CYEN

ISTITUTO DI INFORMATICA E TELEMATICA

ECCO
European Cybersecurity COmmunity

How to take control the Cybersecurity Risk before it takes control of us?

July 4 at 14:00 - 15:00 CET, online

Christian Banse

Fraunhofer AISEC/ECCO

Iva Tasheva

CYEN

Artsiom Yautsiukhin

IIT CNR

CYEN

ISTITUTO DI INFORMATICA E TELEMATICA

ECCO
European Cybersecurity COmmunity

Christian Banse
Fraunhofer AISEC/ECCO

Iva Tasheva
CYEN

Artsiom Yautsiukhin
IIT CNR

14:00	14:10	14:20	14:30	14:35	14:40	14:55
Intro	Cybersecurity risk management basics	Relevant EU Legislation	Cybersecurity risk management challenges	Future research needs	Q&A	Conclusions and next steps

ECCO
European Cybersecurity COmmunity

INTRO

ECCO Community Roadmapping WG

- **Governance & Participants**
- Chairs:
  - Roadmapping: Christian Banse (Fraunhofer AISEC)
  - Development of the Community: Fabio Martinelli (CNR)
- ECCO Proto-Community on “Road-Mapping”:
  - The members of this Community Group are stemming from the ECCO experts and the ones in the initial proposal (from ECSO and the 4 Pilots).
  - The initial experts have been carefully selected to ensure a diverse composition, with contributors representing the research and industry community …
  - or with close links to ensure an interesting mix of competencies for the identification of relevant topics in support to the ECCC Strategic Agenda implementation and as such the European cybersecurity ecosystem.
- It is in the process to be expanded with other experts from ECCO proposal and according to suggestions by ECCC, NCCs, etc.

ECCO Community Roadmapping WG (II)

- **Objectives**
- The initial objectives of the ECCO Community Group on road-mapping are:
  - **Build the ECCO proto-community of experts** on road-mapping for capability and capacity building **to address the priorities of the Strategic Agenda** (future DEP projects and pan-European actions).
  - Map concepts from the **ECCC Strategic Agenda to other roadmaps** (e.g. results of pilots, ECSO, ENISA, etc.) as well as to the cyber resilience landscape.
  - **Support the NCCs in the implementation** of the Strategic Agenda's Action Plan, e.g., through a series of webinars.

Initial planned webinars

- Perform knowledge sharing webinars with ECCC, NCCs and wider community

- Initial topics identified by the community WG to be covered

1. Cyber-Resilience
2. Digital Twins and Cyber Security
3. Trustworthy AI
4. **Cyber Risk Management (TODAY)**
5. Data Spaces and Data Sovereignty
6. 6G and Cyber Security
7. …

- We are open re-address and insert new ones for the future according to ECCC and NCCs' needs and requests.

BASICS

RISK ASSESSMENT

Risk Assessment in a nutshell:

- ❑ Weight your capabilities and needs by identifying your
  - ❑ main assets
  - ❑ potential threats
  - ❑ Weaknesses or installed security controls
- ❑ Analyse the current state, and possible improvements
  - ❑ Are you happy with the current risks?
  - ❑ What can you do to improve your risk level.

