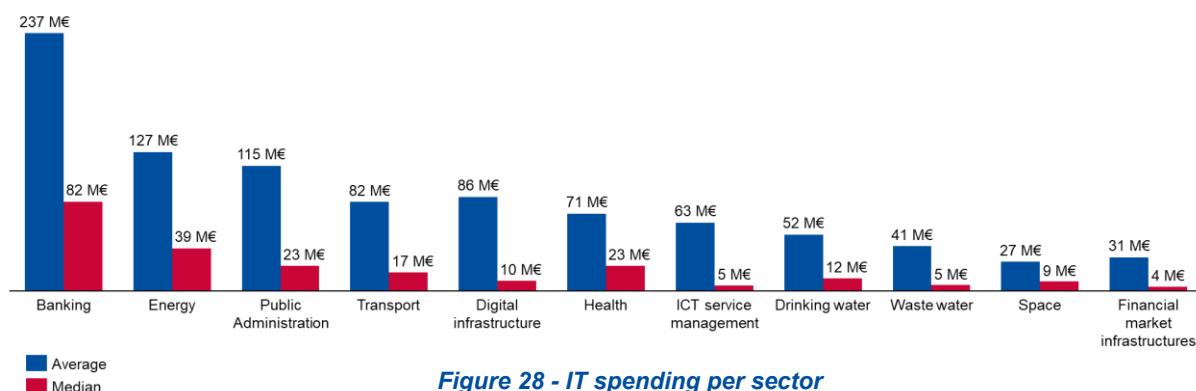


Figure 28 - IT spending per sector

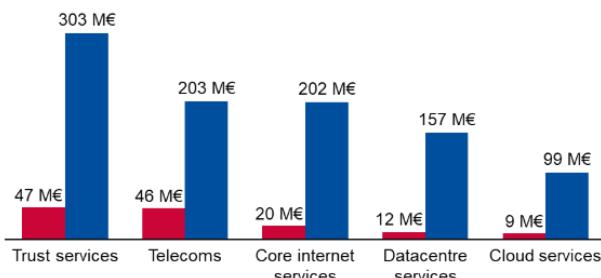


Figure 29 - IT spending, Digital Infrastructure

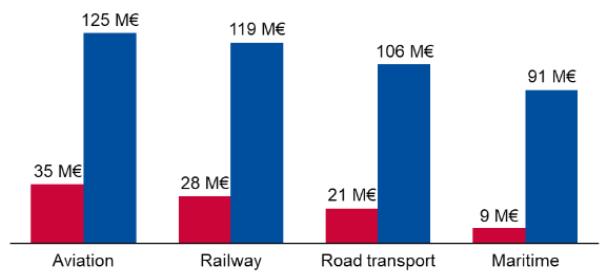


Figure 30 - IT spending, Transport

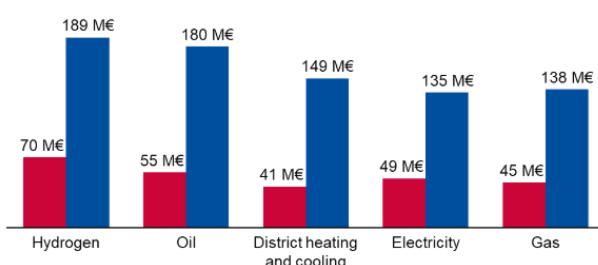


Figure 31 - IT spending, Energy

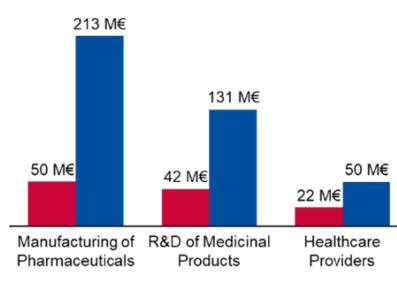
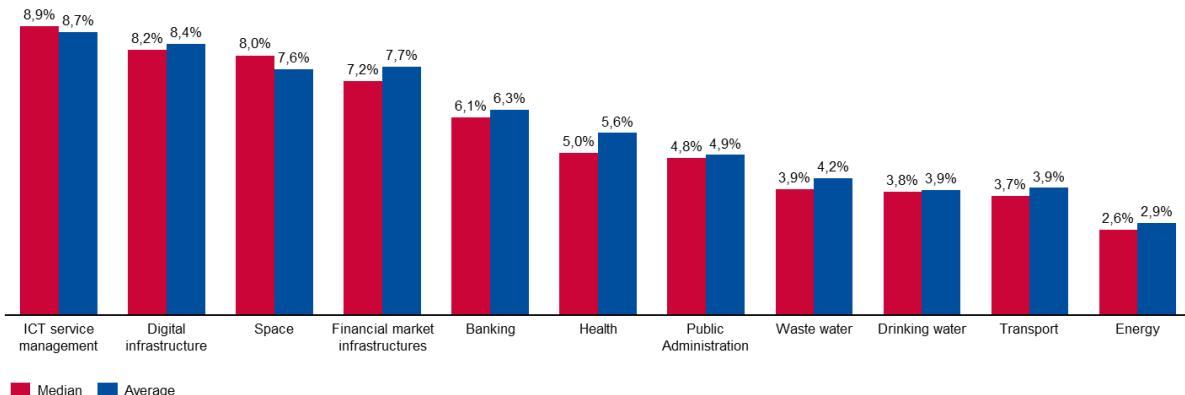


Figure 32 - IT spending, Health

<sup>1</sup> Note: EU reference laboratories are included in the Health sector sample. However, the results for these entities are not shown separately in the breakdown due to their low representation in the sample.

### 3.2 IT spending as a share of revenues

**Calculated field:** This metric is a calculated field that expresses the proportion (or percentage) of an organisation's revenue that is allocated to IT.



*Figure 33 - IT spending as a share of revenues per sector*

### 3.3 IS spending

**Survey Question:** What was your organisation's estimated Information Security budget or spending in Euros for 2024 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

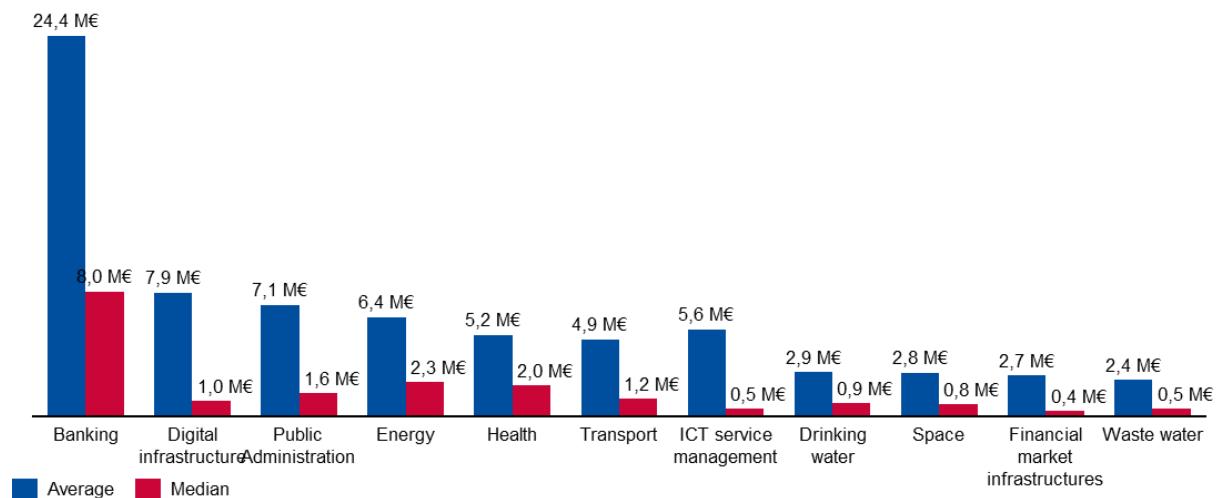


Figure 34 - IS spending per sector

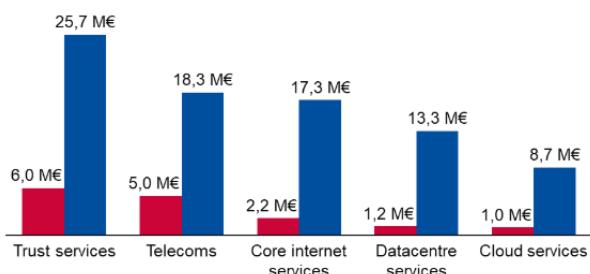


Figure 35 - IS spending, Digital Infrastructure

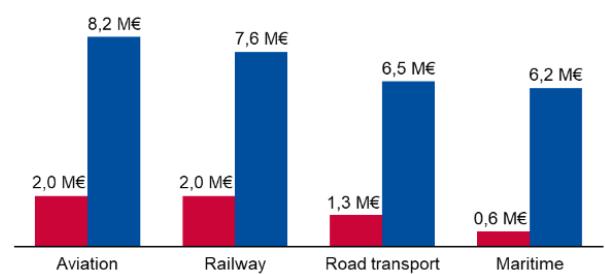


Figure 36 - IS spending, Transport

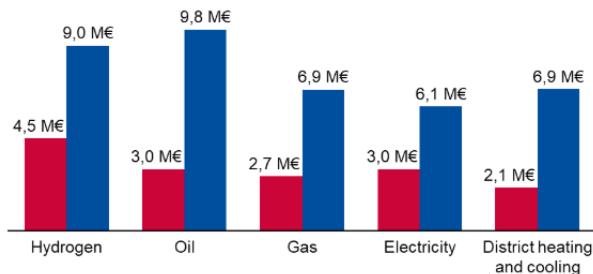


Figure 37 - IS spending, Energy

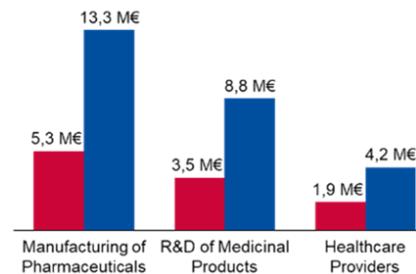


Figure 38 - IS spending, Health

### 3.4 IS spending as a share of IT spending

**Calculated field:** This metric is a calculated field that expresses the proportion (or percentage) of an organisation's IS budget or spending compared to its total IT budget or spending.

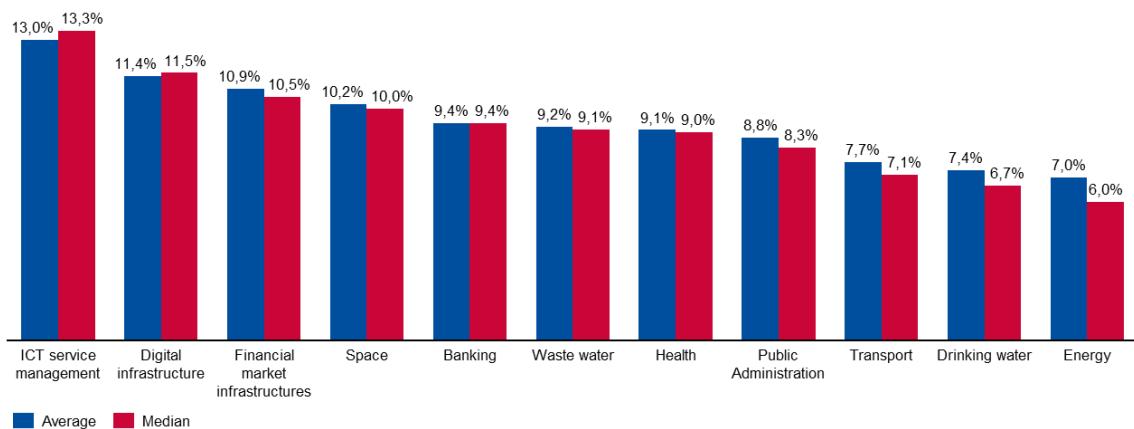


Figure 39 - IS spending as a share of IT spending, per sector

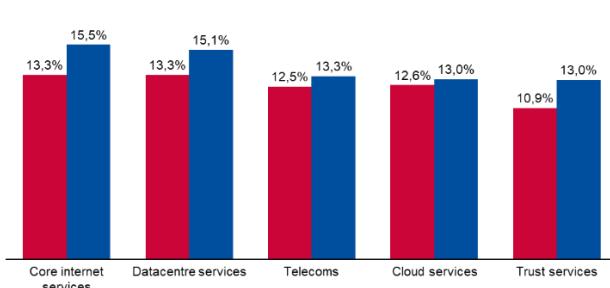


Figure 40 - IS spending, Digital Infrastructure

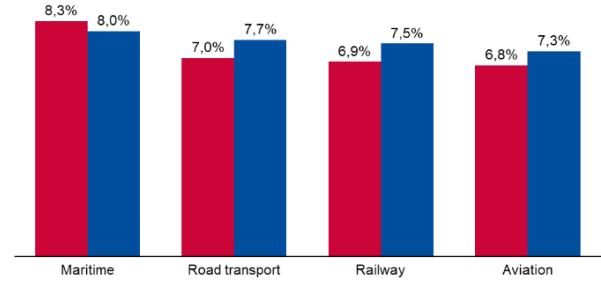


Figure 41 - IS spending, Transport

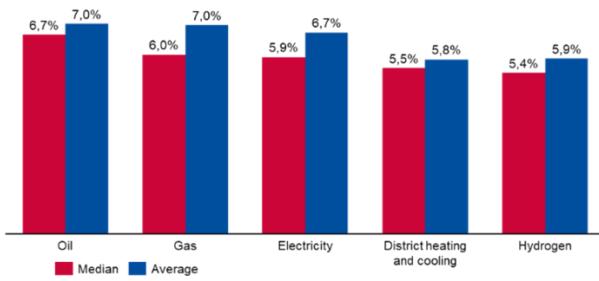


Figure 42 - IS spending, Energy

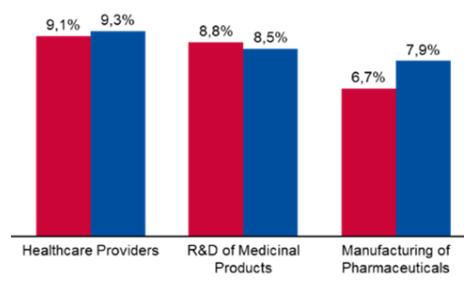


Figure 43 - IS spending, Health

### 3.5 Outcomes attained via cybersecurity investment in 2024

**Survey Question:** Which of the following outcomes has your organisation achieved as a result of its cybersecurity investments in the past year? (Select up to three)

