Definition hot topics of internet safety, country differences

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Index

1. Introduction

Nowadays almost every information goes online and almost every single act of regular person has some impact - imprint on the NET (social media, e-mails, money transfers, cookies, etc.).

Also, in these days almost everything has direct connection on the NET and thanks to the 4th industrial revolution - it's just a beginning.

The main goal of this report is to summarize the most important conclusions regarding two themes: cybersecurity and web security and personal data and internet safety.

Additionally, as we seen in the previous report there are a lot of similarities in the countries involved in this project regarding the topics mentioned above. Therefore, the country differences that exists are more related to some opening clauses that leaves the national legislators some leeway.

2. Main conclusions

In this section we have a list of the main conclusions that where found in the Intellectual Output 2 - Legal aspects of Internet safety. The conclusions are divided into two themes.

2.1. Cybersecurity and web security

2.1.1. Work/Companies

- Attacks are becoming more complex and frequent and the main motivation behind attacks is monetization;
- Cloud security is becoming a critical issue and companies are expected to become increasingly dependent on cloud providers;
- The importance of organizational measures (e.g. risk management) will increase in future compared to purely technical measures;
- The dependence of companies on hardware and software products represents an increasing threat;
- There are not enough incentives for security investments in companies;
- Lack of security awareness and standards;
- There are still missing or obsolete legal foundation in countries that difficult the understanding and the application of security measures;
- Lack of safety awareness by most of the people;
- Lack of skilled/qualified cybersecurity personnel and digital competences;
- Lack of training activities to improve the knowledge and a much secure behavior by people;
- Lack of employee awareness of the cybernetic threats and IT security rules;
- Lack of a clear and concise technical guides related to cybersecurity and internet safety;
- Escalating salary requirements of skilled cybersecurity personnel can complicate the situation;
- Many separate security tools ultimately increase operational complexity and reducing visibility into overall security posture;

- Organizations often do not have a formal cybersecurity incident response team or even a named individual who is responsible for dealing with such an incident;
- There are a lack of collaboration between privacy and cybersecurity teams;
- Many companies don't have a consistent cybersecurity response plan;
- Lack of time and skilled resources necessary to implement cybersecurity plan;
- Lack of a proper budget necessary to boost security capabilities;
- Obsolete IT security hardware and software;
- Lack of commitment by management along with an insufficient budget;
- Lack of involvement between all the workers in the cybersecurity strategy (if there is one);
- The inventory of assets with cybersecurity impact is not well known by all the workers in the company;
- Cybersecurity culture needs to be interiorized, security programs and measures such as processes, environment or labor risk prevention management;
- Few initiatives focused on industrial cybersecurity;
- There is no cybersecurity solutions tested enough;
- Lack of cooperation among company and government initiatives;
- Inefficient communication between the different teams because of their differences regarding their knowledge and capabilities about the use of software and hardware;
- There are activities that may endanger the systems and, as a consequence, the security of the industrial processes and facilities;
- Lack of awareness of the effects and of the need of new technologies used to assure the interoperability of control systems;
- General perception that the threat is uncertain and quite unlikely;
- Espionage by modern digital means threatens national competitiveness and productivity;
- Different cybersecurity needs among different activity sectors;
- Lack of financial support for cybersecurity development;
- Shortage or absolute lack of specific standards for cybersecurity;
- Misunderstanding of the topic due to a shortage of focused training programs and public communication material;

- Wrong implementation of security solutions and technologies such as firewalls, solutions IDS/IPS, antivirus, etc;
- No relationship or agreement among authorities, business and providers in relation to cybersecurity;
- Little coordination among the different state members of the EU.

