Introduction to cybersecurity in construction

Managing and Sharing Construction Data

Computing in Construction

Metropolia

Nature of security as a goal

- Security concerns are generally broad, ranging from
  - not allowing your friend to read your messages to
  - protecting a nation's infrastructure against attacks
- Security is a negative goal
  - it is fundamentally the absence of wrong things, not the presence of right things
  - systems and processes should be design to prevent all possible ways to breach the security
  - it must be made difficult to side-step the security mechanism, for instance, by bribing someone on the inside
  - just one hole is enough for an adversary to break in, and often the break-in remains unnoticed, unless the adversary informs about it
- A negative goal means that every possible hole should be blocked
  - to consider all possible holes, a broad view to security is required
  - for example, strong encryption of data transfers is not a panacea if the end-point security is poor – after all, the encrypted data needs to be decrypted at the end-point if the data is going to be utilized

Metropolia

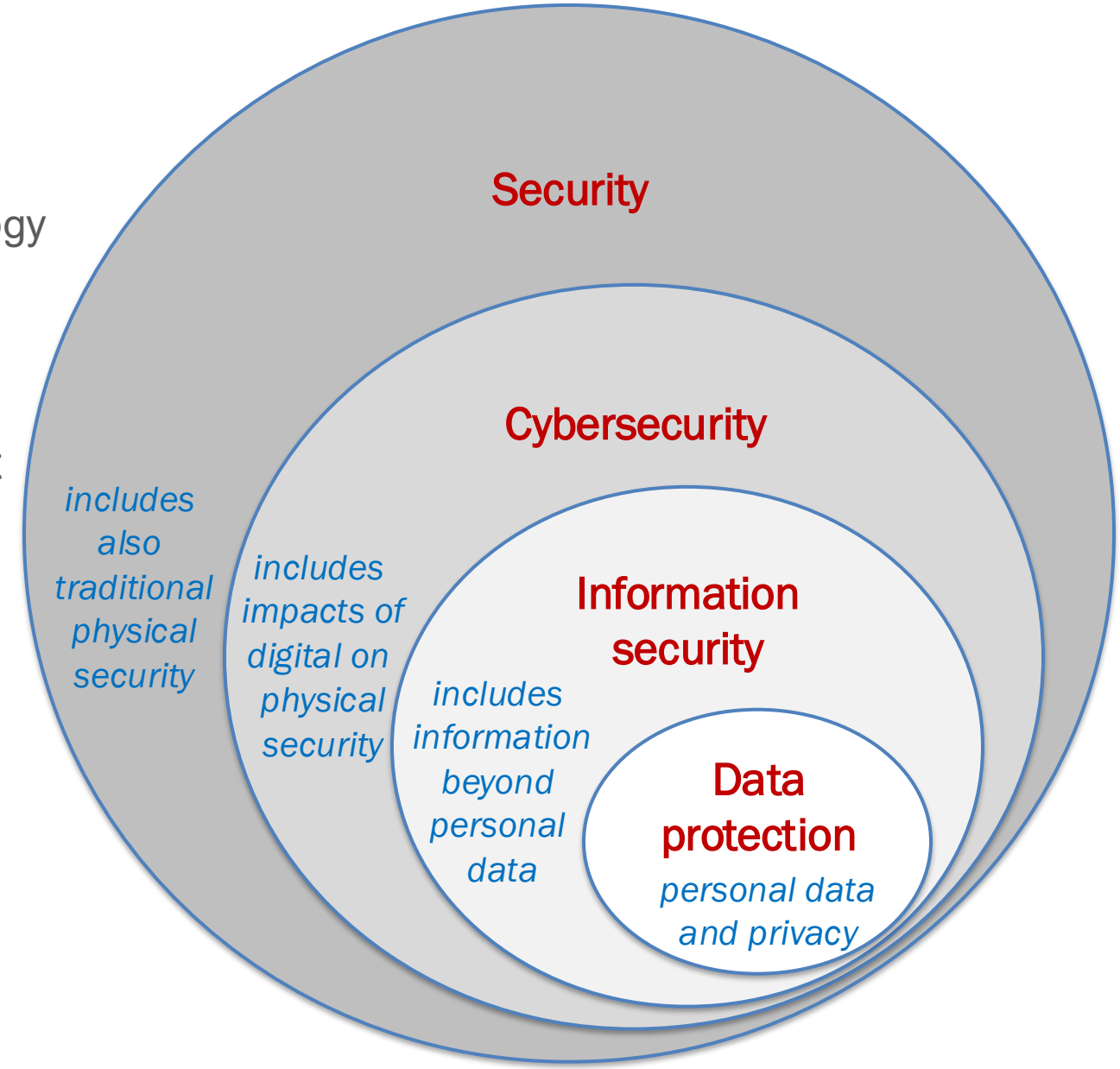
Interpretation of the terms in Finland and EU

- Cyber security
  - security of the digitalized and networked **society –** and its systems, organizations, and individuals
  - challenge: impacts of problems in digitalized and networked systems on critical functions of society and its systems, organizations, or individuals
    - identify, prevent, and prepare for
  - combines aspects of
    - information security, continuity management, and preparation for crises
- Information security
  - ensure the confidentiality, integrity, and accessibility of **information**
  - challenge: unauthorized or inappropriate access to data or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information
    - prevent or reduce the probability or impact
- Data protection
  - ensure safety of personal data and privacy of **individuals**
    - the rights to access, rectify, erase, or transfer their data
  - GDPR – General Data Protection Regulation (EU, 2018)

Metropolia

Scopes of the security terms

- "Cyber" ~ digital realm
  - related to
    - information and communication technology
    - information networks and data transfer
    - information systems
  - includes the impacts of the digital realm on the physical realm that depends on it
- Information security
  - personal data is just one area
  - includes national and trade secrets, competitive data, bookkeeping of companies, information to run different functions of society, etc.