#### Across EU view

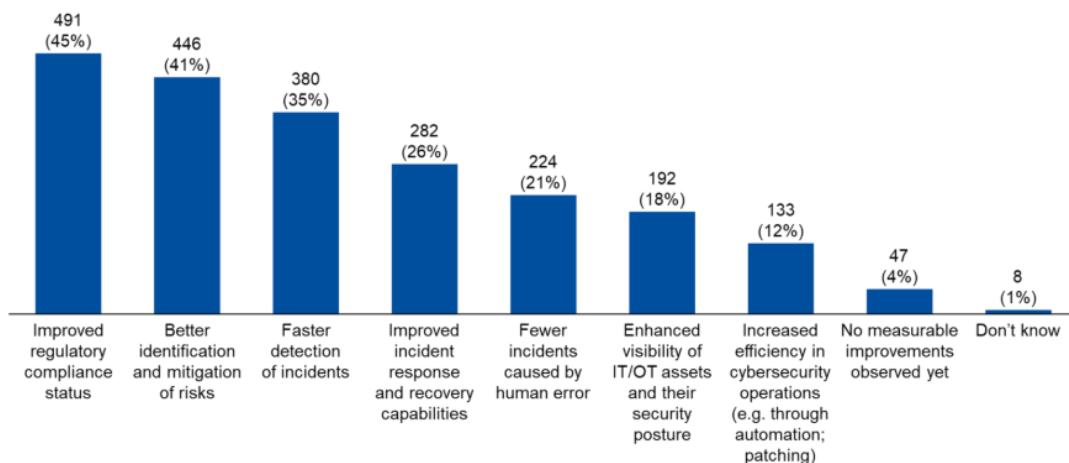


Figure 44 - Outcomes attained via cybersecurity investment in 2024

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

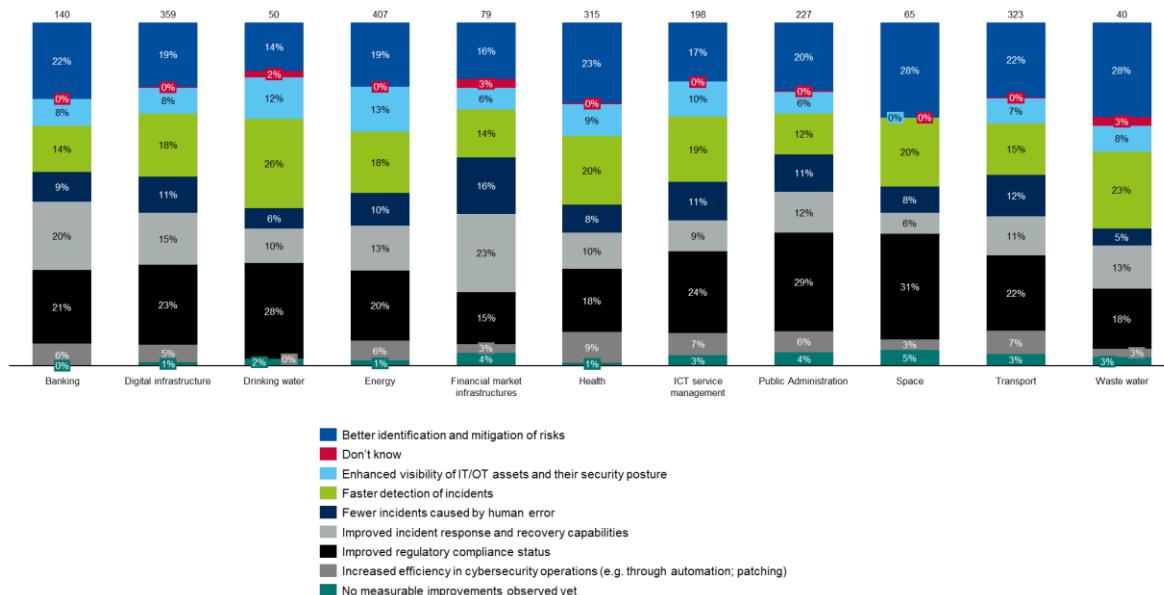


Figure 45 - Outcomes attained via cybersecurity investment in 2024, per sector

### 3.6 Key cybersecurity investment drivers for 2024

**Survey Question:** In the past year, which of the following has most significantly driven cybersecurity investment in your organisation? (Select up to 3)

#### Across EU view

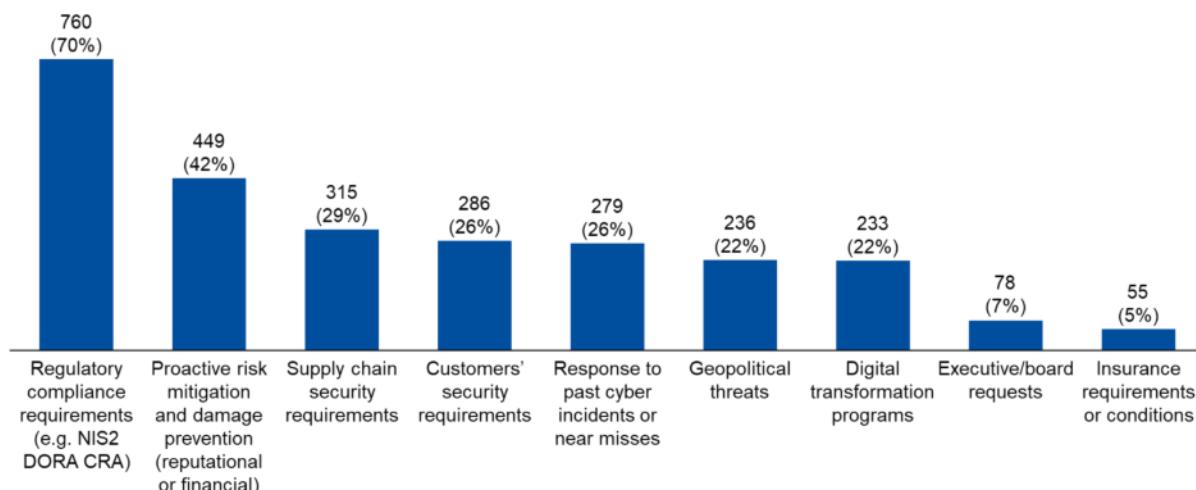


Figure 46 - Key cybersecurity investment drivers for 2024

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

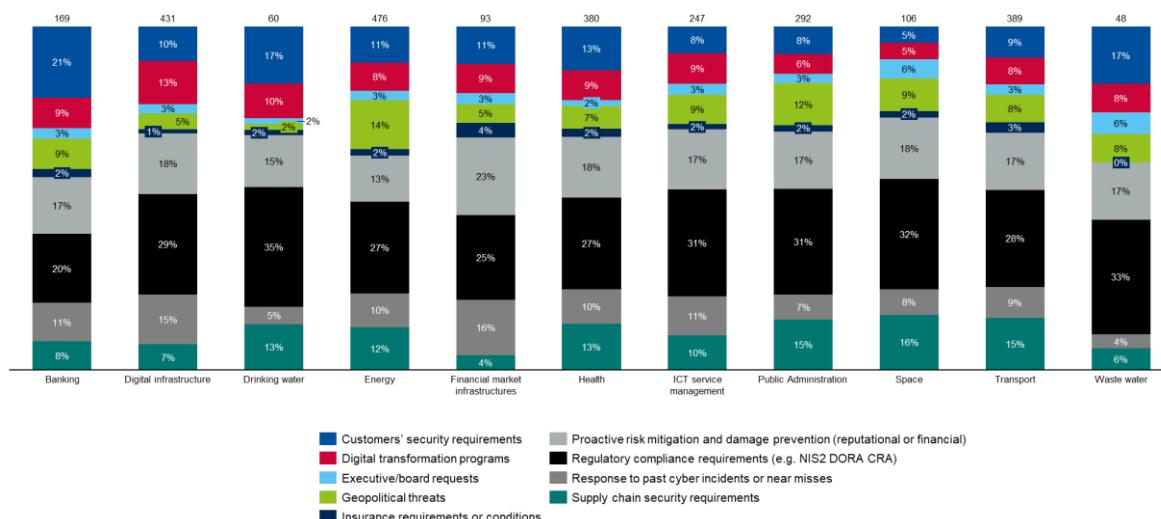


Figure 47 - Key cybersecurity investment drivers for 2024, per sector

### 3.7 Targeted outcomes of cybersecurity investment in the coming year

**Survey Question:** Which of the following outcomes are you primarily targeting with your cybersecurity investments in the coming year? (Select up to three)

#### Across EU view

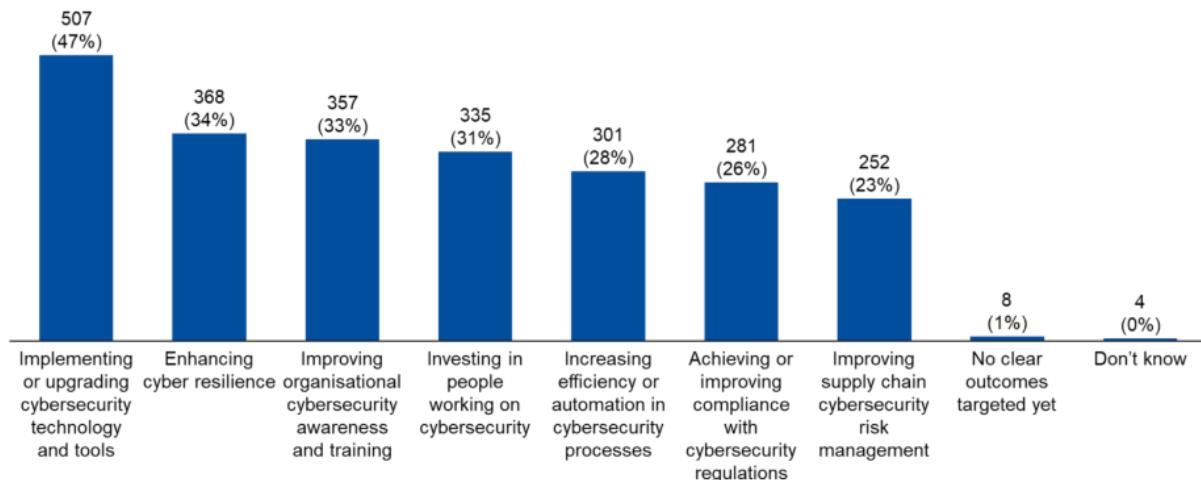


Figure 48 - Targeted outcomes of cybersecurity investment in the coming year

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

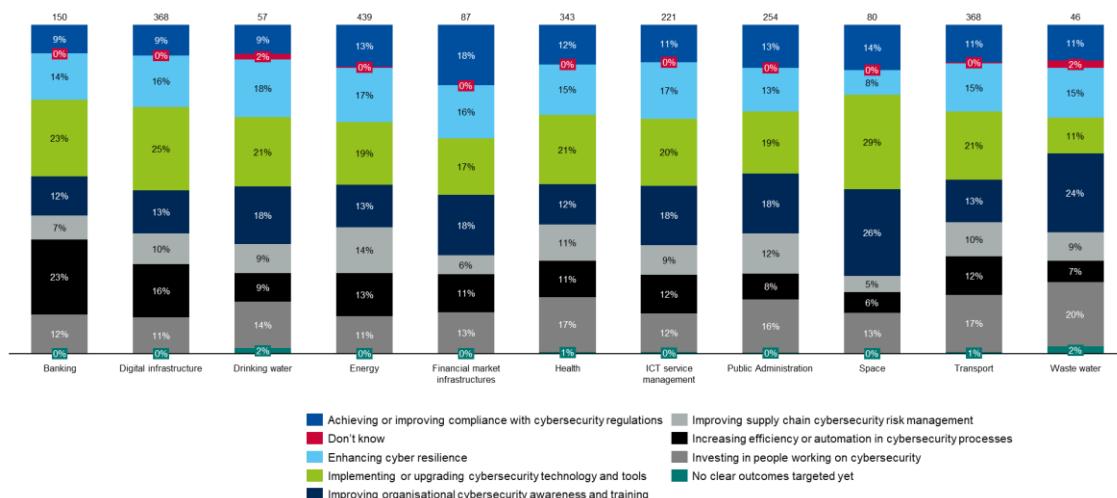


Figure 49 - Targeted outcomes of cybersecurity investment in the coming year, per sector

### 3.8 IT FTEs

**Survey Question:** What was your organisation's estimated number of IT FTEs for 2024 including internal staff and contractors?

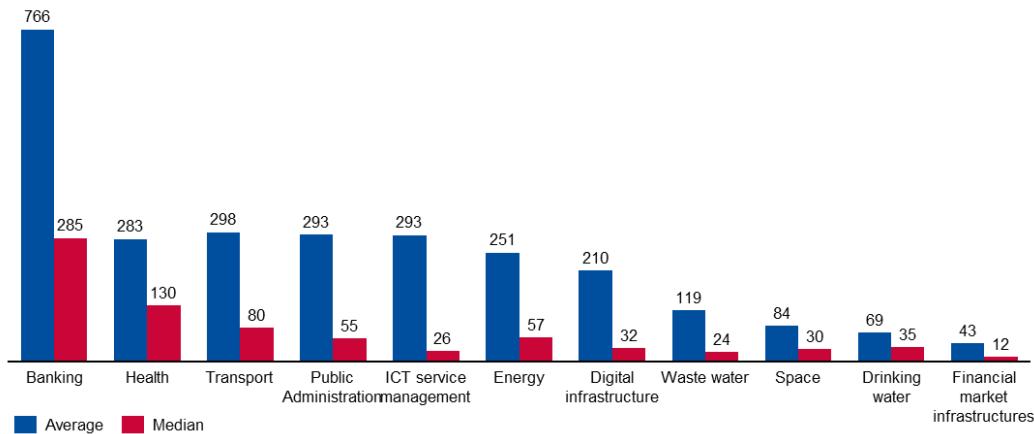


Figure 50 - IT FTEs per sector

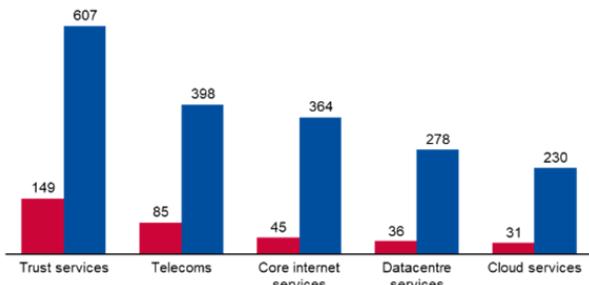


Figure 51 – IT FTEs, Digital Infrastructure

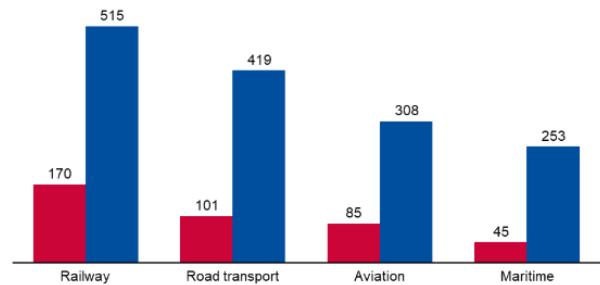


Figure 52 – IT FTEs, Transport

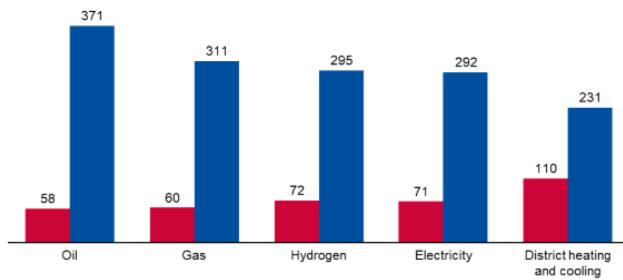


Figure 53 – IT FTEs, Energy

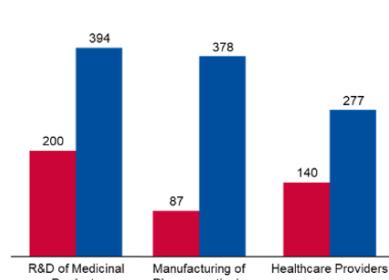


Figure 54 – IT FTEs, Health

### 3.9 IS FTEs

**Survey Question:** What was your organisation's estimated number of Information Security FTEs for 2024 including internal staff and contractors?

