Cybersecurity

Jakub Harašta & Attila Kiss

Information Society

- Not new – just better
- Availability – ICT dependency

Information Society II

- Changes
  - Commerce
  - Social life
  - Education
  - Entertainment
  - Government
  - Geography
  - Threats!

Cyber Security

- CIA
  - Confidentiality
  - Integrity
  - Availability
- Alternative concepts
  - Parkerian Hexade
    - confidentiality, possession or control, integrity, authenticity, availability, utility

Confidentiality

- Unauthorized cannot access
  - Authentication – who are you?
    - Knowing, having, being…
  - Authorization – can you do that?

- Perfect situation:
  - Computer minus Internet plus finite list of users plus heavy encryption
    - So…

Integrity

- Preventing change of data
  - Authentication
  - Authorization
  - Nonrepudiation
- Every change has to be listed with possible recovery

Availability

- You need it?
  - Up and running

Threats

- Cyber crime
- Hacktivism
- Cyber warfare
- Cyber espionage

Or…

- Violation of obligation
  - Non-reporting, updating
  - Private
- Cyber crime
  - Criminal
- Cyber Terrorism
  - Non-state actors
- Cyber Warfare
  - State actors

So far

- Duping the Soviets
  - 80s?
- Estonia 2007
  - DDoS, solely cyberspace
- Georgia 2008
  - DDoS in war, cyberspace within conventional
- Stuxnet
  - APT, sophisticated, air gap
- Red October
  - Espionage
- Anonymous
  - Hacktivism
- Sony 2011
  - More than 75 million accounts stolen

Cyber Security

- Prevention
- Reaction
- Investigation

Prevention

- Standards (ISO, NIST)
- Security policy
- Security proceedings
- Evaluation/re-evaluation

- GET READY!

Reaction

- People and institutions
  - CERTs

- FIX IT and WARN!

Investigation

- Either outside the scope…
  - Police
- …or back to prevention.
  - What happened and how do we prevent it from happening again?

- WHO and HOW?

Legislation

- Act No. 181/2014 Sb.
- Act L of 2013, on the Electronic Information Security of Central and Local Government Agencies
- Law on the Security on Information Technologies (2010) Revised proposal in Germany (August 2014)
- COM 2013/48 Proposal for a directive concerning measures to ensure a high common level of network and information security across the Union

But also…

- Discussion
- Education
  - banka123
  - nbu123

CySec != InfoSec

- Information Security
  - China, Russia
  - Content
  - Also offline

But…

- NATO talk
  - Cyber defense
- EU talk
  - Network and information security
    - What did I just say?
  - ICT security

International Cooperation

- Estonia 2007 – CCD COE (NATO)
  - Tallinn Manual (Schmitt et al.)
  - Tallinn Manual 2.0
  - EU reaction?
- ENISA (EU)
- ICRC
- UN: ITU - IMPACT

Czech legislation

- Main issues:
  - What‘s the point of having a legislation constantly challenged?
  - Proportionality
    - Distributive and non-distributive rights

Who is obliged?

- Critical infrastructure operators
  - Critical information infrastructure
  - Critical communication infrastructure
- Significant information systems
- Significant networks
- Provider of electronic communication services

Why?

Basic obligations

- Contact information
- Detection of cyber incidents
- Reporting of cyber incidents
- Security documentation
- NSA CZ

CSIRT/CERT/CIRC

- Explicitly in 181/2014
- Implicitly in 181/2014
- Outside of scope of 181/2014

Other

- Plethora of different models
  - Hungary
  - EU

Proceedings

- 2012/2096(INI) - European Parliament resolution of 22 November 2012 on Cyber Security and Defence
- Online public consultation on 'Improving network and information security in the EU – 57% experienced incidents
- The European Commission and High Representative's 2013 Cyber Security Strategy
  - comprehensive policy document
  - internal market, justice and home affairs and foreign policy angles of cyberspace
- 2013/0027 (COD) NIS Directive Proposal

To achieve

- Freedom and openness:
  EU values and fundamental rights in cyberspace
- Apply laws as much in cyberspace:
  Reduce the level of cybercrime
- Cyber security capacity building:
  the EU engages with international partners and organisations, the private sector and civil society
- International cooperation in cyberspace:
  preserving open, free and secure cyberspace is a global challenge
- **Need for a comprehensive**
  EU vision

to ensure a high common level of network and information security (NIS)

Achieved by:

1. requiring the Member States to increase their preparedness
2. to improve their cooperation with each other
3. to manage security risks and report serious incidents
   - of ‘critical infrastructure’
   - to the national competent authorities.

