Funded by the European Union

CYBER4Dev

Developing CII Protection

Priit Kaup

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Topics

- **Developing CIIP**
  - What kind of support can the state provide?
  - What can the state do?
- **Monitoring of the Vital Service providers**
  - “Soft” monitoring
  - Technical monitoring
- **Improving CIIP protection**

Funded by the European Union

Who is responsible for CIIP?

- The owner of the CII?
- The Vital Service Provider?
- The state?

Funded by the European Union

- Cybersecurity Act (English version)
  - Principles of ensuring cybersecurity
    - **the principle of personality** – ensuring the security of a system shall be arranged by the service provider;
    - **the principle of integral protection** – the service provider shall ascertain potential risks posed to the system and apply appropriate organizational and technical measures for the protection of the system;
    - **the principle of minimizing adverse effect** – in the case of a cyber incident the service provider shall apply due care and measures to avoid the escalation of the effect of the cyber incident and its possible spread to another system and shall notify the supervisory authority provided for in this Act of the cyber incident;
    - **the principle of cooperation** – in ensuring cybersecurity and resolving cyber incidents the parties shall cooperate and, if necessary, take into account the mutual connection between and dependence of the systems and services.

Funded by the European Union

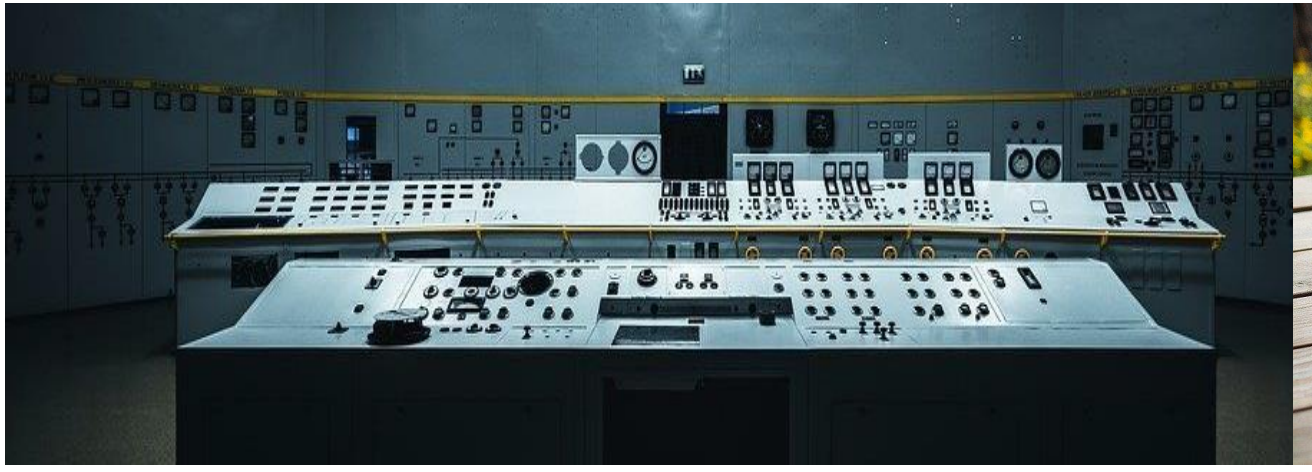
How is protecting CII different?

- Traditionally, in IT networks C-I-A of data is protected
  - Confidentiality
  - Integrity
  - Availability

Funded by the European Union

How is protecting CII different?