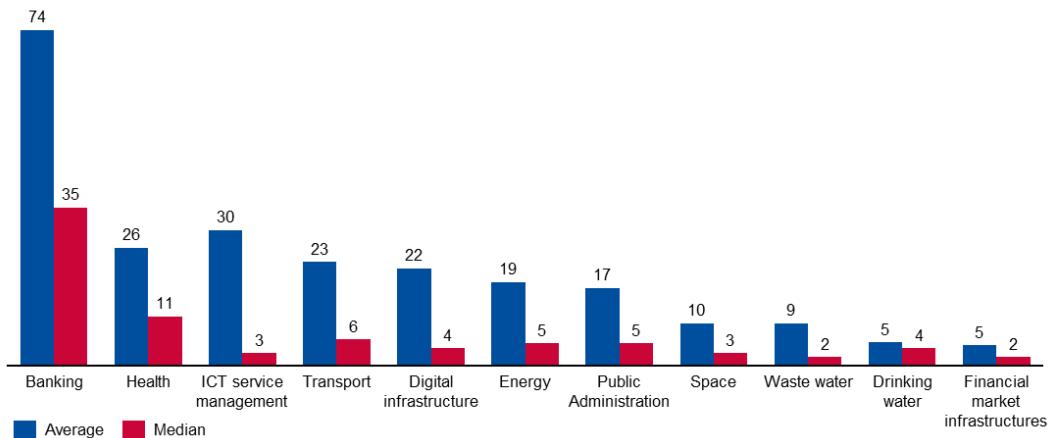


Figure 55 - IS FTEs per sector

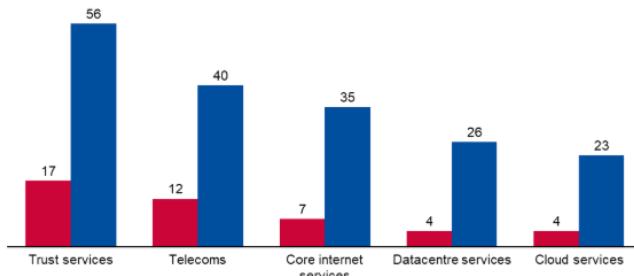


Figure 56 – IS FTEs, Digital Infrastructure

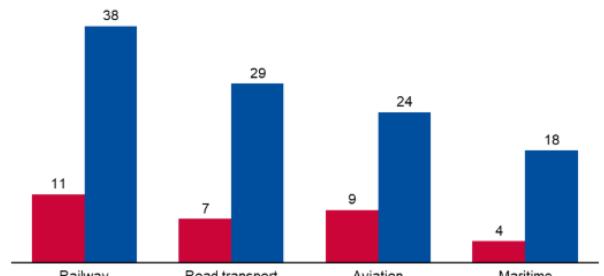


Figure 57 – IS FTEs, Transport

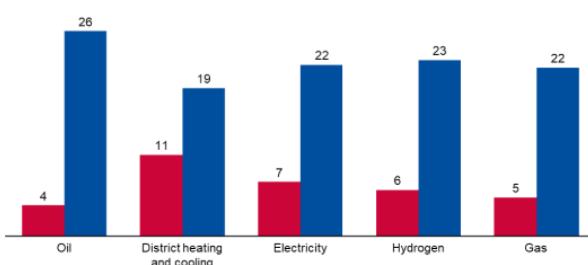


Figure 58 – IS FTEs, Energy

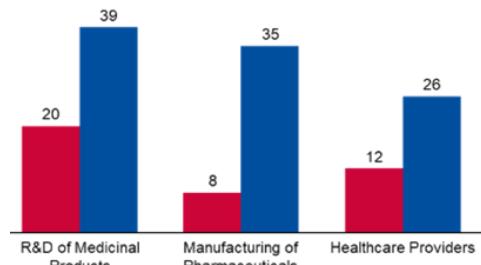


Figure 59 – IS FTEs, Health

### 3.10 IS FTEs as a share of IT FTEs

**Calculated field:** This metric is a calculated field that expresses the proportion (or percentage) of an organisation's IS FTEs over IT FTEs.

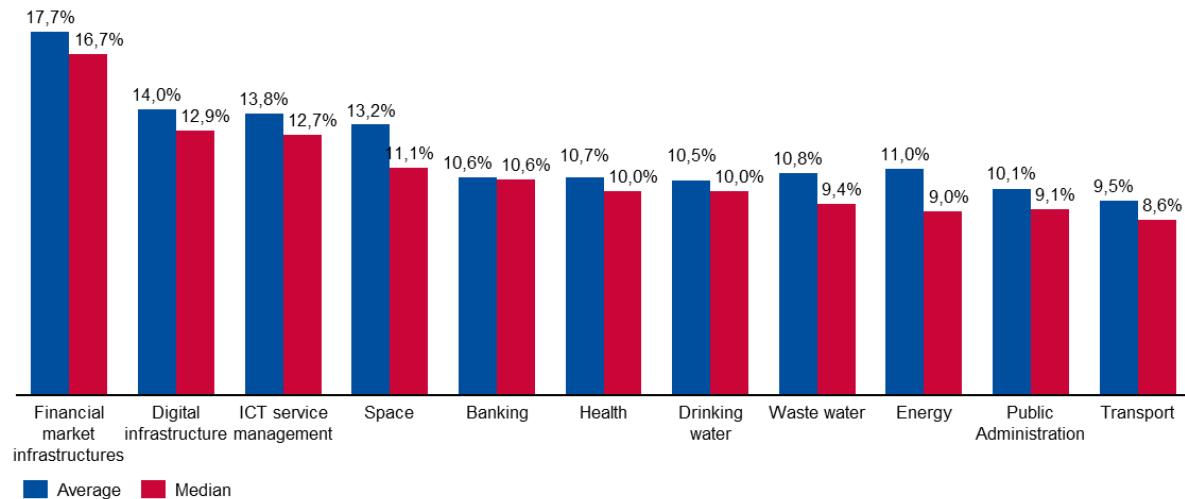


Figure 60 - IS FTEs as a share of IT FTEs per sector

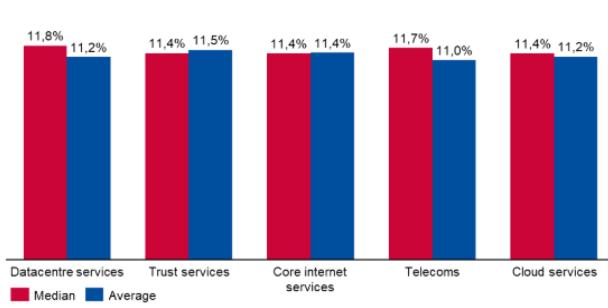


Figure 61 – IS/IT FTEs, Digital Infrastructure

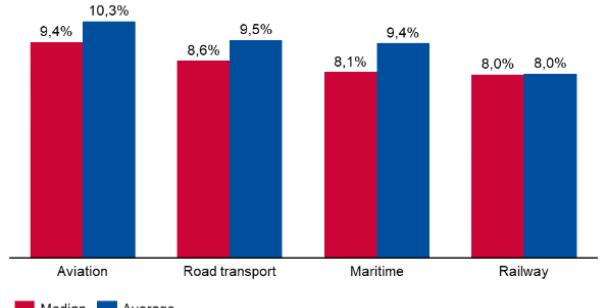


Figure 62 – IS/IT FTEs, Transport

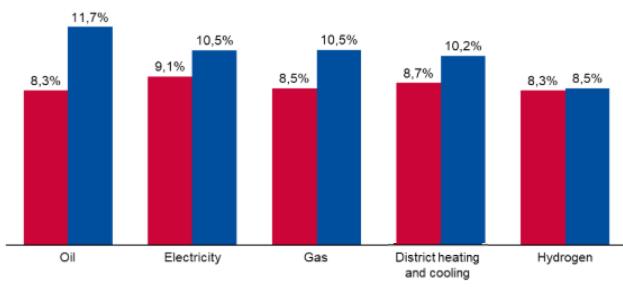


Figure 63 – IS/IT FTEs, Energy

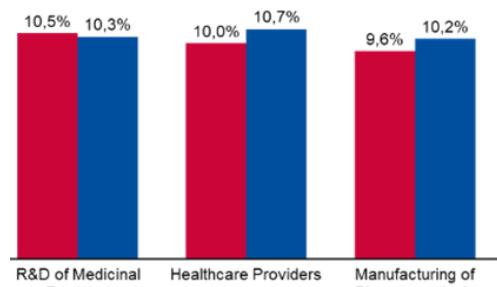
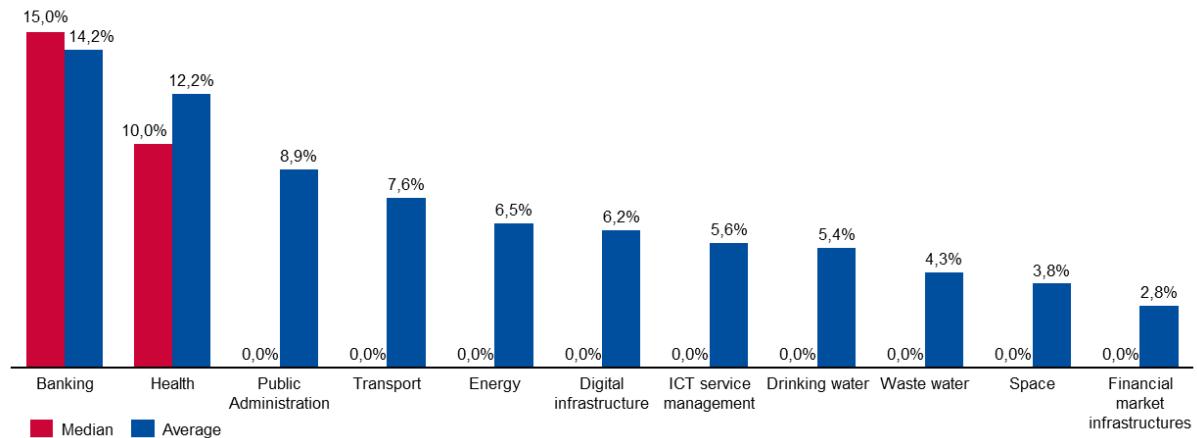


Figure 64 – IS/IT FTEs, Health

### 3.11 Proportion of women in IS FTEs

**Survey Question:** Please share what percentage of your IS FTEs are women?



*Figure 65 - Proportion of women in IS FTEs per sector*

### 3.12 Challenges to attracting cybersecurity talent

**Survey Question:** Which barriers does your organisation face in attracting cybersecurity personnel?  
 (Select up to three)

#### Across EU view

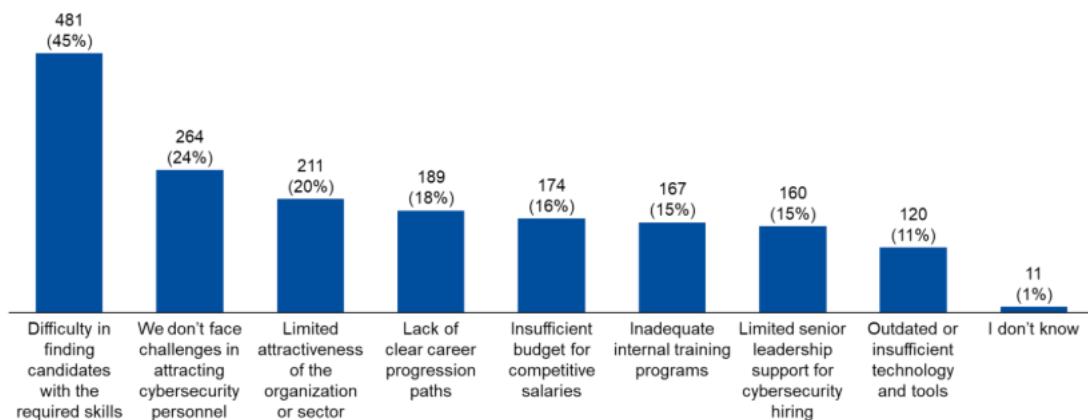


Figure 66 - Challenges to attracting cybersecurity talent

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

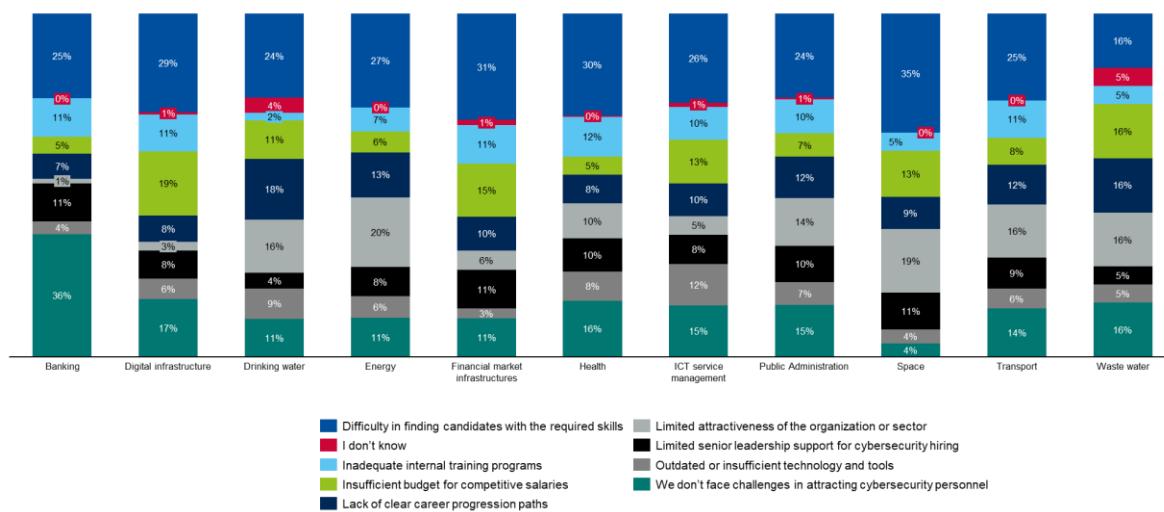


Figure 67 - Challenges to attracting cybersecurity talent, per sector

### 3.13 Challenges to retaining cybersecurity personnel

**Survey Question:** What are the main challenges your organisation faces in retaining cybersecurity personnel? (Select up to three)

#### Across EU view

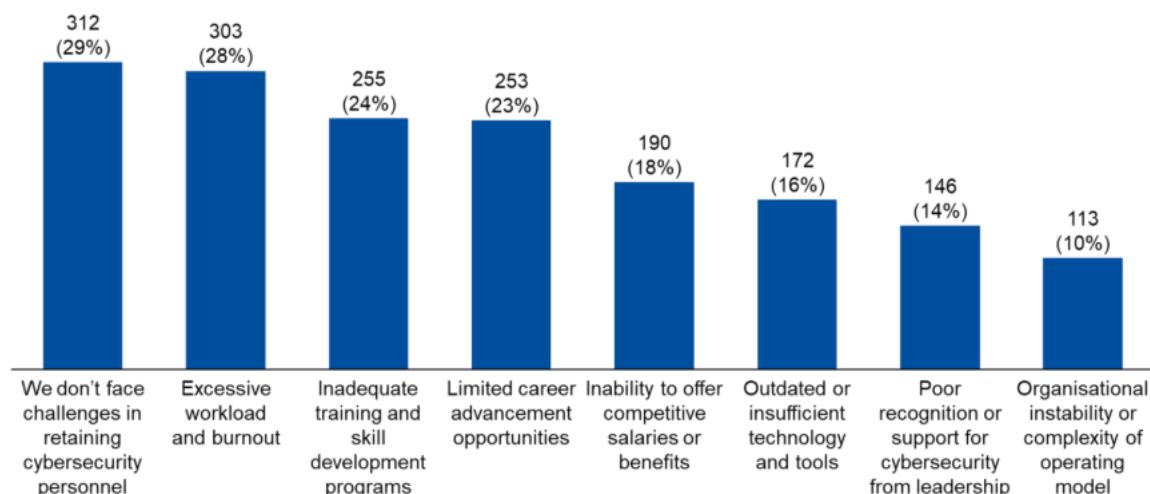


Figure 68 - Challenges to retaining cybersecurity personnel

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

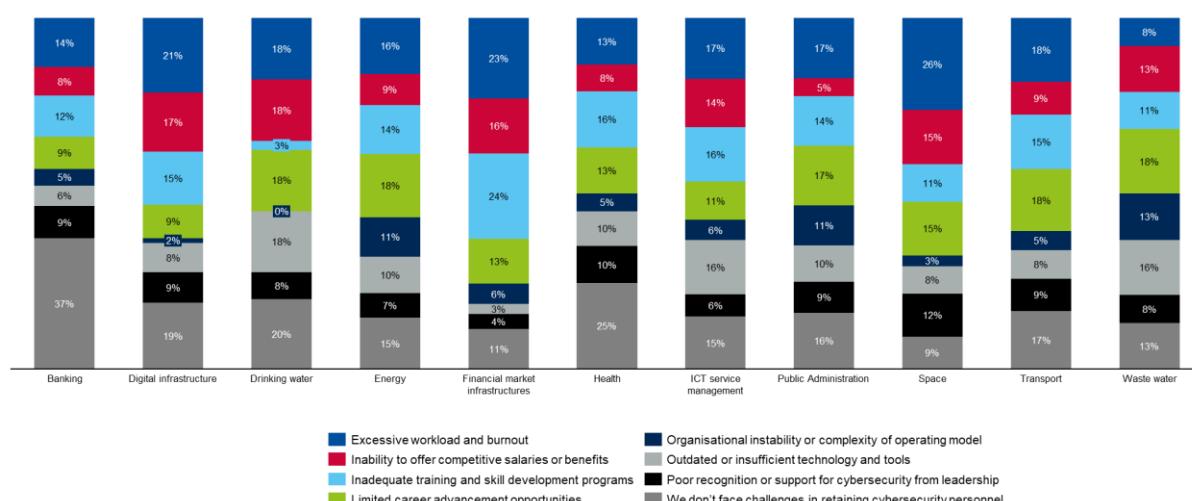
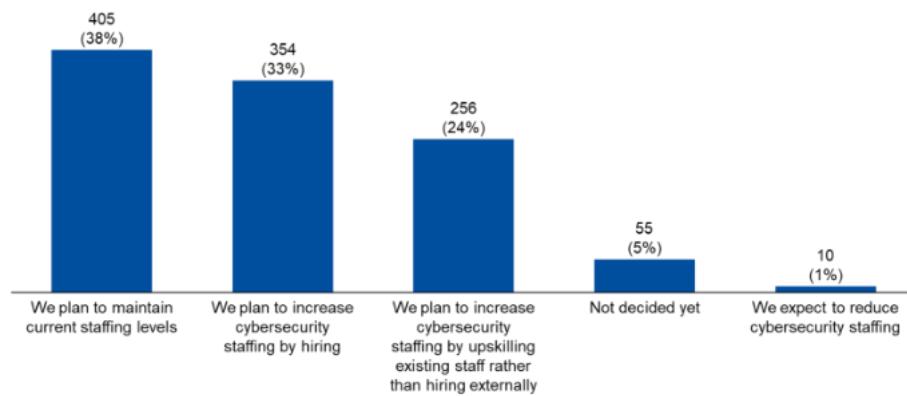