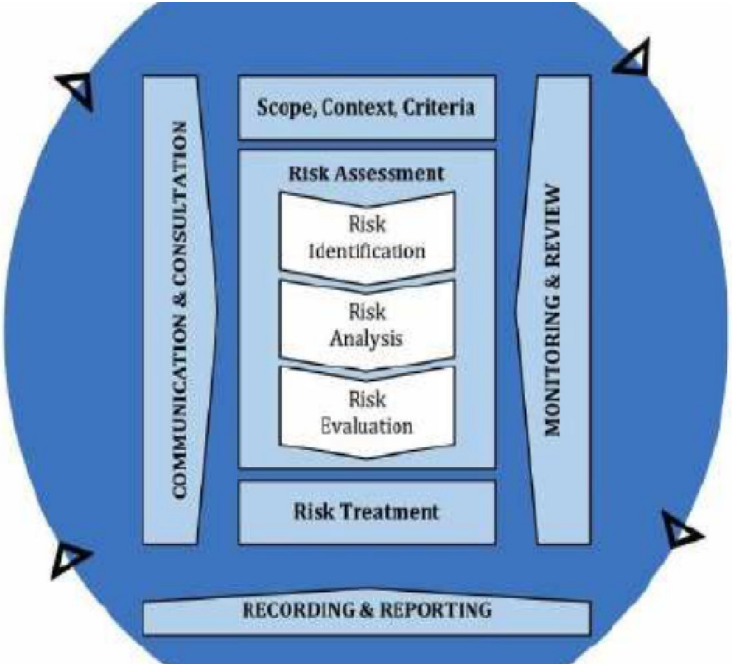
- ❑ Addresses your needs
- ❑ Optimises decisions
- ❑ Easy to understand and use by manager
- ❑ Supports justification of the taken decisions

BASIC TERMS

- **Risk** is the **possibility** of suffering harm or **loss** [NIST SP800-30]
  - **Threat** – cause of risk
  - **Vulnerability** – existing flow or weakness
  - **Impact** – possible loss

  - **Asset** – something valuable
  - **Incident** – threat occurrence

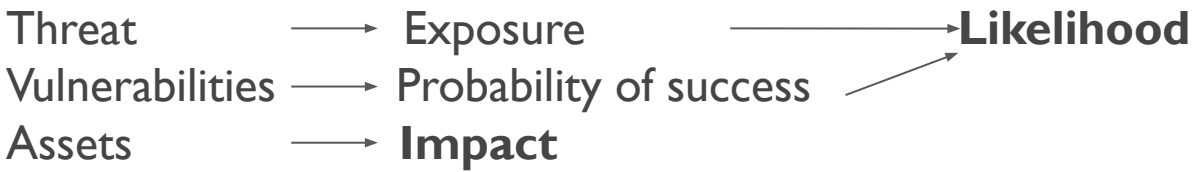
Risk Management – coordinated activities to direct and control an organization with regard to risk [ISO 31000]



RISK ASSESSMENT

Risk Assessment – overall process of risk analysis and risk evaluation [ISO 27000]

RISK Analysis



Risk = Likelihood × Impact

Quantitative	**Quantitative**
Loss – measured in euro, dollars, etc.	Loss – {low, medium, high}
Likelihood – positive real value	Likelihood – {low, medium, high}

RISK TREATMENT

- Risk assessment estimates the **current level** of risks
  - Where are we?
- Risk treatment helps to plan the steps to **deal with** the excessive risks
  - What are we going to do?

- Implementation of more or better controls is only one way (risk reduction) to treat risks!
  - Identified problems can (and should be) solved on risk level, with other instruments (including, risk avoidance, risk transfer and risk acceptance).

RISK/SECURITY MANAGEMENT STANDARDS

- Cyber Risk Management
  - ISO 31000 – Risk management – Guidelines
  - ISO 27001 – Information security management systems — Requirements
  - NIST 800-37 – Risk Management Framework for Information Systems and Organizations
  - NIST Cybersecurity Framework
- Cyber Risk Assessment
  - ISO 27005 – Information security risk assessment
  - NIST 800-30 – Guide for Conducting Risk Assessments
  - Other risk management methodologies: CIS RAM, OCTAVE, Magerit, Mehari, Microsoft, etc.
- General Security Control lists and guidelines:
  - ISO 27002 – Code of practice for information security controls
  - NIST 800-53 - Security and Privacy Controls
  - CIS Controls

ECCO
European Cybersecurity COmmunity

RELEVANT EU LEGISLATION

ISTITUTO DI INFORMATICA E TELEMATICA CNR

ECCO European Cybersecurity COmmunity

CYEN

Network & Information Systems Directive (NIS2 2022)

Requirements for entities in scope:
Art. 20: Management bodies (...) are required to follow training (...) to **enable them to identify risks and assess cybersecurity risk-management practices and their impact** *on the services provided by the entity.*