How?

Increase preparedness:

- National NIS Strategy
- National Competent Authority (monitoring)
- Computer Emergency Response Team (CERT) (handling and mitigating the risk of incidents)

Cooperation

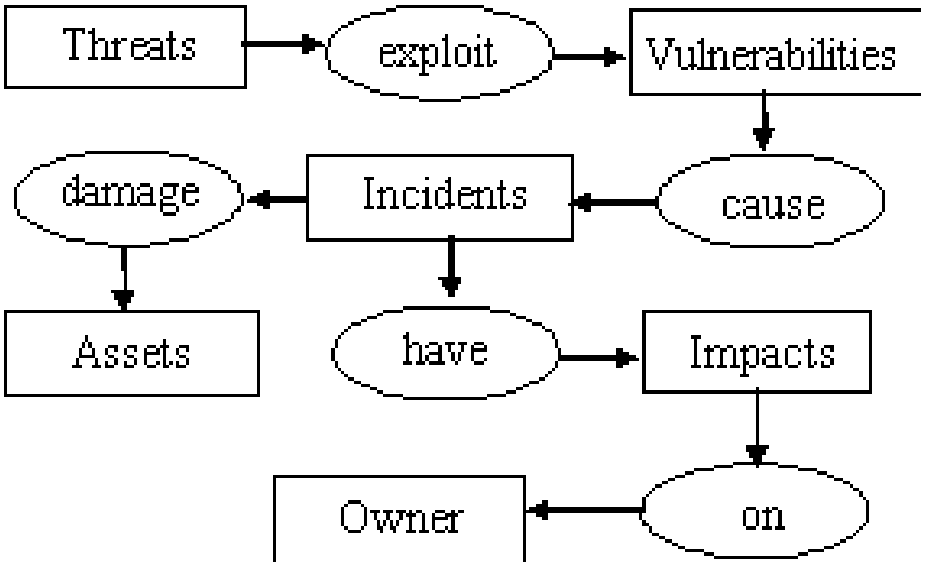
- NIS competent authorities to cooperate within a network at EU level
- Early warnings and coordinated response
- Capacity building
- NIS exercises at EU level
- ENISA to assist

Identify and facilitate the up-take of risk management best practices

- Draw from international standards and best practices
- Cross-cutting / horizontal approach
- No imposition of standards