Figure 69 - Challenges to retaining cybersecurity personnel, per sector

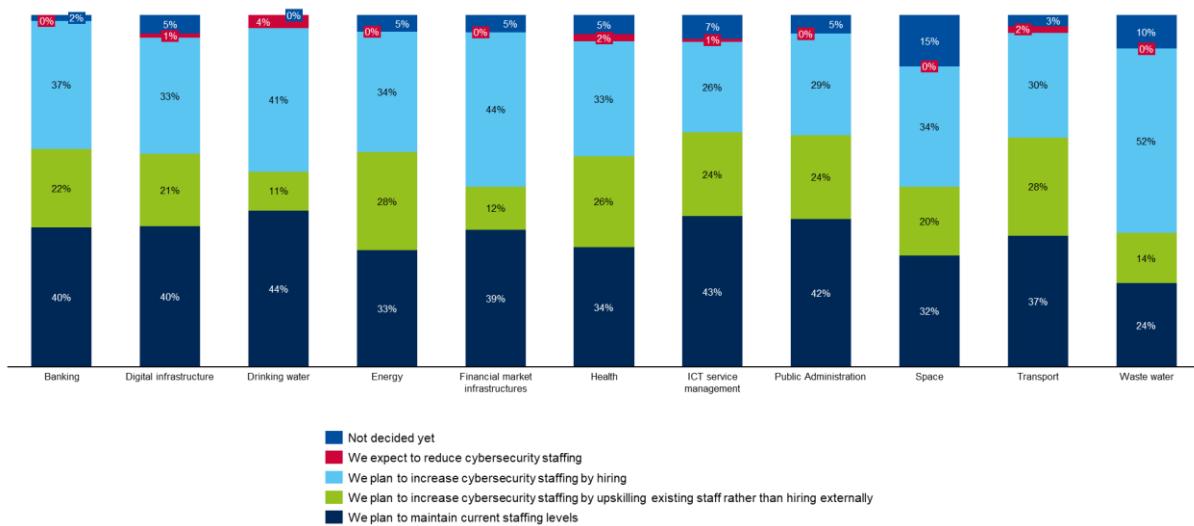
### 3.14 Cybersecurity staffing strategy

**Survey Question:** What best describes your organisation's cybersecurity staffing plan for the next 12 months?

**Across EU view**



**Figure 70 - Cybersecurity staffing strategy**



**Figure 71 - Cybersecurity staffing strategy, per sector**

### 3.15 Cost reduction measures affecting cybersecurity staffing

**Survey Question:** In the past year, did your organisation take any of the following cost reduction measures affecting cybersecurity staffing?

#### Across EU view

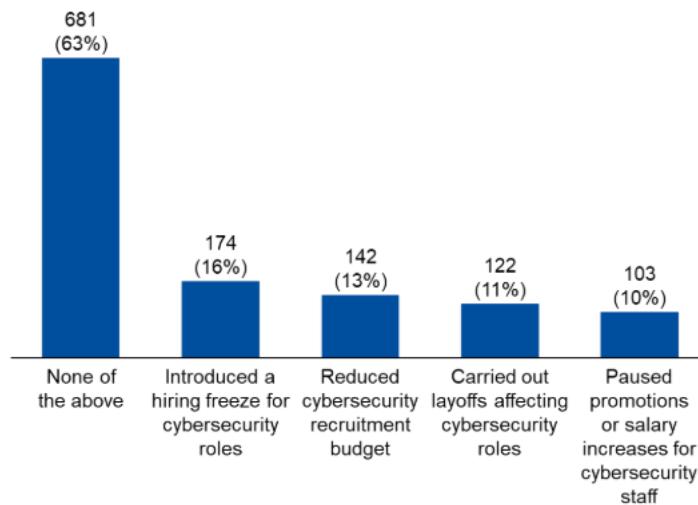


Figure 72 - Cost reduction measures affecting cybersecurity staffing

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

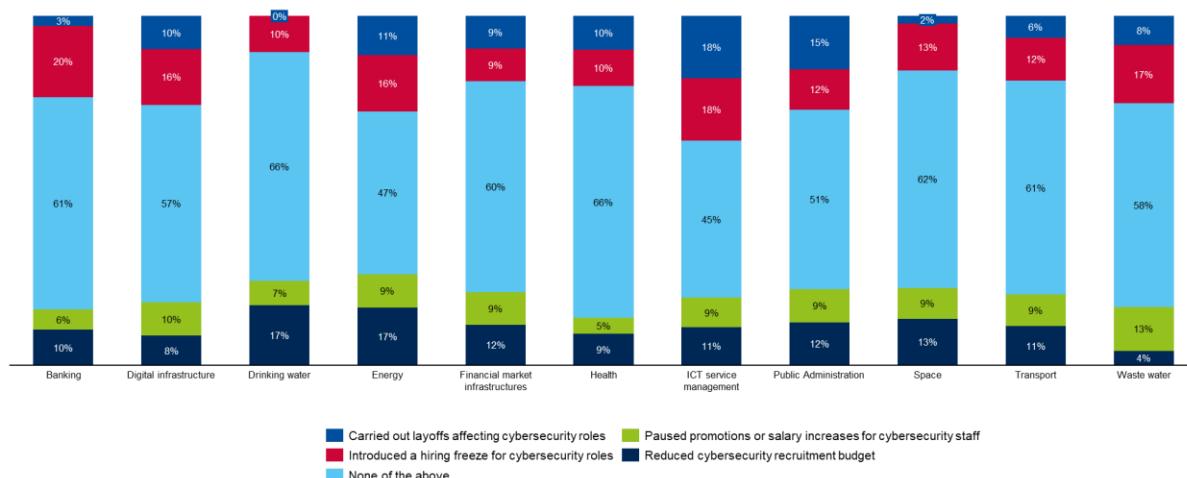


Figure 73 - Cost reduction measures affecting cybersecurity staffing, per sector

### 3.16 Most in-demand cybersecurity skills currently

**Survey Question:** Which of the following are the most in-demand cybersecurity skills in your organisation right now? (Select up to 3)

#### Across EU view

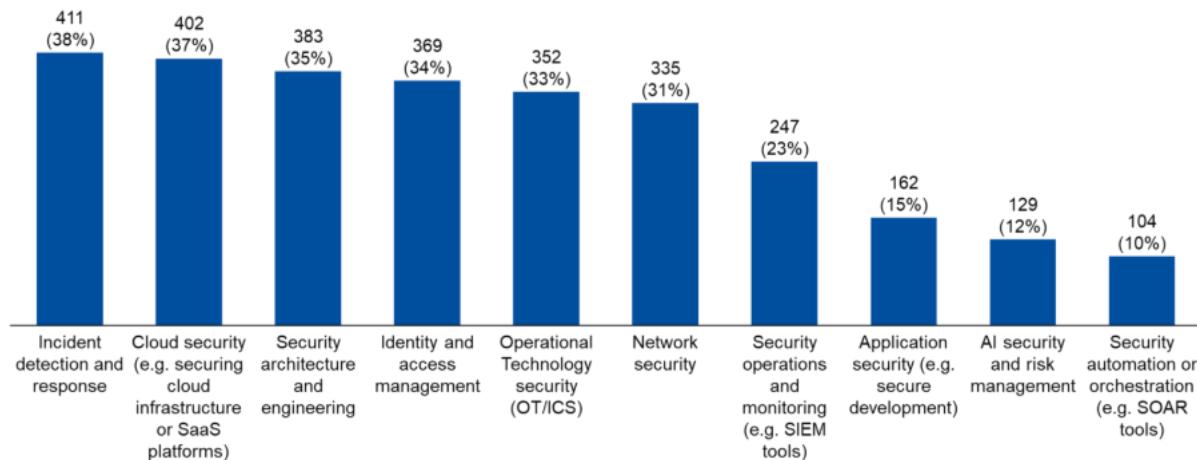


Figure 74 - Most in-demand cybersecurity skills currently

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

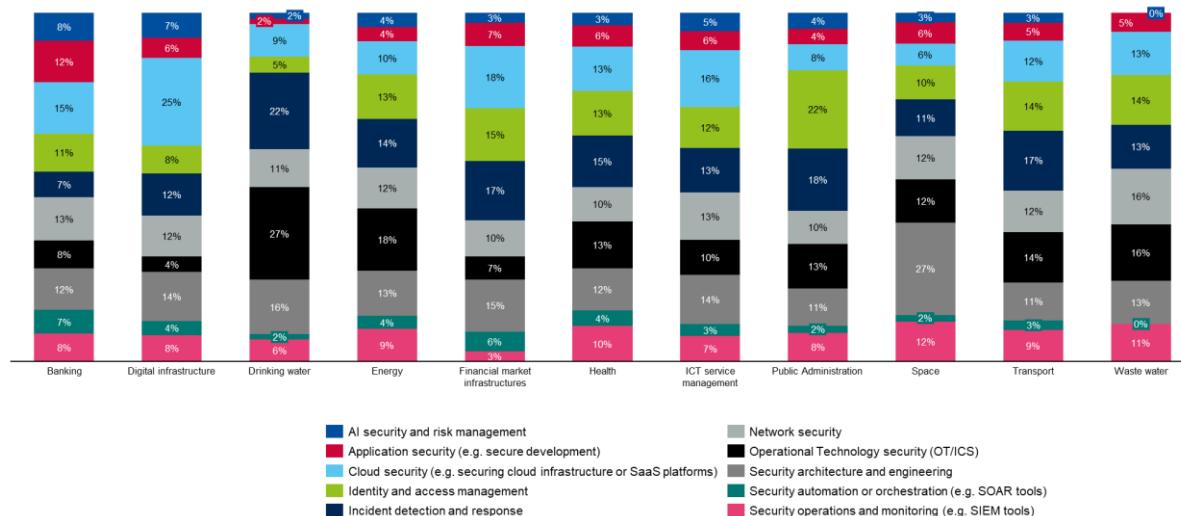


Figure 75 - Most in demand cybersecurity skills currently

### 3.17 Most challenging NIS2 requirements to implement

**Survey Question:** Which of the following NIS2 areas is the most challenging for your organisation to implement?

#### Across EU view

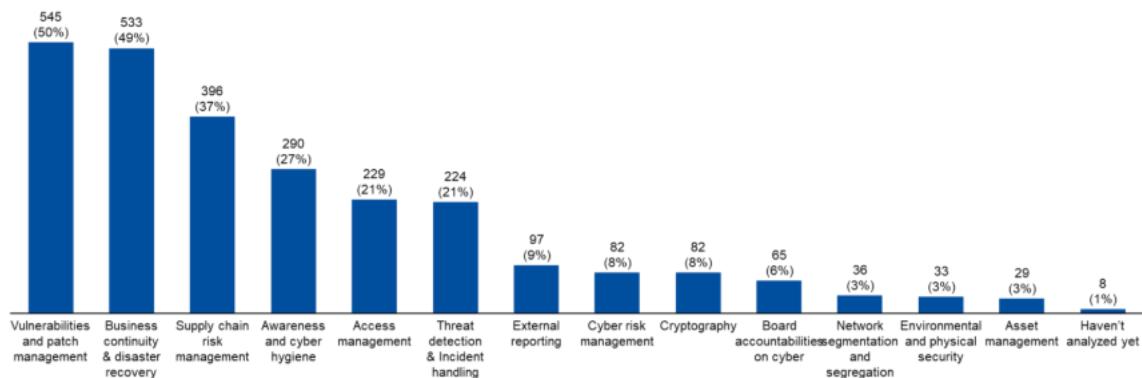


Figure 76 Most challenging NIS2 requirements

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

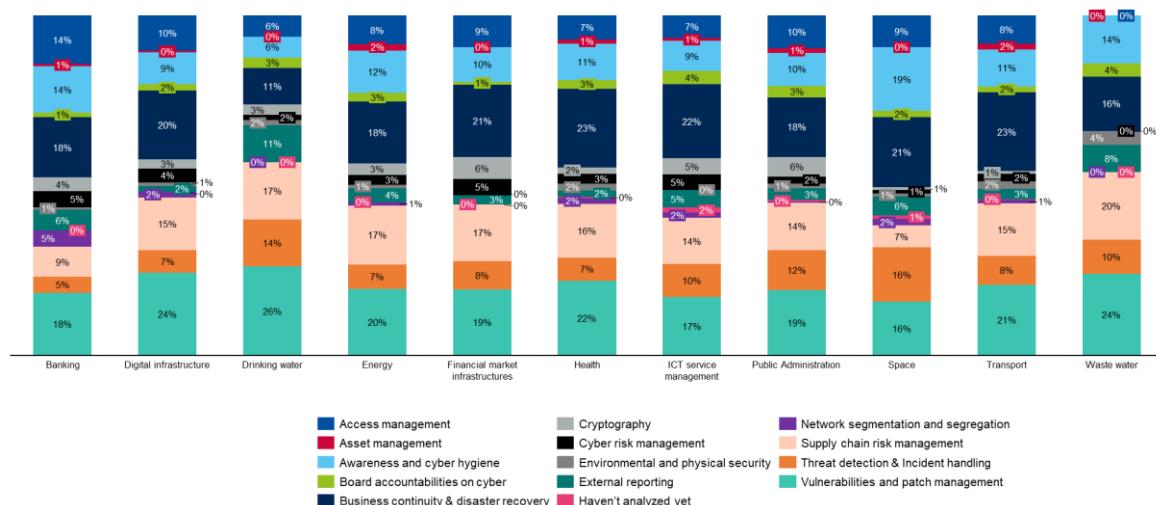
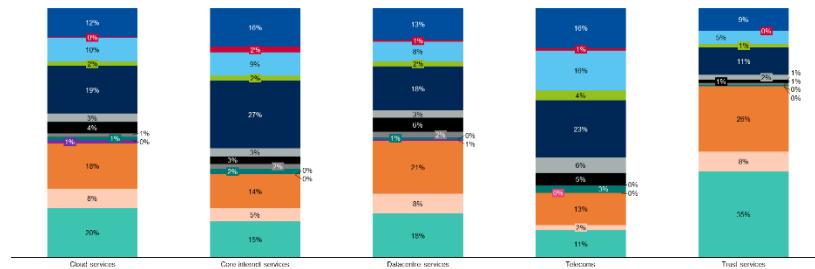
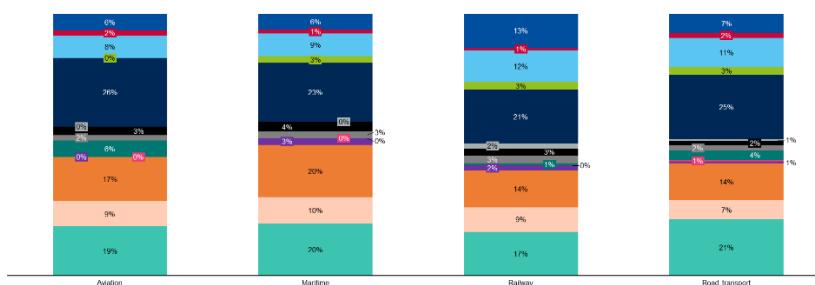


Figure 77 - Most challenging NIS2 requirements, per sector

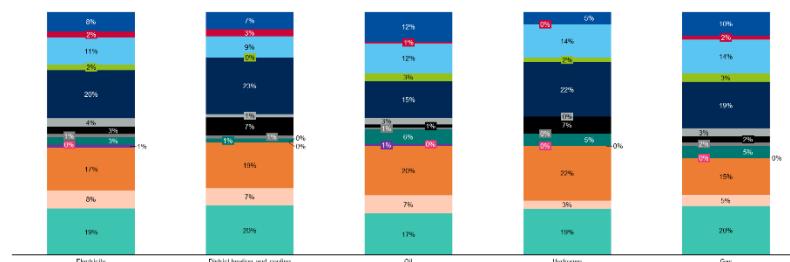
For detailed breakdown per subsector – please consult the next page.



