Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Sanctions and Responsibilities under the CRA

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Why Sanctions Exist

The goal of sanctions is **not to punish**, but to **protect** users, markets, and fair competition.

When one company ignores cybersecurity duties, it puts everyone else at risk.

So, the CRA creates **clear accountability** — everyone knows their role, and what happens if they fail to meet it.

Who Is Responsible

Responsibility under the CRA depends on the role:

The **manufacturer** is responsible for design, security updates, and vulnerability reporting.

The **importer** must verify the CE mark and documentation.

The **distributor** ensures visible compliance and reacts to incidents.

If one of these fails, they can all be held **jointly responsible**, especially if they knew about the issue and did nothing.

Types of Non-Compliance

1

Administrative — missing documents or CE marking.

2

Technical — product does not meet cybersecurity requirements.

3

Behavioral — failure to report incidents, hide vulnerabilities, or ignore risks.

Possible Actions by Authorities

1

Request missing documentation or risk analysis.

2

Conduct on-site inspections or technical testing.

3

Order a **product withdrawal** or **recall**.

4

Notify ENISA and other EU countries through the **Safety Gate** system.

Financial Penalties

Sanctions are described in **Article 53**.

The maximum fine is up to **15 million euros** or **2.5% of the company's global turnover** — whichever is higher.

Lower fines apply for administrative issues (like missing DoC or CE mark), and higher fines for ignoring vulnerabilities or hiding incidents.

These are similar to GDPR penalties — the idea is that cybersecurity must be taken just as seriously as data protection.

Corrective Measures

Fix	Apply	Improve
Fix documentation gaps	Apply patches	Improve vulnerability handling process

Shared Accountability

Another key point — the CRA promotes **shared accountability**.

Manufacturers, importers, and distributors are all part of the same chain.

So, if one link breaks, everyone must help fix the problem.

The message is clear: **no one can say “it’s not my fault.”**

Cybersecurity is a shared duty in the digital market.

Lessons Learned

When we look at past EU regulations, we see a clear trend: transparency and traceability reduce sanctions.

The more you document, communicate, and cooperate — the safer your company is legally.

The CRA continues this philosophy — “**document, prove, and improve.**”

So even if mistakes happen, what matters is how you respond.

Final Words

We learned **which products** fall under the Act.

We saw **who is responsible** – manufacturers, importers, and distributors.

We explored **what they must do** – declarations, documentation, and reporting.

And we discussed **what happens if they don’t comply.**

Next Session – Technical Requirements and Standards

International and regional standards like **ISO/IEC 27001**, **ISO 17025**, **ISO 17065**, and **ETSI EN 303 645**.
– How these are applied in **testing laboratories and certification assessments**.
– The idea of **horizontal standards** (covering all products) and **vertical standards** (for specific sectors).
– Initiatives such as **STAN4CR** and **CYBERSTAND** for sector-specific applications.

Key message and next step

Cybersecurity is not only a technical goal — it's a shared legal and ethical responsibility.

Next session – 10 November 2025: Technical requirements, standards, and certification (ISO, ETSI, ENISA, EUCC).

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitev@dihtrakia.org