Topics summary

I. Combating and preventing transnational ransomware attacks.

- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.
- Transnational ransomware attacks extend across national borders.
- For 94.2% of incidents, we do not know whether the company paid the ransom or not.
- When the negotiation fails, the attackers usually expose and make the data available on their webpages. This is what happens in general and is a reality for 37,88% of incidents.
- We can therefore conclude that the remaining 62,12% of companies either came to an agreement with the attackers or found another solution.

a) Actions to take to mitigate ransomware attacks:

1. Action 1: make regular backups
2. Action 2: prevent malware from being delivered and spreading to devices
3. Action 3: prevent malware from running on devices
4. Action 4: prepare for an incident

- 36 countries met in Washington to discuss malware threats and ways to decrease attacks.
- Many ransomware attacks are not reported or recorded and so they happen much more often than reflected.

II. Using digital tools to protect anonymous whistleblowers world-wide.

- Whistleblowing is the term used when a worker passes on information concerning wrongdoing, such as:

a. A criminal offense, for example fraud
b. Someone’s health and safety is in danger
c. Risk or actual damage to the environment
d. A miscarriage of justice

e. The company is breaking the law – for example, it does not have the right insurance
f. You believe someone is covering up wrongdoing

- Anonymous reporting is a process whereby people can submit a whistleblowing report without revealing their identity.
- In November 2019, the EU Whistleblower Directive ("the Directive") came into force. The Directive requires EU Member States to implement rights and obligations concerning whistleblowers, private organizations and the Member States themselves in national law.
- Whistleblowing is important to maintaining honest companies and keeping regulation in check. Which is why we need to assure the protection of anonymous whistleblowers.

a) Some Raised Concerns for Anonymous Whistleblowing:
    1. anonymous reports allowed only in certain legal and economic sectors, where the risks of wrongdoing are higher
    2. only accepting anonymous reports which already contain sufficient information to constitute a wrongdoing;
    3. appointing an intermediary third party, in charge of investigating whistleblowing reports and follow-up with anonymous whistle-blowers; and
    4. setting requirements for available digital channels that allow for confidentiality or anonymity of the identity of the whistle-blower.

a) Personal Effects that Prevent Whistleblowing:
    1. Whistleblowers may face resentment and hostility from peers and superiors.
    2. Employees in an organization that do not participate in or have no awareness of inappropriate activities are typically affected if the company faces legal claims or public backlash.

- Furthermore, as a result of the Whistleblowing Directive, a number of digital whistleblowing platforms on the market have developed functionalities and features that ensure the anonymity of the whistleblower, such as:
    1. providing a secure web platform to an entirely outsourced service that receives, assesses, investigates and follows up on the whistleblower reports;
    2. functionalities to conduct investigations without collecting data that could be used to identify the reporter (e.g. mitigation of a leaked IP address and

meta data by using encrypted access to the case files through a personal incident number and password);

3. confidential and secured two-way communication with relevant investigators and further information on the progress and outcome of the investigation;
4. provision of robust digital security measures to ensure the confidentiality of the identity of the whistleblower and the data collected (e.g. end-to-end encryption in transmission and in storage, secure multi-factor authentication of the relevant authorized persons, required to investigate the claims); and
5. implementation of a new ISO 37002 standard (expected by August 2021) which provides a higher threshold for confidentiality.