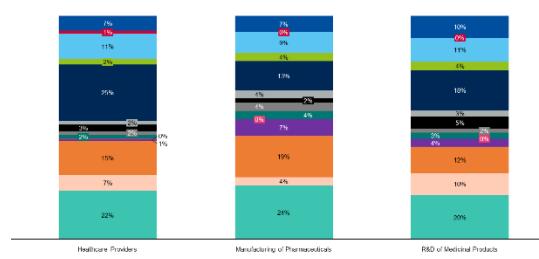
**Figure 78 - Most challenging NIS2 requirements, Digital Infrastructure**



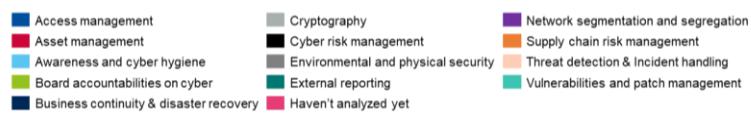
**Figure 79 - Most challenging NIS2 requirements, Transport**



**Figure 80 - Most challenging NIS2 requirements, Energy**



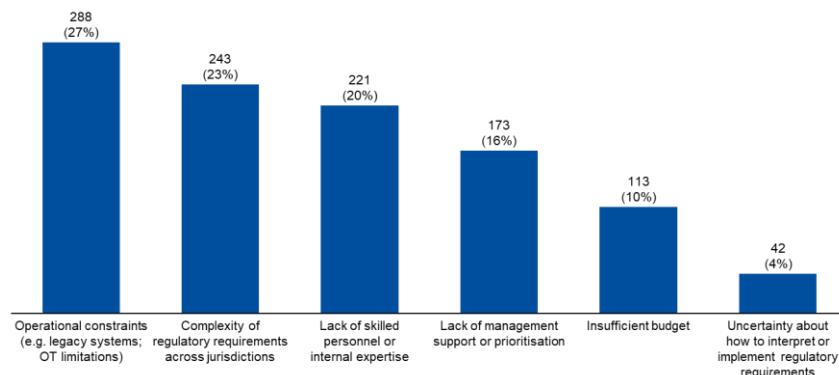
**Figure 81 - Most challenging NIS2 requirements, Health**



### 3.18 Main obstacles to implementing NIS2 requirements

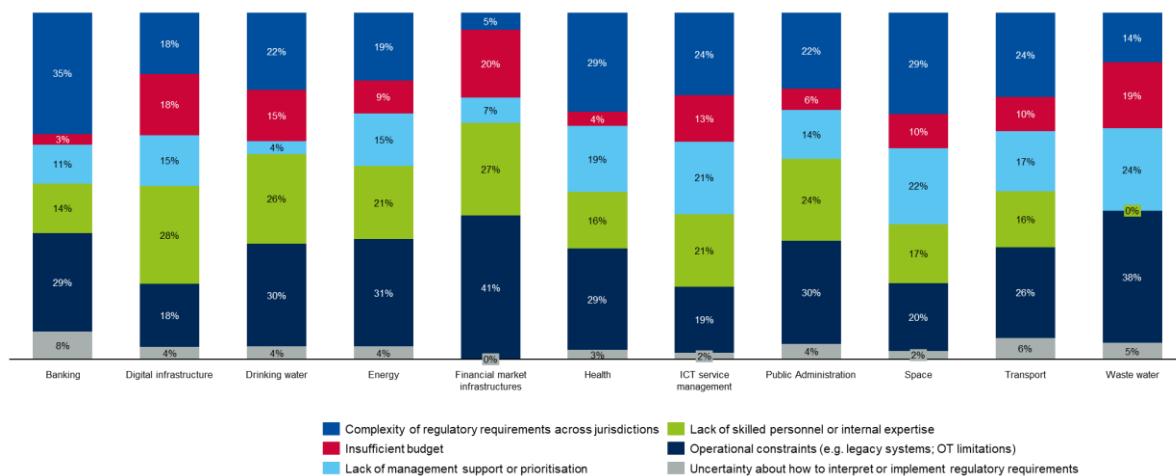
**Survey Question:** What is the main obstacle to implementing these controls effectively?

**Across EU view**



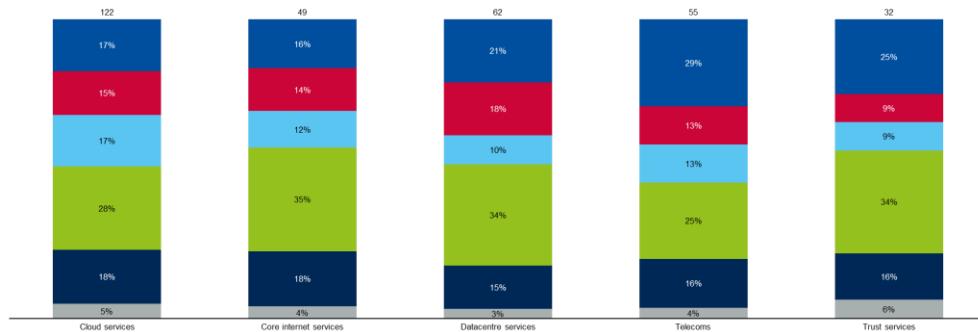
**Figure 82 - Main obstacles to implementing NIS2 requirements**

**Sector view**

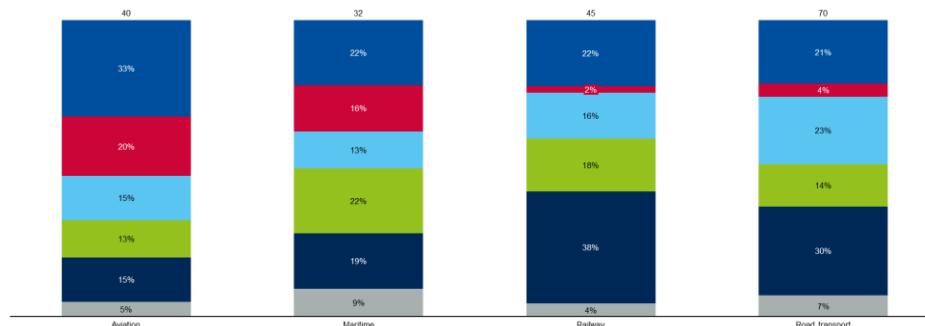


**Figure 83 - Main obstacles to implementing NIS2 requirements**

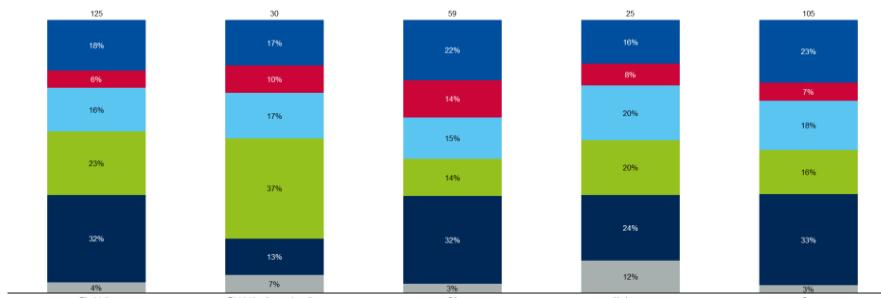
For detailed breakdown per subsector – please consult the next page.



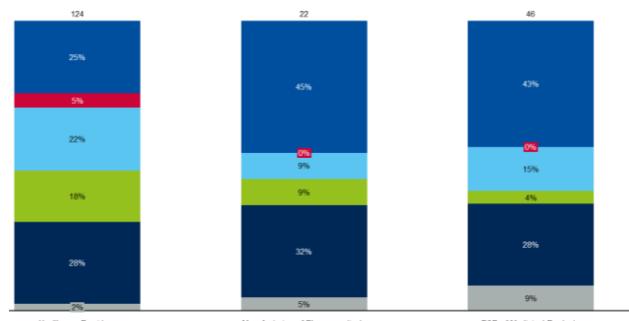
**Figure 84 – Main obstacles to implementing NIS2 requirements, Digital Infrastructure**



**Figure 85 - Main obstacles to implementing NIS2 requirements, Transport**



**Figure 86 - Main obstacles to implementing NIS2 requirements, Energy**



**Figure 87 - Main obstacles to implementing NIS2 requirements, Health**

- Complexity of regulatory requirements across jurisdictions
- Insufficient budget
- Lack of management support or prioritisation
- Lack of skilled personnel or internal expertise
- Operational constraints (e.g. legacy systems; OT limitations)
- Uncertainty about how to interpret or implement regulatory requirements

### 3.19 Cybersecurity assessments

**Survey Question:** Has your organisation conducted any form of cybersecurity assessment or testing (e.g. technical audit, penetration test, red team exercise, maturity assessment) within the past 12 months?

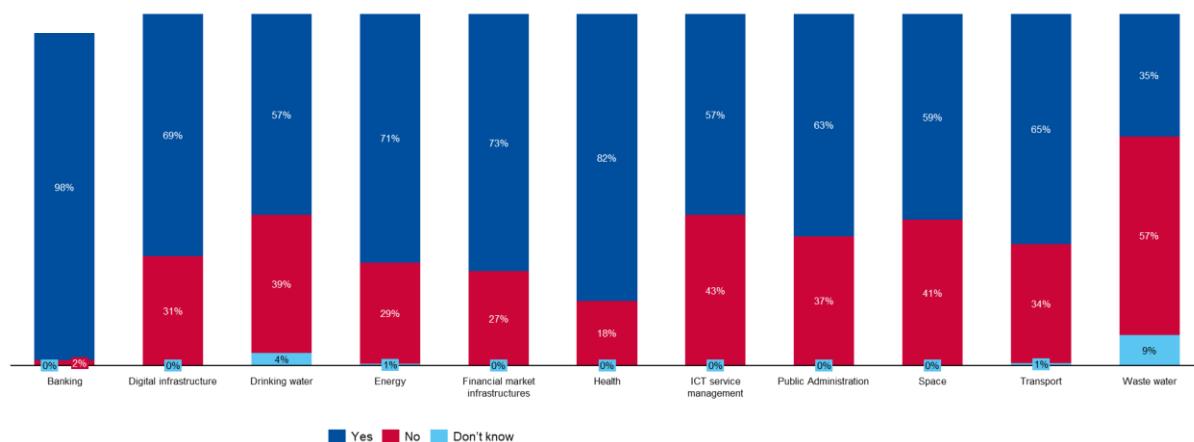


Figure 88 - Proportion of entities having conducted any form of cybersecurity assessment in the past 12 months, per sector

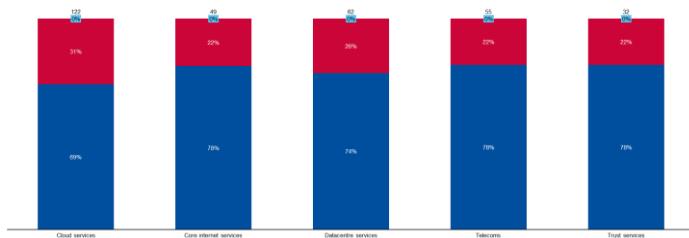


Figure 89 – Cybersecurity assessments, Digital Infrastructure

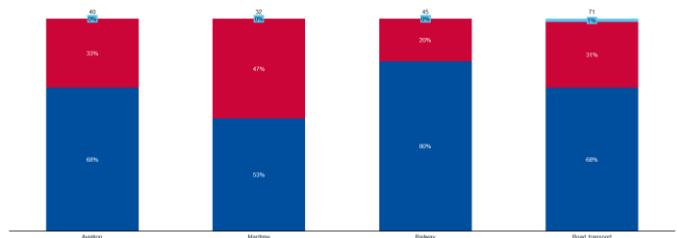


Figure 90 - Cybersecurity assessments, Transport

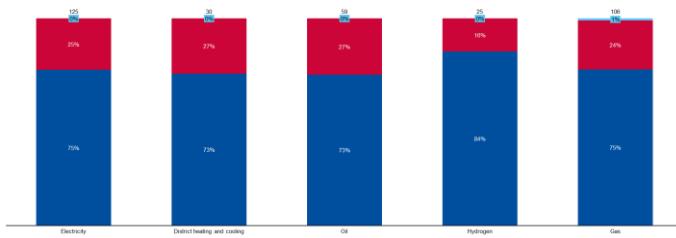


Figure 91 - Cybersecurity assessments, Energy

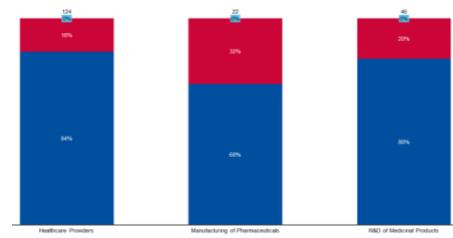


Figure 92 - Cybersecurity assessments, Health

### 3.20 Average time to patch critical vulnerabilities on critical systems

**Survey Question:** What is the average time to patch critical vulnerabilities on your organisation's critical assets (IT and OT)?