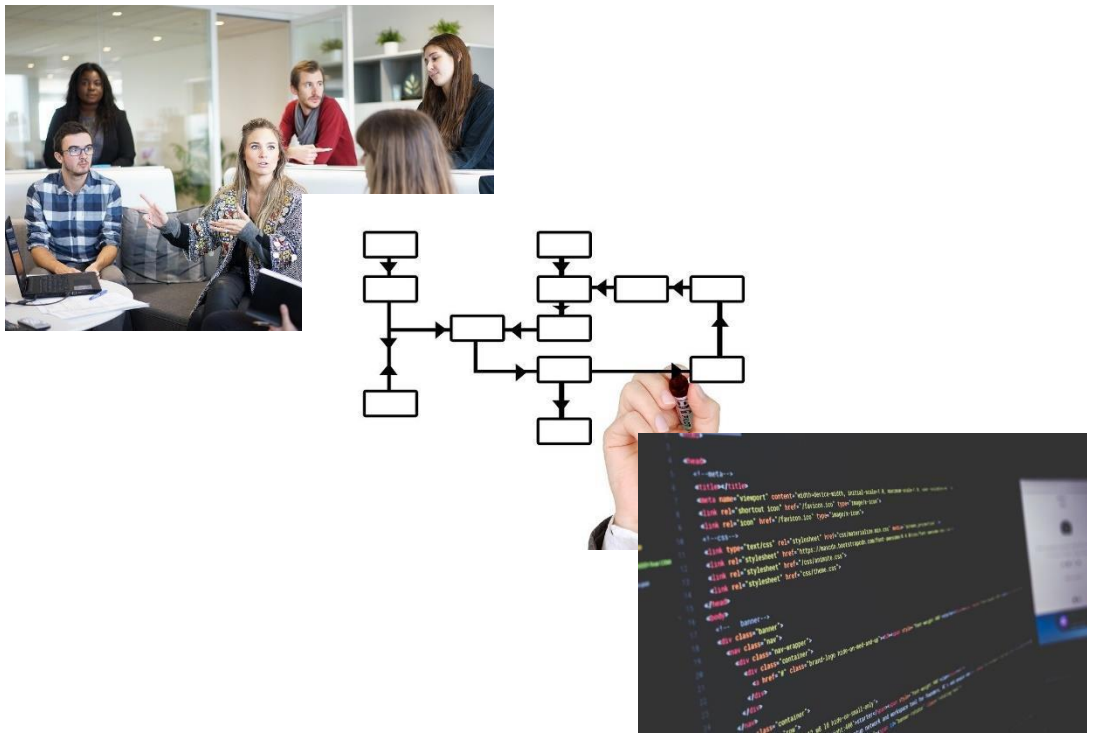
- In ICS/SCADA systems the priorities are different
  - Availability
  - Integrity
  - Confidentiality
- But Vital service providers still have the “office” IT systems



Funded by the European Union

What is needed to protect CII?

- **Resources**
  - People
  - Processes
  - Technology



Funded by the European Union

Services for Vital Service Providers

- **To develop peoples skills**
  - Risk analysis training
  - Cyber Hygiene training for end users
  - Trainings for managers
  - Specific technical trainings for IT specialists
  - Information sharing
  - **Exercises**
  - **Cyber Security Development program**

Funded by the European Union

CYBER4Dev

Exercises

- Tabletop and live-fire exercises for vital service providers
- Tabletop is best for training and testing procedures and identifying areas of improvement
- Live-fire tests capabilities and team work to manage incidents

Excellent manual for organizing cyber exercises by Finnish Traficom

Funded by the European Union

Mentoring program

- Cyber Security Mentoring Program
  - Sectorial, this year water utility companies
  - Introduce different frameworks, evaluation tools, this year CIS20 Controls by Center for Internet Security
  - Share experiences and tools used in sector
  - Sample documents and sample technical solutions
    - IT policy, rules etc
    - Secure remote monitoring solution for ICS/SCADA

Funded by the European Union

Services for Vital Service Providers

- **To develop processes**
  - Guidelines and frameworks to protect CII
    - CIS20
    - ISO27001
    - ISKE
    - E-ITS
    - **Risk analysis/assessment**
  - Recommendations and manuals
    - How to harden Windows based networks
    - How to harden e-mail systems
    - How to protect against ransomware attacks.
    - Etc.

Funded by the European Union

Risk assessment

- Legal obligation for Vital Service Providers
- Risk assessment helps to find out how to allocate resources.
  - State can ask to see if it is done and if thought has been put in it
  - It helps to concentrate on the highest risks across departments
  - Can be done on many levels
    - State
    - Sector
    - Vital Service Provider
      - Vital service IT risk analysis

Funded by the European Union

Risk assessment

- Risk assessment
  - prepare a system risk assessment in which they shall set out a **list of risks** affecting the security of the system and the continuity of the service and causing the occurrence of cyber incidents, **determine the severity of consequences** of a cyber incident occurring upon the realization of risks, and **describe the measures** for resolving a cyber incident;