Metropolia

Security issues in construction – big picture

- Construction sector faces a range of security issues that can impact the
  - safety of workers
  - security of construction sites
  - quality of construction projects
  - integrity, confidentiality and accessibility of information
- General solutions
  - risk analysis
  - security plans
  - training of personnel
  - employing security technologies
  - protocols to respond to incidents

Metropolia

Scope of security challenges

- Worker safety and health
- Labor issues
- Theft, vandalism, trespassing, sabotage
- Contractor fraud
- Substandard materials
- Non-compliance with environmental regulations
- Supply chain disruptions
- BIM models end up to unauthorized parties
- Breach of intellectual property rights
- Tender prices are leaked

Digitalization, collaboration, and interoperability

The attempts to improve the productivity, quality, and sustainability of construction all increase the

- digitalization of activities and processes
- collaboration between project parties
- interoperability solutions between systems

Resulting problems

- Digitalization: more digital information will be produced and consumed
- Collaboration: more information is shared between larger groups of people
- Interoperability: information is shared so as to be easily used by other systems

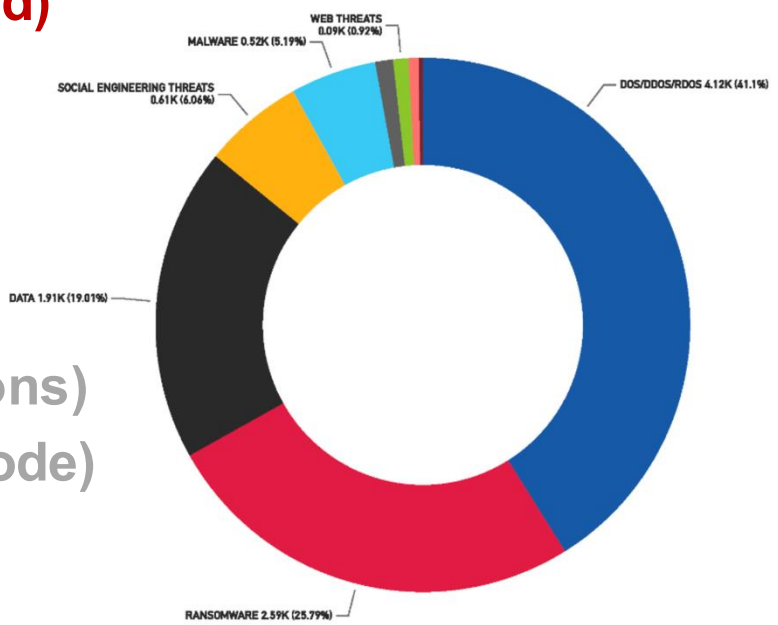
New vulnerabilities: digital information can be

- stolen remotely without leaving any traces
- spread around fast (in seconds or minutes)
- utilized in the original (structural) form (not just as a printout)

Metropolia

ENISA – cybersecurity threat landscape

- 7 prime cybersecurity threats were identified 7/2023 – 6/2024
  1. **Ransomware (threat to make data inaccessible/exposed)**
  2. **Malware (malicious code)**
  3. **Social Engineering (use human errors to gain access)**
  4. **Threats against data (stealing data)**
  5. **Threats against availability (denial of service)**
  6. **Information manipulation and interference (e.g., elections)**
  7. **Supply chain attacks (e.g., backdoor in open-source code)**



- Based on the analysis of several thousand publicly reported cybersecurity incidents and events
  - *ENISA threat landscape 2024*, DOI: 10.2824/0710888

Metropolia

Ensuring cybersecurity – range of measures

1. **Technical measures**
   - Network security
   - Endpoint security
   - Access control
   - Data security
   - Application security
   - Cloud security
2. **Procedural and policy measures**
   - Cybersecurity policies
   - Incident response plans
   - Disaster recovery
   - Business continuity planning
3. **Organizational measures**
   - Cybersecurity governance
   - Compliance and standards
4. **Human-centric measures**
   - Cybersecurity awareness training
   - Insider threat management
5. **Supply-chain security**
   - Third-party risk management
   - Supply-chain transparency
6. **Advanced defensive measures**
   - Zero-trust architecture
   - Threat intelligence
7. **Physical security measures**
   - Secure facilities and infrastructure
8. **Resilience and adaptability measures**
   - Adaptive defence mechanisms
9. **Regulatory and legal measures**
   - Adherence to legal requirements
   - Engagement with law enforcement

Metropolia

Metropolia : 10+1 Information security instructions

1. Be sufficiently skeptical
   - ask enough why-questions
2. Think twice about what you share online
   - once published online, it stays on there
3. Ensure the authenticity of links and communicators
   - know the identity of the communication party
4. Look after the updates and security of your devices
   - including mobile devices and computers
5. Count to ten if a situation involves money
   - cyber criminals desire your bank information and personal data
6. Public and open networks always entail risks
   - use a VPN when connecting to an unfamiliar network
7. Remember to back up your data
   - also, never plug unknown equipment, such as a USB stick, into a device
8. Use strong passwords and password managers
   - use multi-factor authentication when available.
9. Be realistic
   - anything too good to be true, is not likely to be true
10. The digital world give more than it takes
    - don't be unnecessarily scared
11. Look after others' information security as well
    - for example, your kids and parents

Thank you!

Metropolia