#### Across EU view

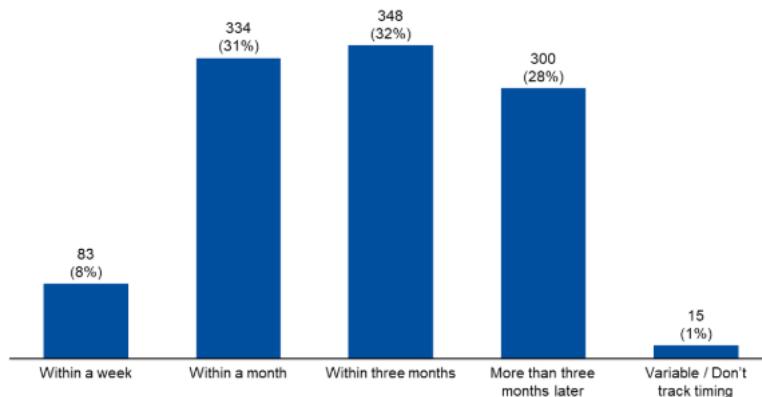


Figure 93 - Average time to patch critical vulnerabilities on critical systems

#### Sector view

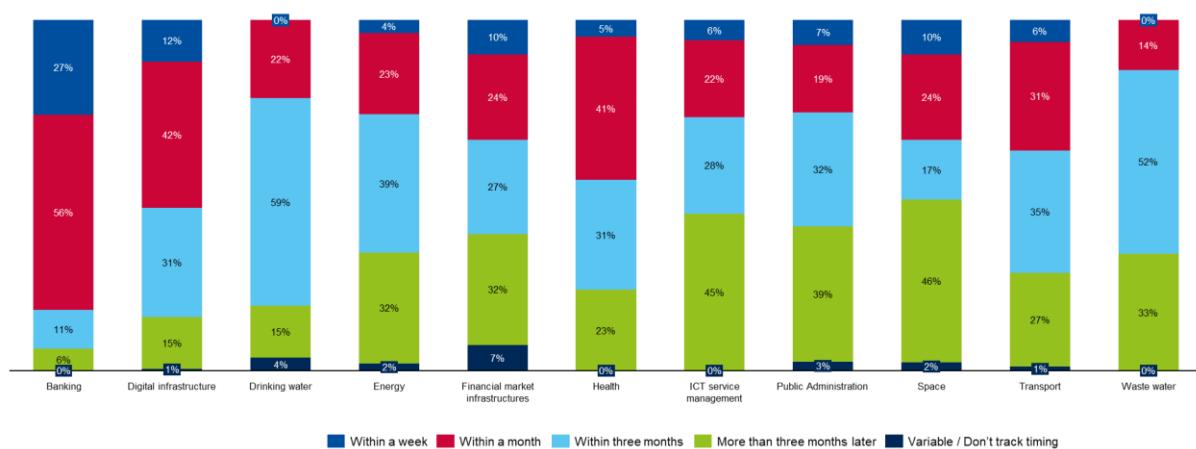
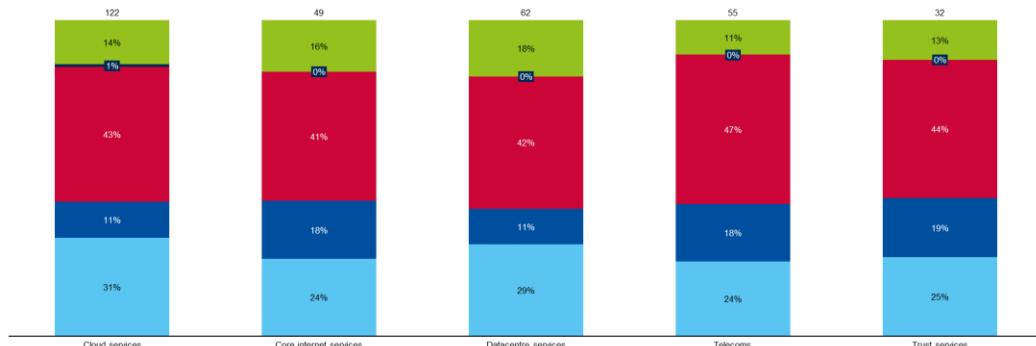
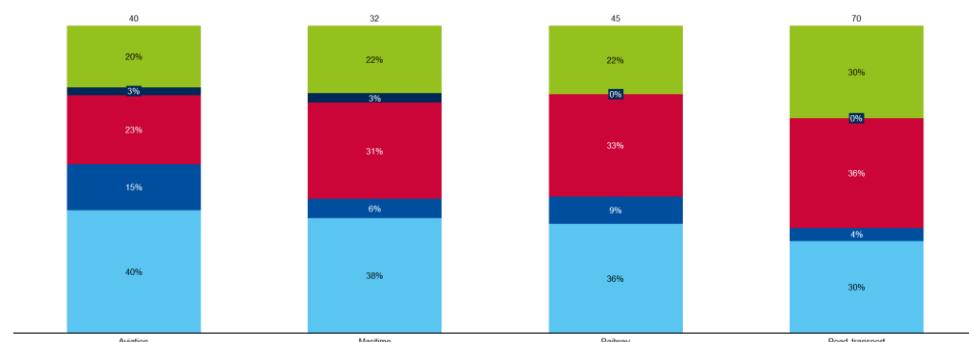


Figure 94 - Average time to patch critical vulnerabilities on critical systems, per sector

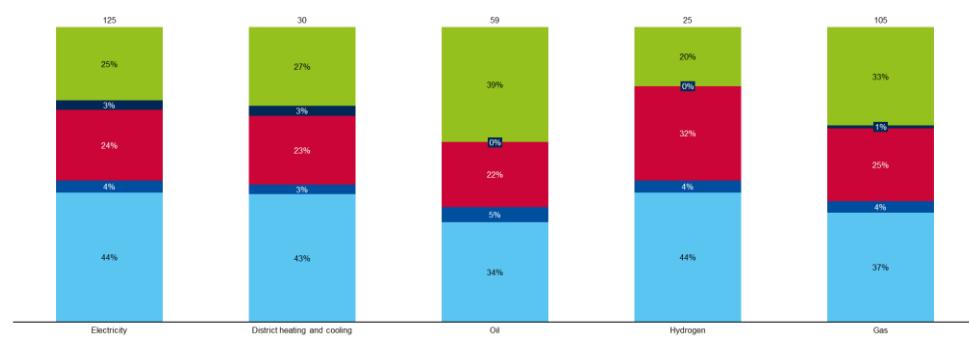
For detailed breakdown per subsector – please consult the next page.



**Figure 95 – Average time to patch, Digital Infrastructure**



**Figure 96 - Average time to patch, Transport**



**Figure 97 - Average time to patch, Energy**



**Figure 98 - Average time to patch, Health**

- More than three months later
- Variable / Don't track timing
- Within a month
- Within a week
- Within three months

### 3.21 Supply chain risk management practices implemented

**Survey Question:** Which of the following supply chain risk management practices are currently in place in your organisation?

#### Across EU view

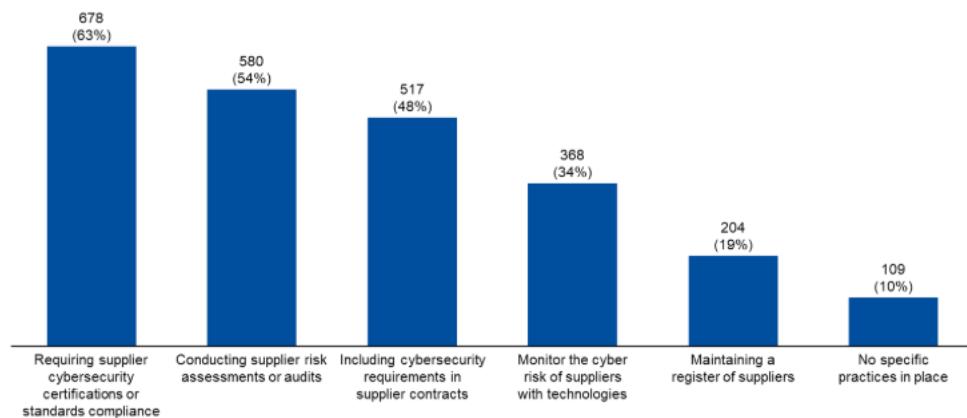


Figure 99 - Supply chain risk management practices implemented

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

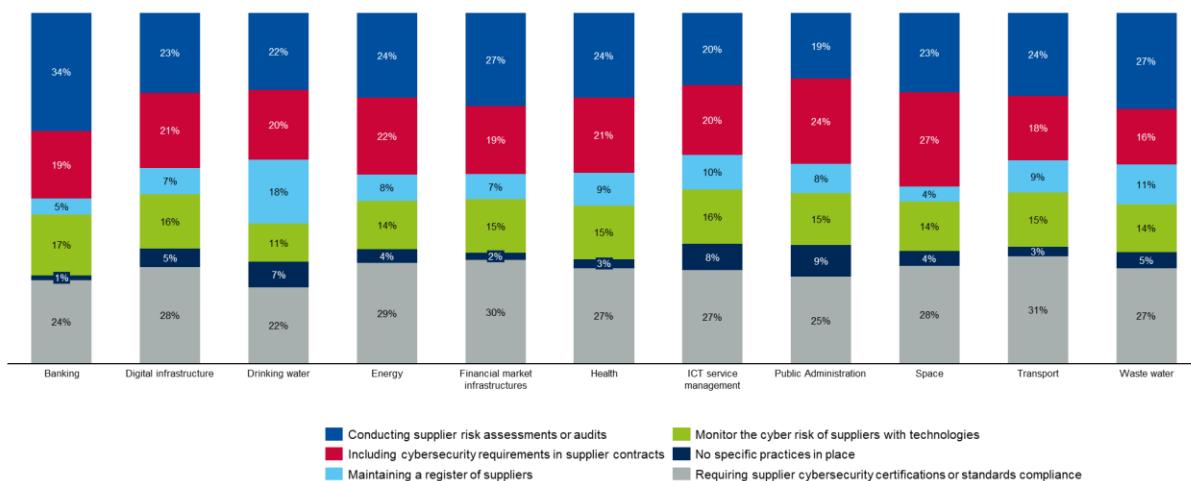


Figure 100 - Supply chain risk management practices implemented, per sector

### 3.22 Characteristics of preferred suppliers of digital products

**Survey Question:** When procuring products with digital elements (hardware or software), which supplier categories do you commonly use? (Select all that apply)

#### Across EU view

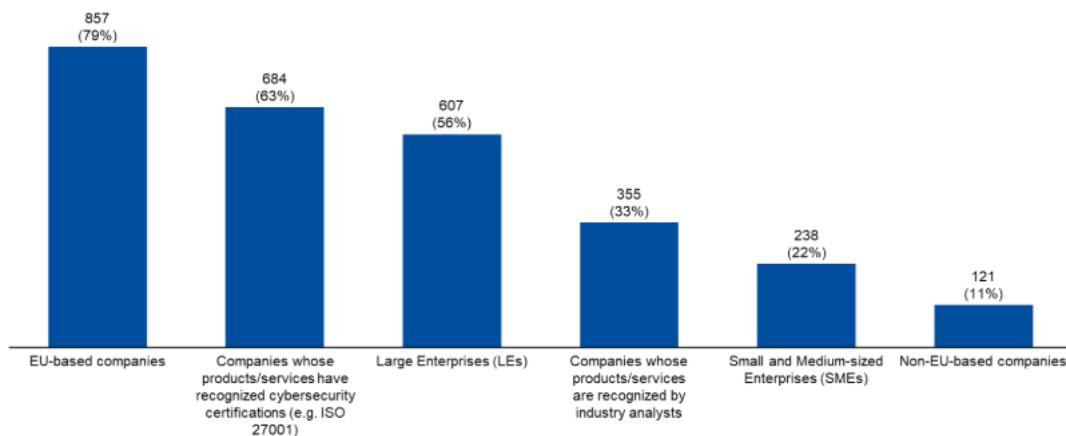


Figure 101 - Characteristics of preferred suppliers of products with digital elements

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

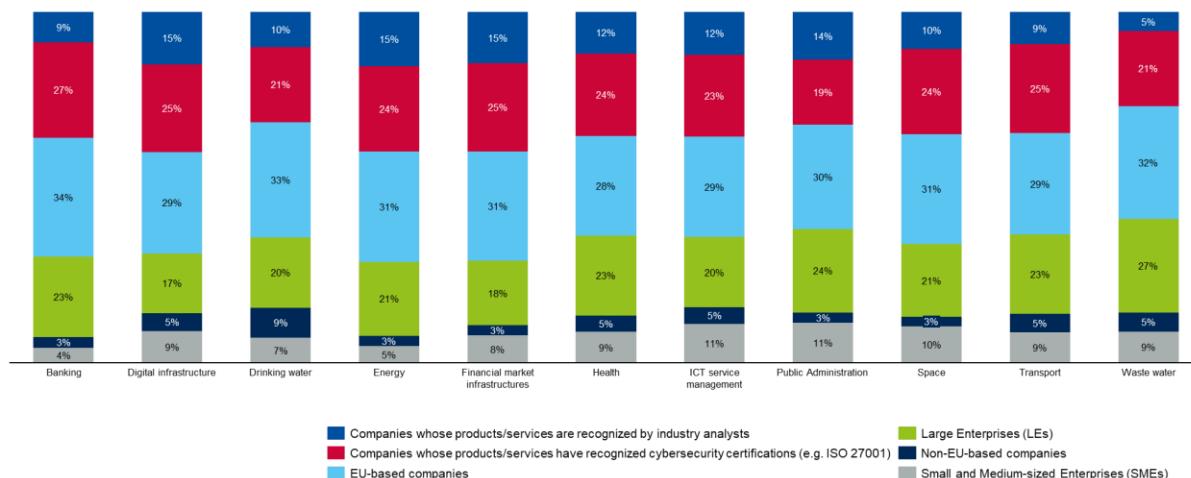


Figure 102 - Characteristics of preferred suppliers of products with digital elements

### 3.23 Information Sharing

**Survey Question:** Does your organisation engage in collaboration and information sharing with others? (Multiple choices possible)

#### Across EU view

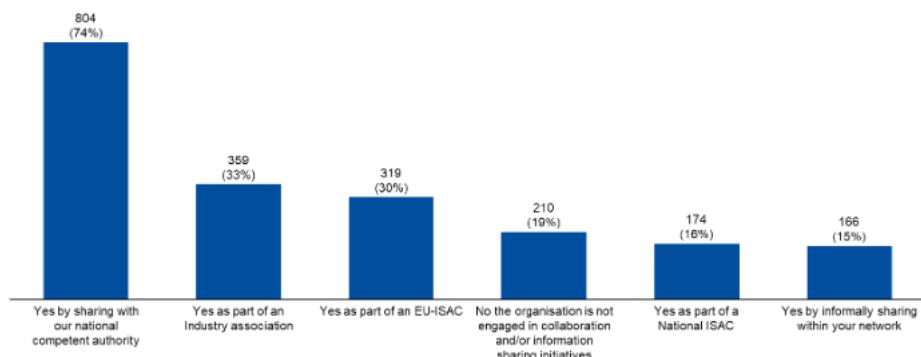


Figure 103 - Participation in information sharing

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

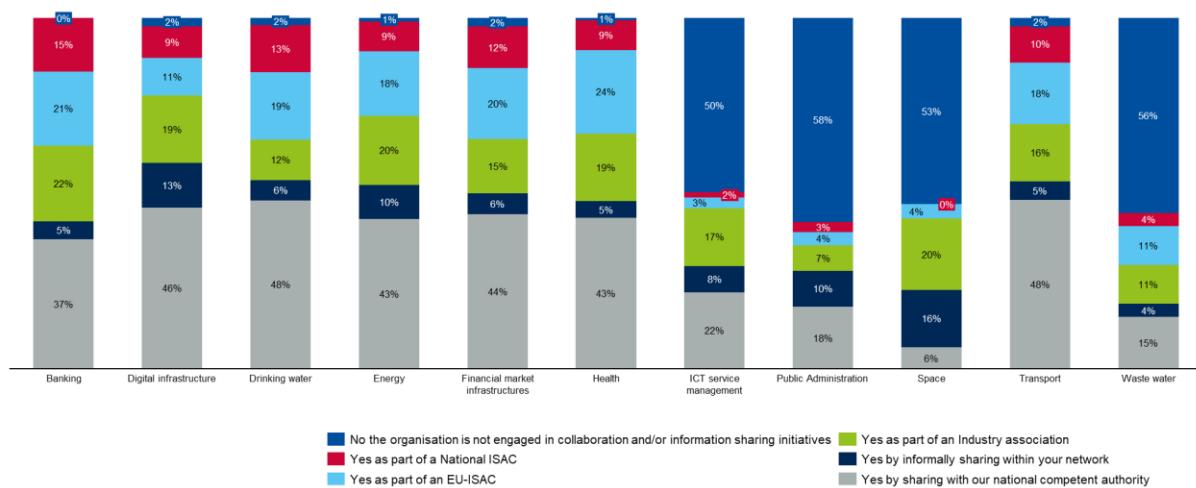


Figure 104 - Participation in information sharing, per sector

### 3.24 Attacks with the greatest operational impact on day-to-day operations

**Survey Question:** In the past 12 months, which type of cyberattack had the greatest impact on your day-to-day operations?