Funded by the European Union

Risk assessment

Stages of risk analysis	Key activities
Identification of critical activities, systems, and resources	• Describing the activities critical for providing the service • Mapping, describing, and critically assessing important systems. • Mapping the resources related to the systems.
Identification of threats	• Identification of the threats that could lead to cyber incidents and thus compromise the security of the system or the continuity of the service. • It is important to remember that threats are not static or exhaustive.
Identification of vulnerabilities	• Identification of vulnerabilities that can lead to the realisation of threats causing harm to assets or the organisation. • Linking vulnerabilities to previously mapped systems and identified threats.
Assessment of likelihood	• Identifying existing security measures to prevent, detect, and mitigate interruptions. • Identifying the likelihood of threats
Assessment of consequences	• Identifying the business impact on the organisation when threats materialize.
Risk assessment	• Risk classification. • Creation of a risk matrix.
Risk management	• Listing the risks in order of priority with the preventive and mitigating security measures as well as the persons responsible for their implementation and the deadline.

Table 1 Stages of risk analysis

Funded by the European Union

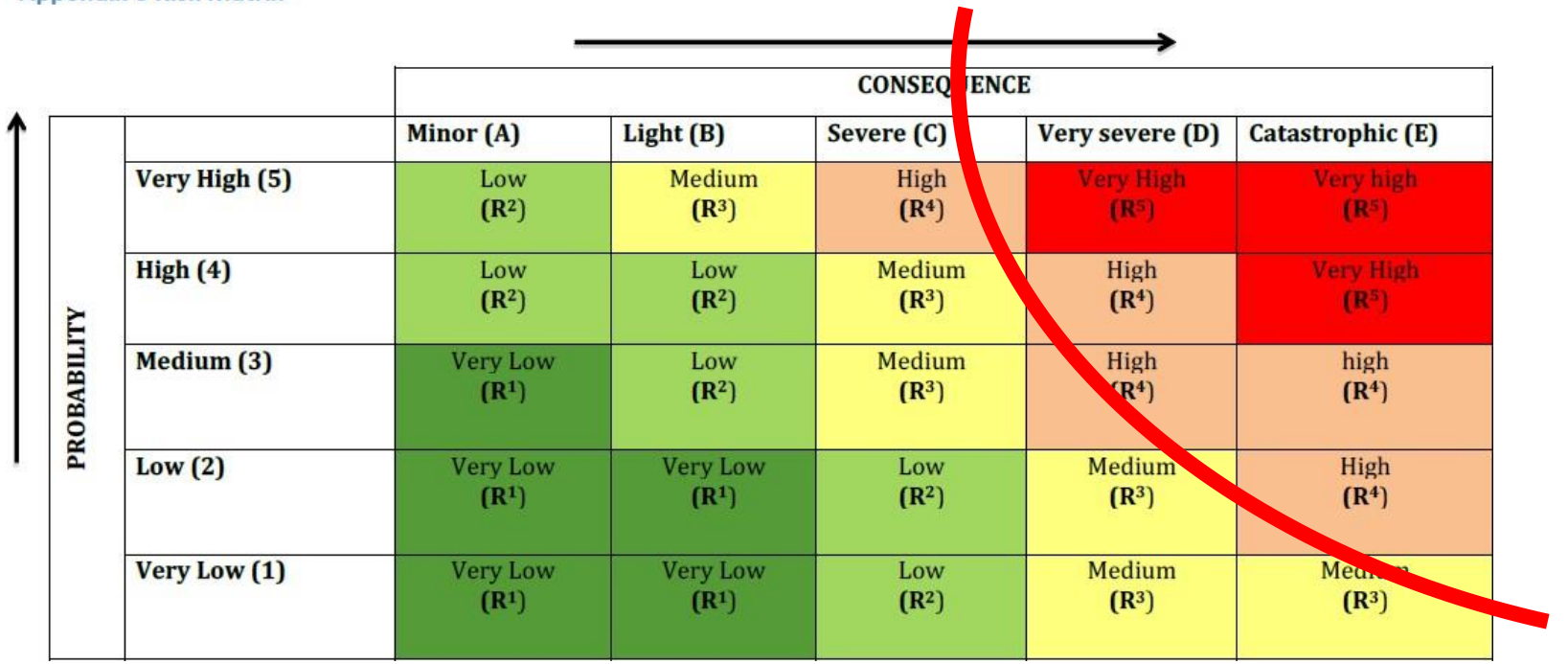
Guidelines for preparing an IT risk analysis