2.1.2. Private life

- Lack of security awareness and standards;
- Negligent behaviors when using internet;
- Current undergraduate school programs do not include, most of the times, cybersecurity topics;
- Although there are good initiatives, tips and hints but it doesn't reach the general population;
- High number of malicious software on the market;
- Inadequate understanding of the cyber-attack status;
- There are many rural areas in which not very many further training offers are possible due to the location;
- Help with difficulties is usually only available over the phone or online (with the exception of going directly to the police). A direct contact point is needed, to which people can also contact directly in case of problems;
- Regulations, policies and laws are not formulated in a user-friendly way;
- Information on the supporting materials is sometimes very difficult to find (on the internet) and it needs a faster and an easier access;
- Using a weak password, a one password to log in to multiple accounts and not changing password;
- Lack of study materials about cybersecurity;
- People easily trust email attachments;
- People share a lot of personal information on social networks;
- General lack of interest of young people about internet safety;
- Lack of awareness of the cybernetic threats and IT security rules;
- There are not many cybersecurity platforms to exchange and share information;

- Lack of financial support for promotion of internet security to people and cybersecurity development;
- Few initiatives focused on internet safety in every day life;
- Shortage educational and training programs and public materials about internet safety;
- Low digital literacy of end users;
- Basic awareness of potential threats is missing from public users;
- There is not created a cybersecurity culture;
- Lack of a clear and concise technical guides regarding internet safety and cybersecurity;
- The inventory of assets with cybersecurity impact is not well known;
- Lack of awareness of the effects and the need of new technologies used to assure the interoperability of security/control systems;
- Misunderstanding of the cybersecurity and internet safety due to a shortage of focused training programs and public communication material;
- Policies and procedures are not suitable from the cybersecurity point of view;
- Cybersecurity risks are not integrated in tools and systems;
- There are no cybersecurity solutions tested enough;
- Wrong implementation of security solutions and technologies such as firewalls, solutions IDS/IPS, antivirus, etc;
- Little coordination among the different state members of the EU.

2.2. Personal data protection and internet safety

- The new rules concerning personal data protection will place considerable demands on companies;
- There are still missing, obsolete legal foundation and simple information in countries that difficult the understanding and the application of GDPR and other personal data protection legislation;
- The existence of divergences regarding the information, the measures and the procedures necessary to a proper implementation of the GDPR because lots of companies still don't know exactly what to do;

- The need to have access to simples, clear information and user-friendly information;
- Lack/Low implementation of measures to increase personal data protection in a daily basis;
- Lack of measures, tips and accessible training regarding personal data protection to everyone regardless their age, knowledge or geographic location;
- Lack of training activities since early stages;
- Developing student's digital citizenship through appropriate technology, including online communication etiquette and digital rights and responsibilities;
- Europeans call for stronger privacy protection online;
- A lot of companies still recognize the need to reinforce the information and training for the workers regarding GDPR;
- The majority of the companies need a first assessment related to the level of the conformity and the adequacy of current policies and processes for a correct identification of possible changes regarding GDPR;
- The actual challenges related to the modernization, globalization, technology and digitalization implies a revision of the GDPR process that already exists continuously;
- Engage all the community involved in the personal data protection as soon as possible;
- Define and review, on frequent basis, the knowledge, skills, attributes and other characteristics that people can and must be trained for, regarding the topics in analysis;
- Stimulate the production of creative and educational online content for all people that must be simple and accessible for everyone;
- Digital technologies are constantly changing and teachers/trainers need to receive constant training in order to be able to help and give appropriate training activities;
- Designate data protection responsibilities to your team;
- Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc;
- Train your staff and implement technical and organizational security measures.

2.3. Cybersecurity in Europe

During the past few years, the European Commission have introduced a series of measures as an alternative to ensure a safer online environment in the EU. Also, the European Commission is working on increasing cybersecurity capabilities and cooperation, strengthen the EU as a cybersecurity player worldwide.

Since 2017, the EU started to become more commit to provide cybersecurity measures and to increase the trust of citizens and businesses in the digital society in Europe but it was only in June 2019 (with the Regulation (EU) 2019/881 of the European Parliament) that were implemented a series of measures that aim to develop a strong cybersecurity within the EU and the safety of the EU digital environment. Also, the Cybersecurity Act is a part of the EU overall cybersecurity and stablishes some notification and security requirements for operators of essential services and digital service providers such as cloud providers.

Additionally, since June 2019, the European Cybersecurity Act entered into force setting the new mandate of ENISA, the EU Agency for Cybersecurity and establishing the European cybersecurity certification framework.