#### Across EU view

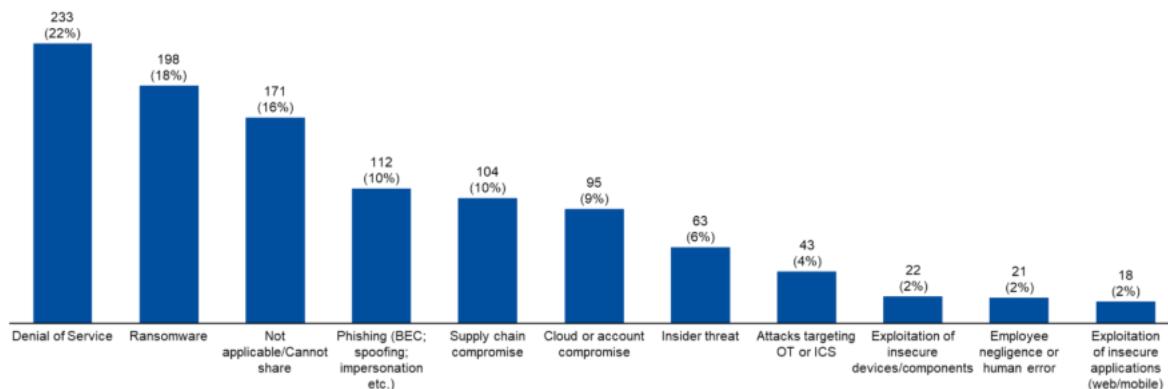


Figure 105 - Attacks with the greatest operational impact on day-to-day operations

#### Sector view

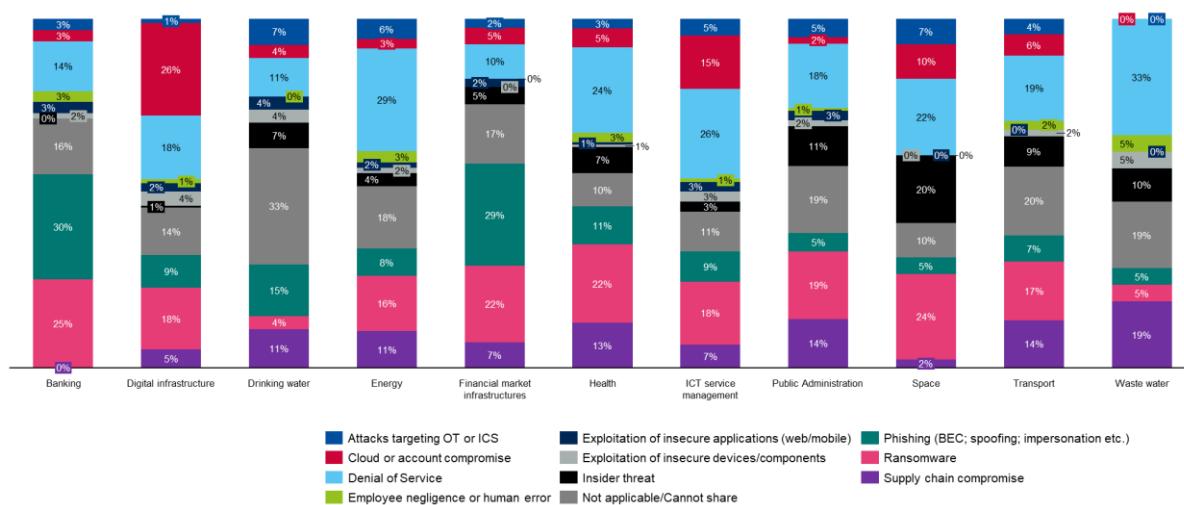


Figure 106 - Attacks with the greatest operational impact on day-to-day operations, per sector

### 3.25 Cybersecurity threats of most concern looking ahead

**Survey Question:** Which of the following cybersecurity risks or attack types concern you the most looking ahead? (Select up to 3)

#### Across EU view

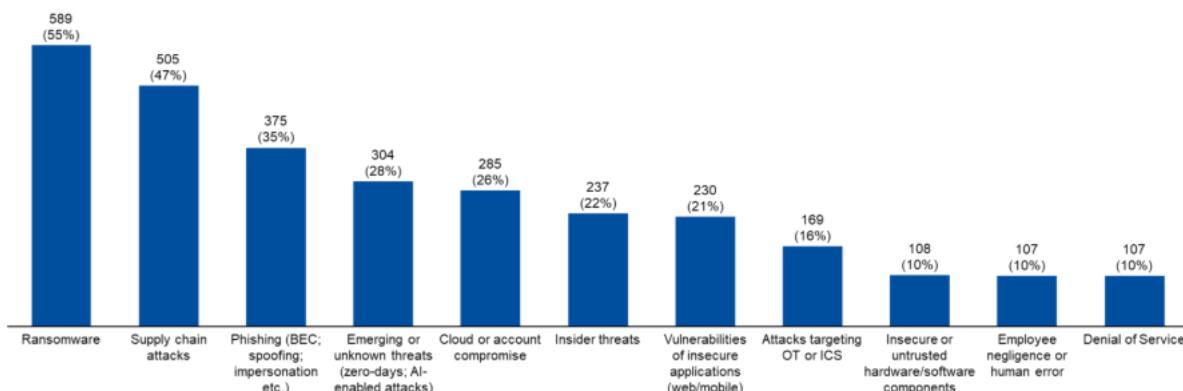


Figure 107 - Cybersecurity threats of most concern looking ahead

#### Sector view

**Disclaimer:** This graph visualises the proportion that each response represents out of all responses received from organisations within the respective sector. Not the proportion of entities within the respective sector, having provided that answer.

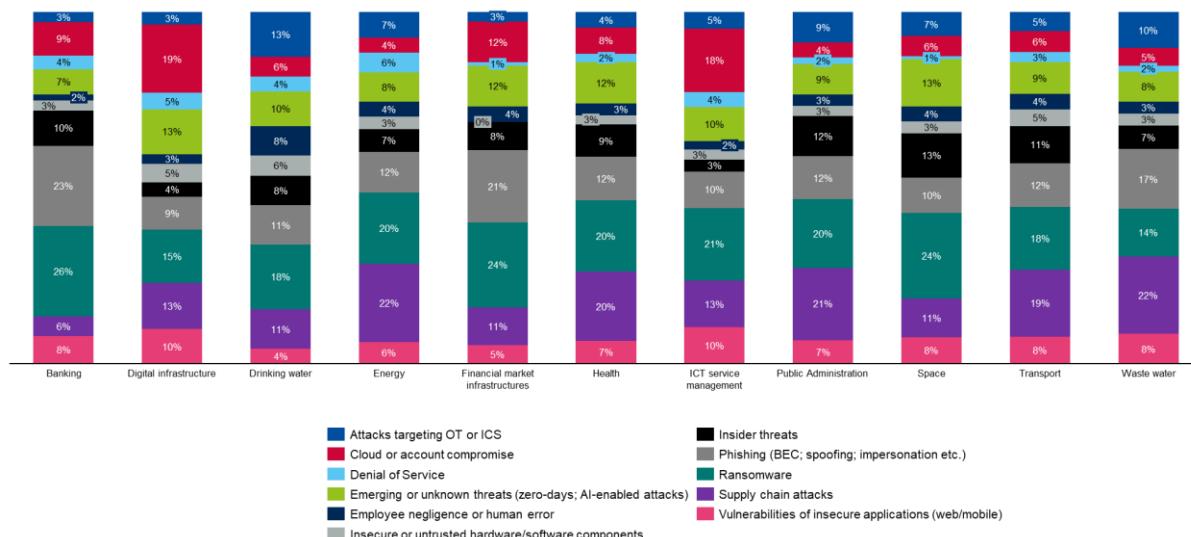


Figure 108 - Cybersecurity threats of most concern looking ahead, per sector

### 3.26 Preparedness against scenarios

**Survey Question:** For each of the following scenarios, would you categorize your organization's current stance as predominantly prepared or unprepared? –

(Cybersecurity preparedness refers to your organisation's ability to anticipate, prevent, respond to, and recover from cyber incidents effectively)

#### A ransomware attack that encrypts critical systems

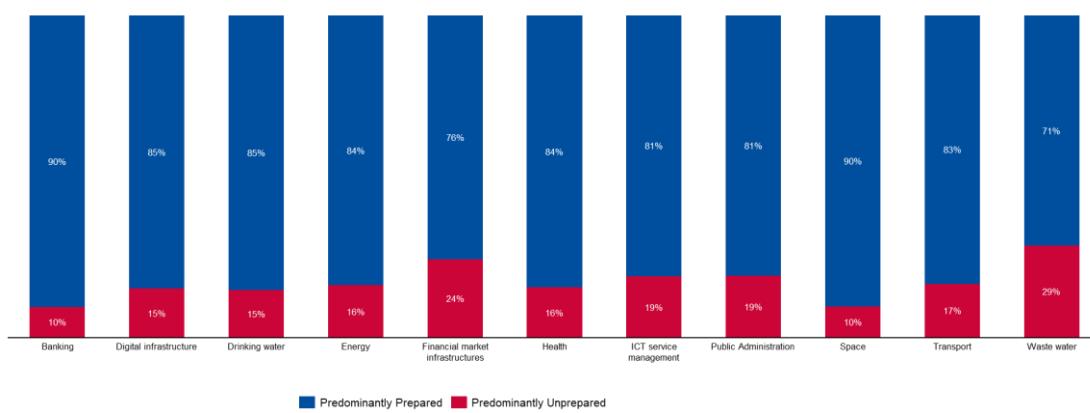


Figure 109 - Preparedness against ransomware, per sector

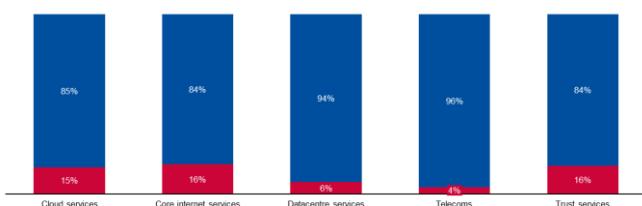


Figure 110 - Preparedness against ransomware, Digital Infrastructure

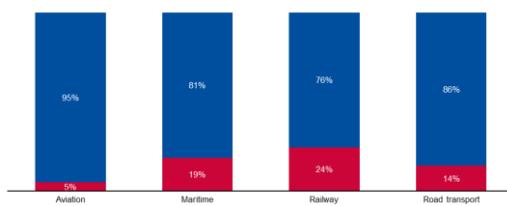


Figure 111 - Preparedness against ransomware, Transport Infrastructure

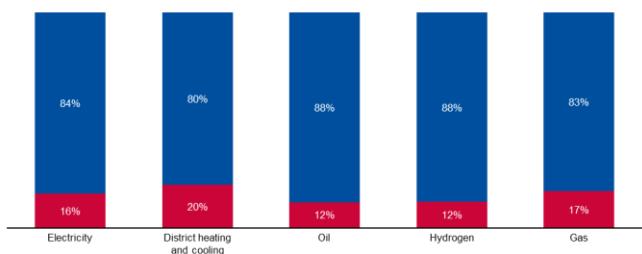


Figure 112 - Preparedness against ransomware, Energy

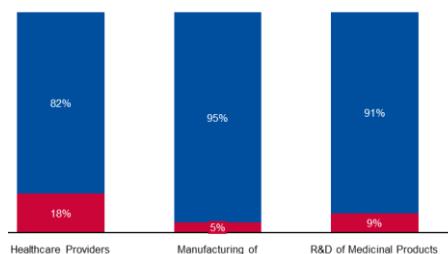


Figure 113 - Preparedness against ransomware, Health

**Survey Question:** For each of the following scenarios, would you categorize your organization's current stance as predominantly prepared or unprepared? –

### A supply chain attack or compromise to a third-party service

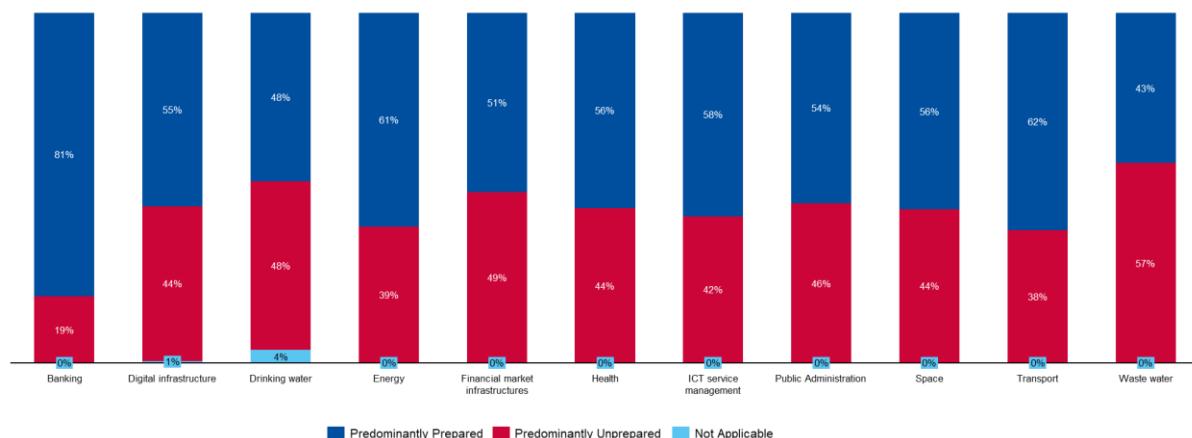


Figure 114 - Preparedness against supply chain attack or third-party compromise

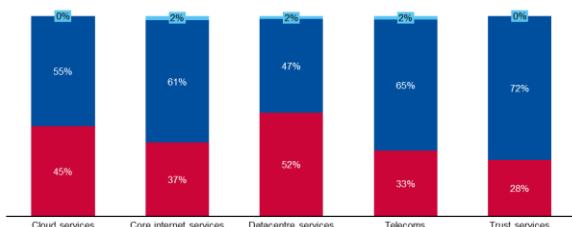


Figure 115 - Preparedness against supply chain attack or third-party compromise, Digital Infrastructure

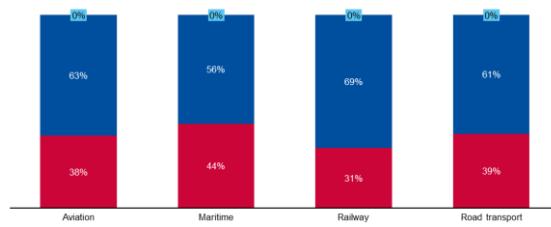


Figure 116 - Preparedness against supply chain attack or third-party compromise, Transport

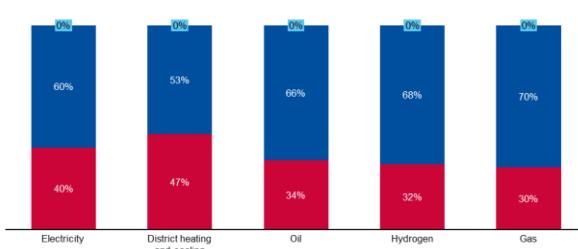


Figure 117 - Preparedness against supply chain attack or third-party compromise, Energy

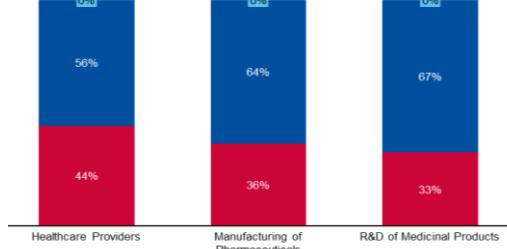
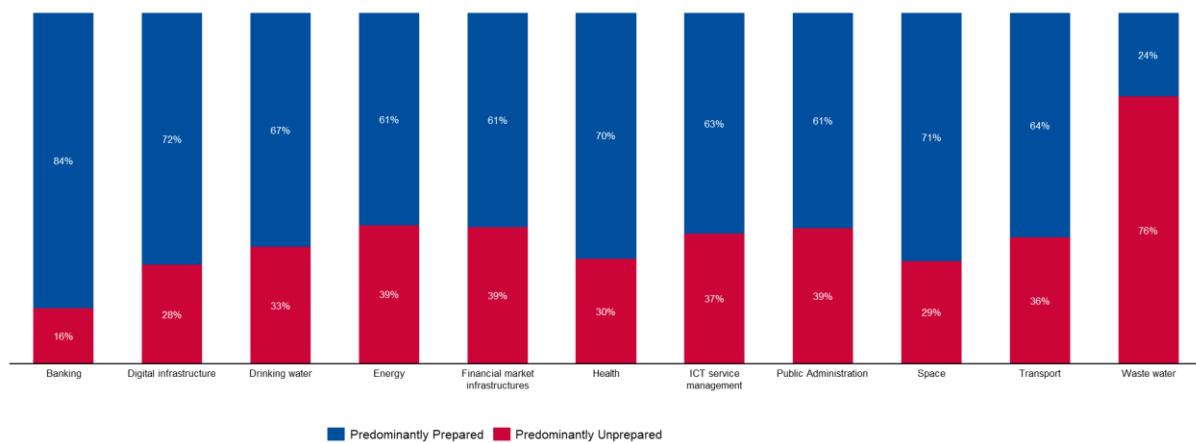


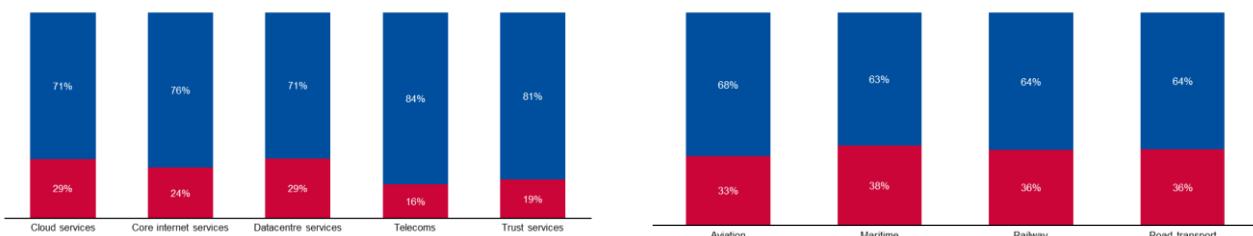
Figure 118 - Preparedness against supply chain attack or third-party compromise, Health