September 2019

13 pages guideline document
Complete with an example

Risk analysis

Appendix 6 Risk Matrix



PROBABILITY	CONSEQUENCE				
	Minor (A)	Light (B)	Severe (C)	Very severe (D)	Catastrophic (E)
Very High (5)	Low (R²)	Medium (R³)	High (R⁴)	Very High (R⁵)	Very high (R⁵)
High (4)	Low (R²)	Low (R²)	Medium (R³)	High (R⁴)	Very High (R⁵)
Medium (3)	Very Low (R¹)	Low (R²)	Medium (R³)	High (R⁴)	high (R⁴)
Low (2)	Very Low (R¹)	Very Low (R¹)	Low (R²)	Medium (R³)	High (R⁴)
Very Low (1)	Very Low (R¹)	Very Low (R¹)	Low (R²)	Medium (R³)	Medium (R³)

Funded by the European Union

Risk analysis

Risk	Risk classification	Measure	Estimated cost of the measure	Responsible for implementing the measure	Deadline for implementation of the measure
Server malfunction due to flooding	R5-Very High	Provisioning backup servers in ISO certified datacentre	20 000€/year	Priit Kaup	March 2021

Excellent tool to explain the needs of IT/Cyber Security to management

Funded by the European Union

Services for Vital Service Providers

- To provide technological capabilities, that would be out of reach otherwise
  - Penetration testing/vulnerability assessments
  - Malware analysis – Cuckoo Sandbox
  - Cyber Forensics
  - Network monitoring/IPS – Suricata4All

Funded by the European Union

Penetration testing

- A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might
- Provides a report with found vulnerabilities, risks and remediation recommendation
- Excellent tool to measure the overall security of the company, provides input for both management, IT department and State
- Can be a bit expensive, but well worth it. Scope can be adjusted.
- Main goal is to raise awareness

Funded by the European Union

Malware analysis

- If suspicious file is found, how to analyse, what is does?
- Free automated tools are available, but what about confidentiality?
- CERT-EE provides Cuckoo Sandbox

Funded by the European Union

Cyber Forensics

- In case of incident, forensic capabilities are needed
  - Forensic imaging
  - Analysis
  - Reporting
- Highly specialised personnel needed, practice and tools

Funded by the European Union

Monitoring/IPS

- Network monitoring and traffic logging
  - Helps to discover incidents
  - Helps to determine the scope of incidets
- If there is inadequate logging there is no way to find out what the attacker has done
- Somebody needs to look at the logs and monitor the IPS
- Suricata4All provides a way to centrally help Vital Service Providers to log traffic and monitor their networks.

Funded by the European Union

Monitoring

- Monitoring IP address space for vulnerabilities and misconfigurations
  - Notifying the owners of vulnerable systems
  - https://www.hardenize.com/dashboards/ee-tld/
  - Giving the possibility to benchmark with others

Funded by the European Union

Monitoring of maturity of the companies

- All these services provide valuable insight into vital service providers cyber security posture
- Data can be used to propose new rules and regulations
- Provide additional trainings
- Or start a formal supervisory process

Funded by the European Union

Key takeaways

- We try hard to be friendly partner and help the companies to get better in cyber security.
- Building networks between people is important and helps a lot to avoid misunderstandings and mistrust.
- Documents are important, but only if they are up-to-date and actually used. As much as needed but as little as possible.
- Technical testing reveals the truth, but vulnerabilities exist because of faulty processes/lack of people.

Funded by the European Union

Key takeaways

- Start out small and give companies time to mature
  - It takes years for an organization to reach mature security posture
- Risk assessment is a must-have
- “Soft” approach works very well
    - But “stick” should be available
- Best experts are probably working for vital service providers, let them help

Funded by the European Union

CYBER4Dev

Tomorrow: Sharing is caring

Importance of facilitating Networking and Information Sharing

Funded by the European Union