Ways of risk management

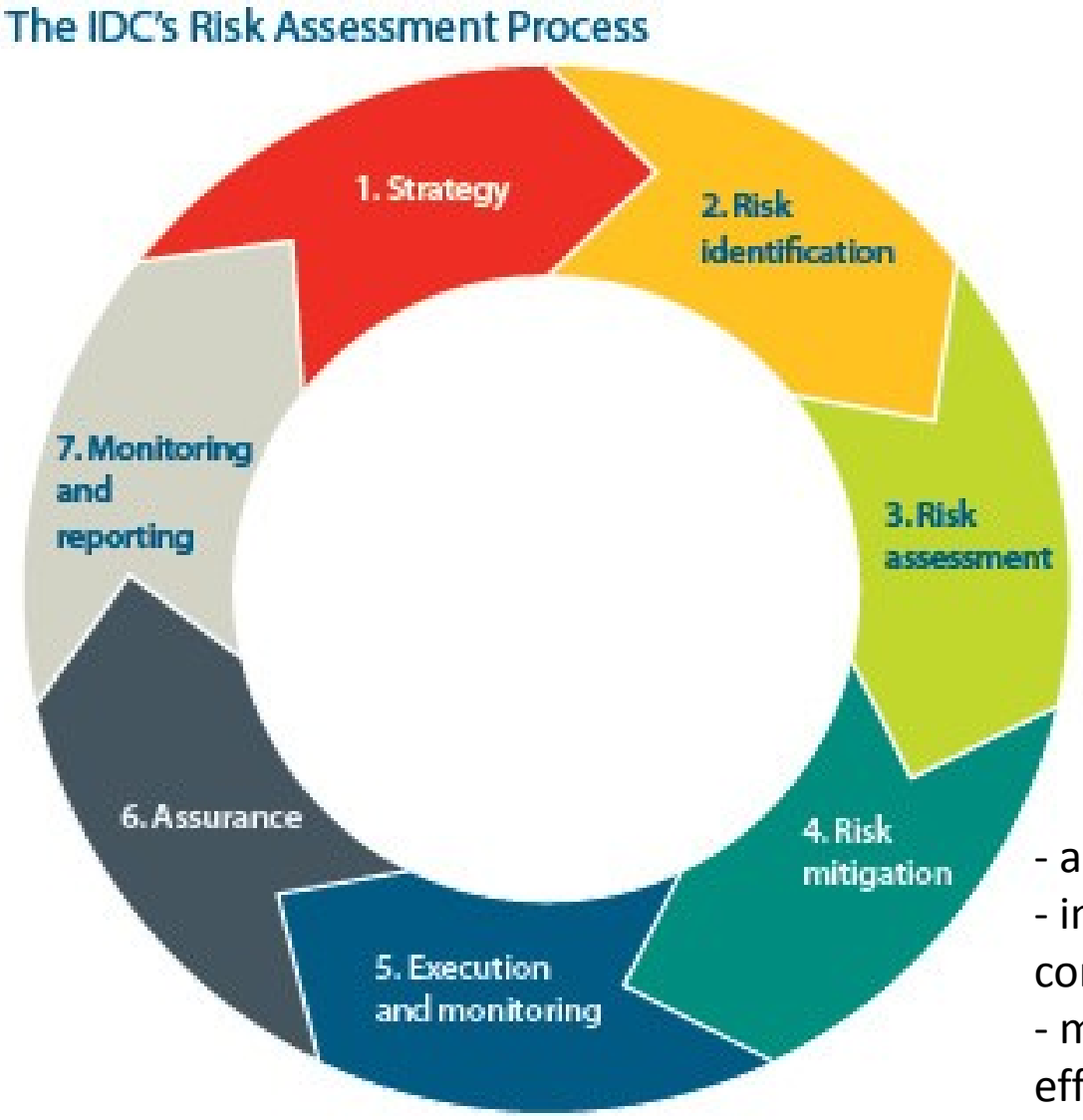
CRAMM-model (UK)
CCTA Risk Analysis and Management Method



But only the necessary level of security:

Risk appetite and risk tolerance

Ways of risk management



probable impact following an occurrence
+ the **likelihood** of the occurrence happening

- allocate accountability
- implement mitigating controls/processes
- monitoring effectiveness of controls

‘critical infrastructure’

- Energy – electricity, gas and oil
- Credit institutions and stock exchanges
- Transport – air, maritime, rail
- Healthcare
- Internet enablers
- Public administrations
- July 2015 – maybe financial market infrastructures, internet exchange points and food chains in addition

Awareness raising

- organisations apply for a Cyber Essentials certification
- Cybersecurity month – October
- Cybersecurity championship – ENISA guidelines
- NIS education and training

At the national level it recommends:

- (a) The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis;
- (b) A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;
- (c) The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors

Useful links

- EU Cybersecurity Strategy High-Level Conference 2014: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0
- Trust and Security: http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security
- Cybersecurity: http://ec.europa.eu/digital-agenda/en/cybersecurity
- Digital Futures: https://ec.europa.eu/digital-agenda/en/digital-futures-objectives-and-scope
- Help up improve our analysis and measurement: http://ec.europa.eu/digital-agenda/en/help-us-improve-our-analysis-measurement