Art.21: (...) take appropriate and proportionate technical, operational and organisational measures to manage the **risks posed to the security** *of network and information systems which those entities* **use for their operations or for the provision of their services**, *and to prevent or minimise the impact of incidents on recipients of their services and on other services.*

Art. 21: (...) shall ensure a level of security of network and information systems **appropriate to the risks** *posed.*
Requirements for member states:

Art. 22: The Cooperation Group, in cooperation with the Commission and ENISA, may carry out **coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains**.
The CSIRTs shall have the following tasks: (...) ***providing dynamic risk*** *and incident analysis and* ***situational awareness*** *regarding cybersecurity;*

NIS2 Risk Management Implementing Act

Risk Management Policy, based on (Article 21(2), point (A):

- *Risk management framework: to **identify and address** the risks posed to the security of network and information systems; update & review, results of risk assessments*
- *Compliance monitoring: **regular reviews of compliance with policies** on network and information system security, topic-specific policies, rules, and standards; entities shall put in place an **effective compliance reporting system***
- *Independent review of information and network security: entities shall **review independently** their approach to managing network and information system security and its implementation*

Public consultation now open: Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers

DIGITAL OPERATIONS RESILIENT ACT (DORA 2022)

- Internal governance and control framework that ensures an **effective and prudent management of ICT risk** (Art. 5 Governance)
- ICT risk management: **a sound, comprehensive and well-documented**
- ICT risk management framework as part of the **overall risk management system**, enabling the companies within the scope to **address ICT risk quickly, efficiently and comprehensively** (Art. 6)

As per a Regulatory Technical Standard, Financial services + Third party ICT providers:

- Establish ICT security policies, procedures, protocols and tools, incl. ICT Risk Managemer
- Comprehensive and systematic approach to treating ICT risk.
- Monitor internal and external vulnerabilities and threats.
- Include details in the ICT risk management framework review report.

CYBER RESILIENCE ACT (CRA) FOR MANUFACTURERS

Cybersecurity is taken into account in **planning, design, development, production, delivery** and **maintenance** phase;

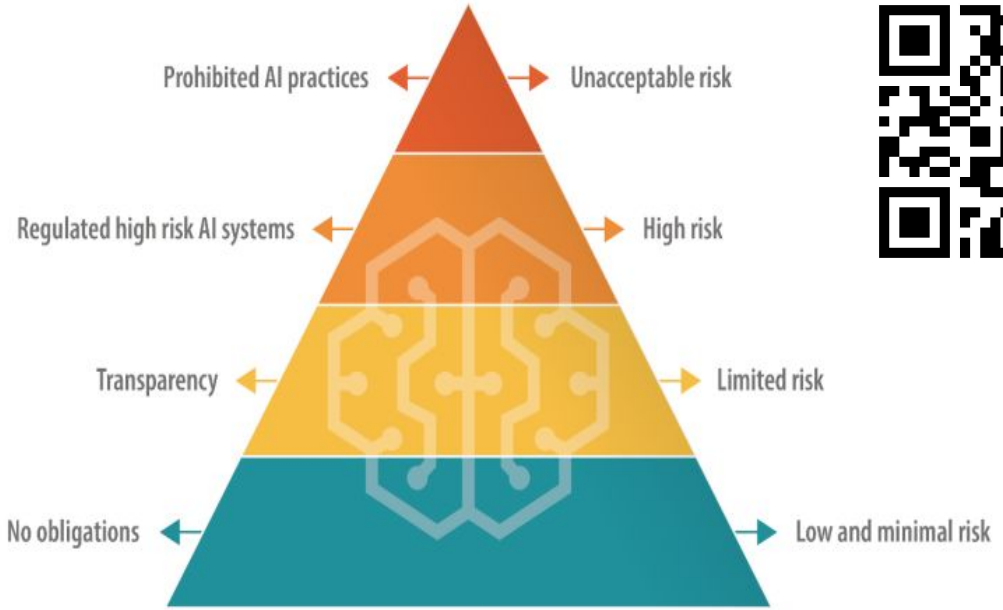
All **cybersecurity risks** are documented;

Source: European Commission, CRA Factsheet

GDPR 2016

- The **processor should implement appropriate technical and organisational measures** to ensure a level of **security appropriate to the risk**

The Pyramid of AI risk



Data source: European Commission.

