AmCham Slovakia | DIGITAL SUSTAINABILITY FORUM | Microsoft

Cybersecurity Challenges: Public Administration, Healthcare and the Private Sector

ONLINE DISCUSSION

TUESDAY
November 30, 2021

TIME
1:00 PM - 4:00 PM

VENUE
online/MS Teams

LANGUAGE
slovak/czech

5 KEY TAKEAWAYS:

1. Necessity of cooperation and collaboration across multiple sectors
2. Cross-sectional education on cyber security from school to the workplace
3. Solutions that respect principles of democracy and the rule of law
4. Protection of personal data leads to citizen trust in the institutions
5. Need for centralized, safe, and functional cyber security system and guidelines to follow

On November 30, 2021, representatives from the public, private, healthcare, and education sector met to discuss the state of play in respect to cybersecurity in Slovakia. The recent advancements in information technology, digitalization processes, and AI have also resulted in increased risks of cyber-attacks and the emergence of new kinds of hybrid threats in the digital space.

The need for cyber security solutions and implementation has never been greater and has been exacerbated by the impending COVID-19 pandemic, which has revealed many blind spots and shortcomings of current systems and processes. For this reason, AmCham Slovakia has organized a roundtable discussion on the topic of Cybersecurity Challenges: Public Administration, Healthcare, and the Private Sector as part of the Digital Sustainability Forum which has been launched in many countries to discuss technological challenges.

The aim of this roundtable has been to facilitate space for discussion, exchange of ideas, and best practice sharing between representatives from sectors such as the government, public sector, private sector, critical infrastructure, and academia. Mr. Florian Pennings, Director Government Affairs for Cybersecurity, Microsoft opened the discussion and introduced his view on the current developments at EU level as well as trends related to digital sovereignty, which have begun to significantly influence the regulation of cyber security. Following up on that the participants agreed that there is the crucial need for redefinition of the way we think about borders and digital and technological sovereignty. Cyber security is a global problem and therefore the approach must also be global in its scope. The discussion resulted in an agreement that the cornerstone for effective cyber security is thecooperation and collaboration between different stakeholders.

"All sectors must work together to create and implement solutions and guidelines to withstand cyber security threats. These solutions must be in line with principles of rule of law and democracy, which is linked to the importance of data protection – only when citizens know that their personal data are safe, will they have trust in their government and its institutions as well as in the private sector."

The discussion provided a view on several successful normative frameworks on the EU level, which aim to ensure the balance between profit-

driven marketplace competition and the safety and protection of citizens and their data. The relationship between the private and public sectors is of utmost importance in the pursuit of cyber security.

"The creation and development of new cyber security solutions are where the private sector comes in – companies should be the drivers of innovation and research and cooperate and offer their solutions to the public administration to ensure the protection of personal data in critical infrastructure such as healthcare providers." Another key area, through which the private sector can contribute to cyber security is education as a form of corporate social responsibility. Human Capital is both the biggest strength and weakness of cyber security. Awareness-raising, skills, and competence building are key to identifying, overcoming, and preventing cyber security threats.

During the discussion we have identified multiple educational initiatives where companies from the private sector, such as Microsoft, ESET, Cisco, Tatra Banka, cooperate with academia, ranging from educating high school teachers and providing them with know-how on teaching about cyber security, offering expert university courses to university students as a part of the curriculum, to offering educational and practical workshops for those employed in the public sector and critical infrastructure. *"Some examples of best practice sharing include using a reward system to motivate employees to implement the knowledge on cyber security from workshops as well as linking the protection of sensitive information and data in their workplace with their private lives."*

Several areas where improvements are necessary to have been identified as well. Multiple stakeholders pointed out the need for a centralized, safe, and functional system that would control and operate a variety of networks as well as offer clearly defined guidelines for others to follow and rely on. *"There is also a lack of resources – an insufficient amount of those educated specifically in the areas of cyber security and a lack in financial resources which could be used to educate those already employed in the public sector as well as for the implementation of modern solutions to ensure the protection and safety of data and information."*

To conclude, it is important to emphasize the need for national cyber security regulations to comply with the EU framework. In practice, some EU Member States often introduce measures beyond the EU's legal framework. It is then impossible to involve modern technologies into the national security programs. However, a balance needs to be taken care of between these two interests, namely the protection and promotion of cyber security and innovation and the involvement of modern technologies.

3 KEY NEXT STEPS:

This fruitful roundtable discussion has allowed us to identify both numerous existing successes and future challenges in cyber security. *"AmCham Slovakia hopes to follow up in the directions sketched out in this discussion and offer more opportunities for different sectors to cooperate and share their knowledge on the topic of cyber security in the future."*

1.
Necessity of creating the list of lists on cybersecurity initiatives.

2.
AmCham Slovakia as a neutral platform for further discussions.

3.
Follow-up event with the representatives of slovensko.sk, MIRRI, and other state and national security organizations.