1. Cybersecurity regulatory framework
2. Evolution of the cybersecurity threat landscape
3. Incidents in finance sector
4. Investments and maturity of the sector
5. Key areas for improvement
CYBERSECURITY REGULATORY FRAMEWORK
NEW LEGISLATIVE TASKS OR ROLES PUT ON ENISA

- Cyber Solidarity Act
- Cybersecurity Act +
- Artificial Intelligence Act
- eIDAS 2
- European Health Data Space legislation
- Cyber Resilience Act
- EUIBAs legislation
- Sectorial legislation (DORA, Electricity Code)
- NIS Directive 2
- Cybersecurity Act
- NIS Directive 1
## LEGISLATION IMPACTING FINANCE SECTOR

<table>
<thead>
<tr>
<th></th>
<th>Security measures</th>
<th>Incident reporting</th>
<th>Crisis management</th>
<th>Certification</th>
<th>Information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>eIDAS2</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DORA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AIA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CRA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DMA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Digital euro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
NIS2 AND DORA OVERLAP

Ensure greater collaboration and information sharing between competent authorities

NIS2 competent authority

DORA supervisory authorities

Supervise security measures

Supervise systemic risks

Digital infrastructure providers

Critical ICT third-party service providers

data centres, cloud computing service providers
Until now there were different incident reporting requirements in Member States

More harmonized 3 step approach in NIS2 and DORA

- 4-24 hours initial report
- 72 hours intermediate report
- 1 month final report
LESSONS LEARNED

ENISA sees cybersecurity as an integral part of EU policies and supports its consistent implementation

- Avoid fragmentation. Ensure harmonized implementation of cybersecurity laws.

- Avoid duplication. Ensure greater collaboration and information sharing.

- Ensure consistency and better alignment of horizontal and sector-specific rules.
EVOLUTION OF THE CYBERSECURITY THREAT LANDSCAPE
**EVOLUTION OF THREAT LANDSCAPE**

- Targeted threats on sectors/groups, Vulnerability exploitation targeting supply chains, Hybrid threats, Threat actors consolidating efforts, Information manipulation,

- Artificial Intelligence, Advanced sophistication by threat actors, Rise of hacktivism, Critical sectors affected

- Cyberthreats-as-a-service model
  - Vulnerability exploitation
  - Misinformation/Disinformation

- Ransomware, DoS, Supply Chain
  - Threats to data

- Malware, DoS
  - Web attacks
  - Cryptojacking

2019

2024
INCIIDENTS IN FINANCE SECTOR
2,580 incidents, with an additional 220 incidents affecting more than one EU MS.
NIS INCIDENT REPORTING 2020-2022

Number of incidents per sector per year

- Communications: 2020 - 95, 2021 - 90, 2022 - 88
- Digital Services: 2020 - 36, 2021 - 32, 2022 - 34
- Finance: 2020 - 12, 2021 - 5, 2022 - 0
- Government Services: 2020 - 24, 2021 - 14, 2022 - 20
- Health: 2020 - 262, 2021 - 252, 2022 - 284
- Other: 2020 - 14, 2021 - 4, 2022 - 0

Legend:
- Red: 2020
- Blue: 2021
- Black: 2022
NIS INCIDENT REPORTING – FINANCE SECTOR

Nature of the incident (%)

- Human errors: 9%
- Malicious actions: 24%
- Natural phenomena: 1%
- System failures: 66%

Technical causes (%)

- Other: 62%
- Faulty software changes/update: 21%
- Software bug: 10%
- DDoS attack: 10%
- Hardware failure: 2%
- Faulty hardware changes/update: 1%
- wildfire: 0%
- Policy/Procedure flaw: 0%
INVESTMENTS & MATURITY OF THE SECTOR
NIS IMPLEMENTATION BUDGETS

<table>
<thead>
<tr>
<th>Industry</th>
<th>Average</th>
<th>Median</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Search Engine</td>
<td>11.0%</td>
<td>10.5%</td>
</tr>
<tr>
<td>Digital infrastructures</td>
<td>10.0%</td>
<td>10.0%</td>
</tr>
<tr>
<td>Financial market infrastructures</td>
<td>10.0%</td>
<td>10.0%</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>10.0%</td>
<td>10.0%</td>
</tr>
<tr>
<td>Online Marketplace</td>
<td>9.2%</td>
<td>9.4%</td>
</tr>
<tr>
<td>Banking</td>
<td>8.0%</td>
<td>7.6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>6.8%</td>
<td>6.7%</td>
</tr>
<tr>
<td>Drinking water supply and distribution</td>
<td>6.4%</td>
<td>6.3%</td>
</tr>
<tr>
<td>Transport</td>
<td>5.7%</td>
<td>5.7%</td>
</tr>
<tr>
<td>Energy</td>
<td>5.3%</td>
<td>5.0%</td>
</tr>
</tbody>
</table>
CYBERSECURITY FTES

% of contractors

Domains with most internal resources

IS FTEs hires in next 2 years
INFORMATION SECURITY GOVERNANCE

Management receives training

- Yes: 542 (50%)
- No: 533 (49%)
- I don’t know: 5 (0%)

Management approves security measures

- Yes: 877 (81%)
- No: 202 (19%)
- I don’t know: 1 (0%)

3rd party cyber risk management policy

- Yes: 835 (77%)
- No: 240 (22%)
- I don’t know: 5 (0%)
NIS 360 - ASSESSMENT OF CRITICALITY AND MATURITY

PRELIMINARY INFORMATION
KEY AREAS FOR POLICY ATTENTION

1. Third party risk management
2. Incident reporting
3. Supervision
FOR MORE INFORMATION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 15231
Attiki, Greece

📞 Evangelos.Ouzounis@enisa.europa.eu
✉️ info@enisa.europa.eu
🌐 www.enisa.europa.eu