**Survey Question:** For each of the following scenarios, would you categorize your organization's current stance as predominantly prepared or unprepared? –

**A cyberattack causes IT/OT infrastructure outage or degradation**

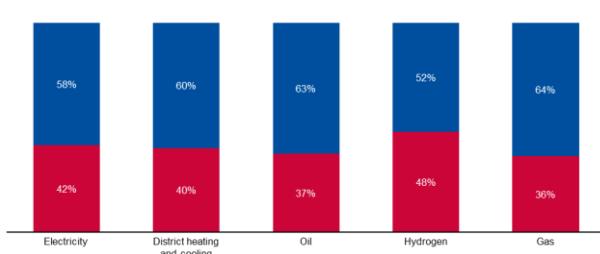


**Figure 119 - Preparedness against attacks causing IT/OT infra outages or degradation, per sector**

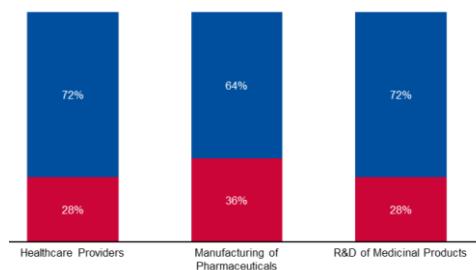


**Figure 120 - Preparedness against attacks causing IT/OT infra outages or degradation, Digital Infrastructure**

**Figure 121 - Preparedness against attacks causing IT/OT infra outages or degradation, Transport**



**Figure 122 - Preparedness against attacks causing IT/OT infra outages or degradation, Energy**



**Figure 123 - Preparedness against attacks causing IT/OT infra outages or degradation, Health**

## SECTION 4

# Survey demographics

## 4. Survey demographics

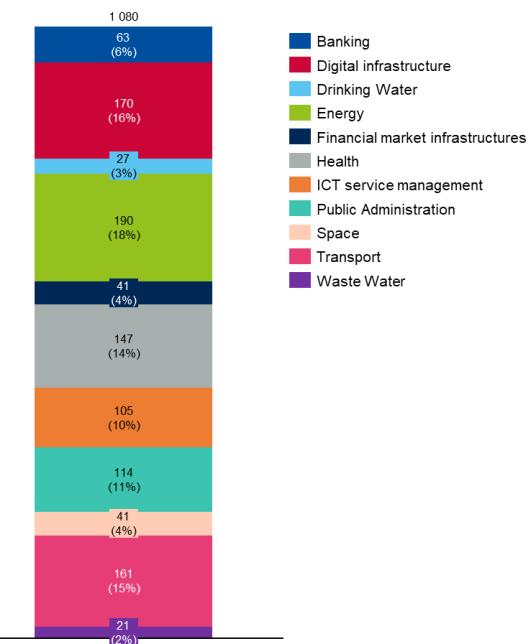


Figure 124 - Sectoral composition of the 2025 study sample

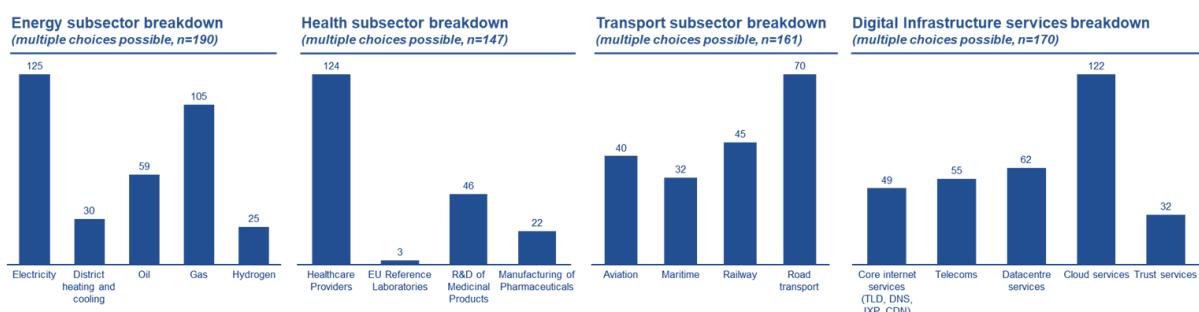
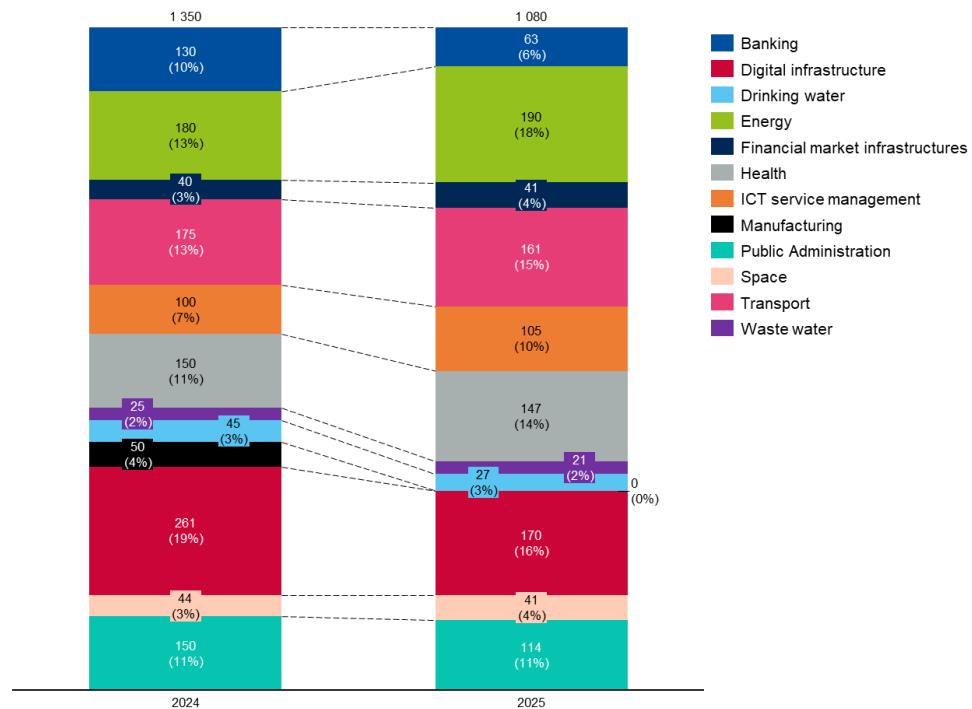
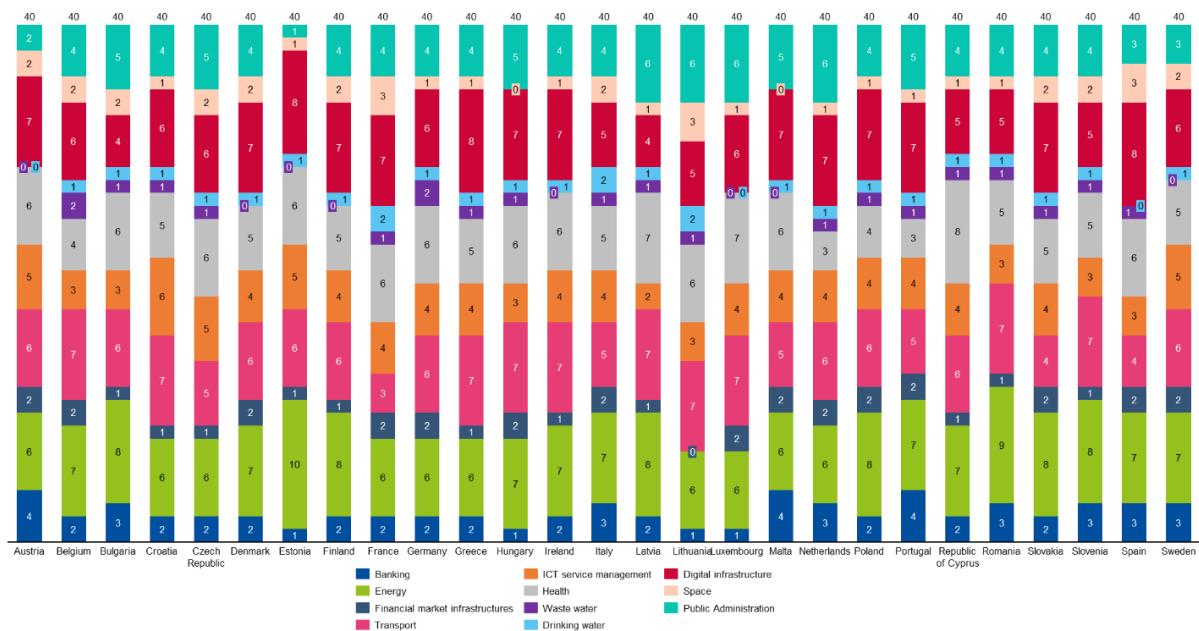


Figure 125 - Subsector composition of the 2025 study sample

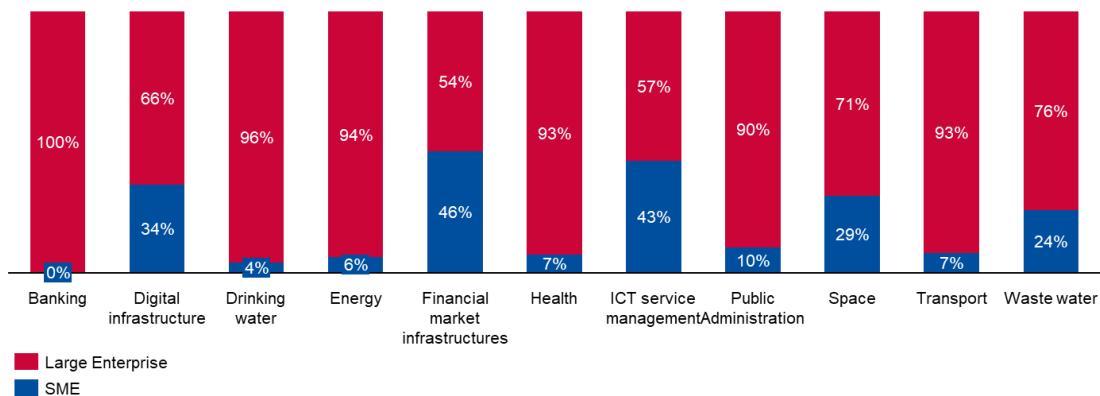


**Figure 126 - Sectoral composition of the 2024 vs. 2025 NIS Investment studies**



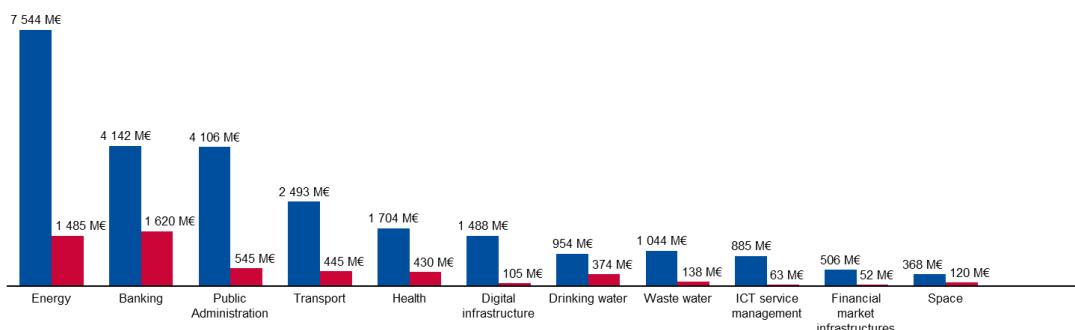
**Figure 127 – Sectoral composition of 2025 study sample, per Member State**

This year's sample consisted of 83% large enterprises and 17% SME, below you may see a breakdown per sector.

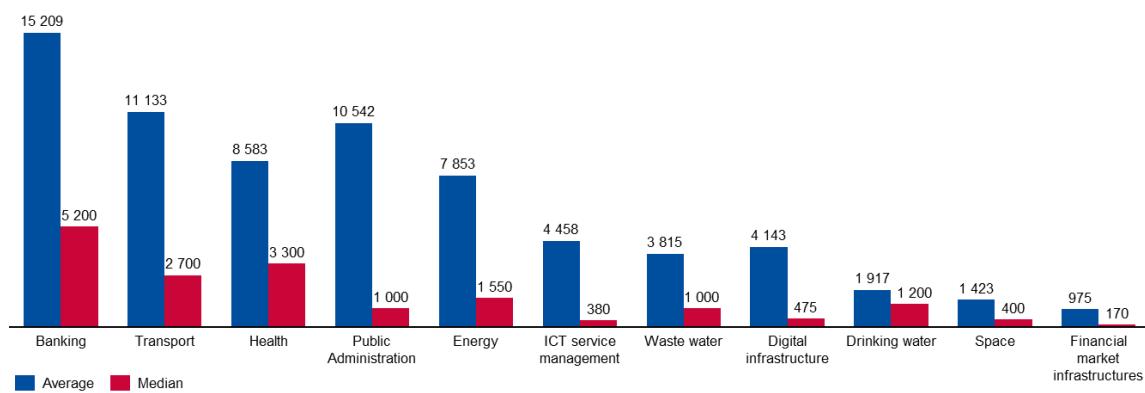


**Figure 128 - SME vs. Large enterprises, per sector**

Participants are also asked to provide an estimated number for the organisation's revenue and full time employees within the business scope and country they have provided. High level estimates or ballpark figures are accepted.



**Figure 129 - Revenues per sector**



**Figure 130 - Employees per sector**

## SECTION 5

# Definitions

## 5. Definitions

### 5.1 Median and average definitions

In this study, both **median** and **average** (arithmetic mean) values are presented to provide a more complete picture of the data.

**The median represents the middle value in a dataset**—half of the entities report higher values and half report lower. It is a robust measure of central tendency, less influenced by extreme values (very large or very small) than the average, and therefore often provides a better sense of what a typical entity reports when data are unevenly distributed. By contrast, the **average is calculated by dividing the sum of all reported values by the number of observations**.

For example, if a few large organisations report exceptionally high cybersecurity investments, the average investment will increase significantly, whereas the median will remain a more representative value. This makes the median especially useful for interpreting data such as cybersecurity budgets or staffing levels, which can vary widely across organisations.

Type	Description	Example	Result
Arithmetic mean	Sum of values of a dataset divided by number of values	$(1 + 2 + 2 + 3 + 4 + 7 + 9)/7$	4
Median	Middle value separating the greater and lesser halves of a dataset	1, 2, 2, 3, 4, 7, 9	3

When median values for investments or full-time equivalents (FTEs) are reported, it is important to interpret them in context. These are absolute figures and can be influenced by the size of the organisation and the structure of the sector in which it operates; a smaller budget or staffing level does not necessarily indicate lower cybersecurity maturity. Additionally, differences in sample composition and size compared with previous studies may affect the results, meaning that changes over time may reflect variations in the sample rather than actual shifts in investment or capability.

### 5.2 SME definition

The main factors determining whether an enterprise is an SME are:

- staff headcount.
- either turnover or balance sheet total

Organisation category	Staff headcount	Turnover	Balance sheet total
Medium-sized	< 250	$\leq \text{€} 50 \text{ m}$	$\leq \text{€} 43 \text{ m}$
Small	< 50	$\leq \text{€} 10 \text{ m}$	$\leq \text{€} 10 \text{ m}$
Micro	< 10	$\leq \text{€} 2 \text{ m}$	$\leq \text{€} 2 \text{ m}$

## **ABOUT ENISA**

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: [www.enisa.europa.eu](http://www.enisa.europa.eu).

## **ENISA**

European Union Agency for Cybersecurity

### **Athens Office**

Agamemnonos 14  
Chalandri 15231, Attiki, Greece

### **Brussels Office**

Rue de la Loi 107  
1049 Brussels, Belgium

[enisa.europa.eu](http://enisa.europa.eu)



Publications Office  
of the European Union