NOT ONLY INTERNAL RISK

NIS2

Art. 21: '**include supply chain security** and **security in network and information systems acquisition**, development and maintenance, including vulnerability handling and disclosure'

Recital 85: 'should **incorporate cybersecurity risk management measures into contractual arrangements** with their direct suppliers and take into account (1)the overall quality and resilience of products and services,(2) the cybersecurity risk management measures embedded in them,(3) their suppliers' cybersecurity practises.

DORA

CHAPTER V: Regulates **managing ICT third-party risks**, as an integral component of ICT risk management framework

Art. 28: **Strategy on third-party risk**, incl. policy on the use of third-party ICT service supporting critical or important functions.

ECCO
European Cybersecurity COmmunity

CHALLENGES

ISTITUTO DI INFORMATICA E TELEMATICA CNR

ECCO European Cybersecurity COmmunity

CYEN

CHALLENGES

enisa

SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES

1

WHAT IF...

State-sponsored actors insert a backdoor in a well-known and popular open-source library on online code repository. They use this to infiltrate information from most major European corporations and use the information to blackmail leaders, espionage, or otherwise initiate disruptions across the EU.

?

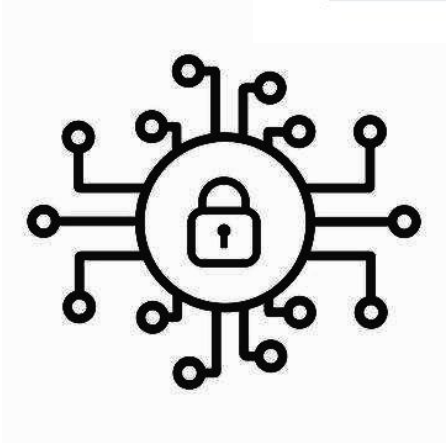
ISTITUTO DI INFORMATICA E TELEMATICA CNR

ECCO European Cybersecurity COmmunity

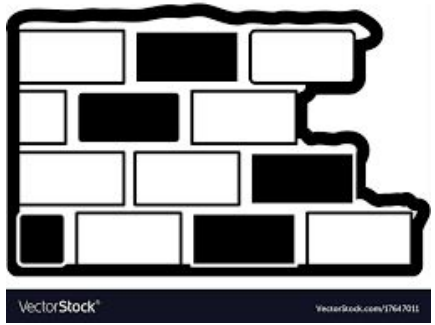
CYEN

CHALLENGES

Dynamic changes:
threat, vul, risks, technology



Lack of statistical data



Time & effort consuming, specialised discipline

Uncertain effectiveness of cyber security controls

ECCO
European Cybersecurity COmmunity

FUTURE RESEARCH NEEDS

ISTITUTO DI INFORMATICA E TELEMATICA CNR

ECCO European Cybersecurity COmmunity

CYEN

FUTURE RESEARCH NEEDS

Policy: Certification, care forward (risk assessment considering user needs)
Metrics: Risk quantification and risk monitoring, incl. systematic risks
Prioritisation: risks, vulnerabilities, measures
Technology: Cryptography, AI, bitcoin

ISTITUTO DI INFORMATICA E TELEMATICA CNR

ECCO European Cybersecurity COmmunity

CYEN

FUTURE RESEARCH NEEDS

Evaluation of risk: how to confirm scale & validity of risks

Fast risk assessment: how to reduce the time and effort for risk assessment?

Dynamic risk assessment: how to compute risk dynamically, taking into account changes in assets, threats and vulnerabilities automatically?

Q&A and Discussion

July 4 2024

ECCO
European Cybersecurity COmmunity

CONCLUSIONS AND NEXT STEPS