Even thought there are some legislation regarding cybersecurity that are in force in each member state there are also some opening clauses that leave the national legislators some leeway regarding the implementation of cybersecurity. Some of the countries in Europe (Czech Republic, Austria, Portugal and Spain) have some legislations/directives/codes that address cybersecurity issues in their own countries. Nevertheless, cybersecurity regulations still need further development because the European Parliament acts as co-legislator and each member state is the primarily responsible for their own cybersecurity. Therefore, it is necessary to implement some measures in order to improve cyber-resilience such as:

- The cybersecurity legislation remains incomplete and there area some delays concerning this topic across the European territory. As a result, it is necessary to improve information exchange and coordination between the legislation actors and the private and public sectors should work alongside to contribute to answer cybersecurity issues that may arise;

- Policy-makers and legislators must develop more simple and direct legislation that must be user-friendly for everyone no matter the background of the person;
- According to a report carried out by European Court of Auditors "Challenges to effective EU cybersecurity policy", 80% of EU businesses experienced at least one cybersecurity incident in 2016; 69% have no, or only a basic understanding of their exposure to cyber threats and 60% have never estimated the potential financial losses. Because of this, cybersecurity in companies must be a top priority and must be evaluated through some audits/external analyses regularly (for example each year). With these audits organizations have access to useful information and they know what they need to develop/focus on. Due to that, they have the responsibility to implement some actions in order to have a better cybersecurity performance;
- Legislation alone does not guarantee resilience and to build a cyber-resilience culture each company must have a proactive and also a reactive plan to answer to some cybersecurity incidents that may happen;
- Having a clear overview about the training needs and weakness of each person concerning this area is also mandatory. Therefore, raising skills and awareness to people since early stages is mandatory and must start as soon as possible in each country. For example, it is important to organize some initiatives and start to implement them in companies, schools and at home. According to this suggestion, for example, companies must have a certified/qualified person in the cybersecurity area that can give training to the rest of the teams especially in the software area and the most common cyber incidents such as: phishing attacks; malware; Trojans; spam; ransomware and data stolen. This is also important to develop a culture of cybersecurity.

All of suggestions mentioned above aim to achieve a greater level of cybersecurity in the EU and also have a more effectively response to cyber incidents.

3. Systematized content catalogue

The most important topics regarding the two themes analyzed in the Intellectual Output 2 are described bellow.

- **Cloud security:** also known as cloud computing security consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customer's privacy as well as setting authentication rules for individual users and devices;
- **Cybercrime:** any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email, internet fraud and identity fraud as well as attempts to steal financial account, credit card or other payment card information;
- **Cybersecurity:** the practice of protecting systems, networks and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing or destroying sensitive information, extorting money from users or interrupting normal business processes;
- **Cyber theft:** stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use;
- **Data breaches:** an intentional or unintentional release of secure or private/confidential information to an untrusted environment. Data breaches may involve personal health information, personally identifiable information, trade secrets and/or intellectual property;
- **Data leaks:** unauthorized transmission of data (electronically or physically) from an organization to an external destination. Data leak threats usually occur via web and email but can also occur via mobile data storages devices such as USB, pen drives, laptops, etc;
- **Data protection:** process of protecting data and involves the relationship

between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes;

- **Data privacy:** information privacy is a branch of data security concerned with the proper handling of data - consent, notice and regulatory obligations. More specifically, practical data privacy concerns: whether or how data is shared with third parties; how data is legally collected or stored and regulatory restrictions (e.g. GDPR);
- **Data security:** a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure. Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, logical controls, organizational standards and other safeguarding techniques that limit to unauthorized or malicious users or processes;
- **Internet safety:** knowledge of maximizing the user's personal safety and security risks on private information and property associated with using the internet and the self-protection from computer crime in general;
- **Malware:** any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users computer activity without their permission;
- **Phishing:** phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in an email or other communication channels. The attacker use phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims;
- **Security breaches:** any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters private, confidential or unauthorized information;

- **Spam:** electronic messaging systems to send out unrequested or unwanted messages in bulk. The most common form of spam is email spam but the term also applies to any message sent electronically that is unsolicited and bulk;
- **Trojan:** type of malware that is often disguised as legitimate software. Trojan can be employed by cyber-thieves and hackers trying to gain access to users systems;
- **Virus:** computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.