SCALE UP
community-driven
bioeconomy development

WS3 Training Programme Protocol

Digitalisation in the Bioeconomy:
Session #3: Safeguarding Progress:
Critical Emphasis on Cyber Security and Data Protection in Advancing the Bioeconomy

27 February 2024

Session #3: Safeguarding Progress: Critical Emphasis on Cyber Security and Data Protection in Advancing the Bioeconomy

In the realm of digitalization within the bioeconomy, Session #3 focused on the safeguarding progress, looking especially at cyber security and data protection. Hosted on February 27, 2024, from 9:00 am to 12:00 pm CET, this session delved deep into the intricate web of challenges and solutions poised at the intersection of technology and bioeconomy.

Michael Pirich, representing Siemens Austria AG, set the stage with an opening Keynote. His discourse illuminated the critical nuances of cybersecurity within bio-based systems, underscoring the imperative of internet security and robust data protection measures.

After the keynote, two case studies were presented: Aneta Łobodzińska, from the Science-Technology Center for Unmanned Systems, gave insights into the digitalization of agriculture, delving into experiences, encountered problems, and strategies for effective data processing and data protecion challenges.

Concluding the session, Volker Kromrey, representing the Bodensee-Stiftung, gave insights into the activities of their projects connected to bioeconomy as well as their experiences with a cybersecurity breach. His honest and prakctical presentation gave the audience extremely valuable insights and brought awareness and maybe aspects of these challenges most of us haven`t thought about yet.

Following the keynote, a short intermission provided attendees a breather to digest the insights shared before diving into the breakout sessions. The breakout sessions moderated in various languages by regional facilitators, facilitated collective discussions on the unique needs and challenges faced within respective regions.

As the session drew to a close, participants engaged in a feedback session, offering reflections on key outcomes and posing pertinent questions. The collective insights gleaned from breakout discussions and presentations laid a sturdy foundation for future endeavors, as the community charted a course forward, armed with newfound knowledge and heightened awareness.

BREAK-OUT ROOMS

AUSTRIA

The group started to discuss the level of awareness about cyber security. It was stated that although cyber attacks are not rare any more and therefore there is awareness for this topic, there are still a lot of people who are very naive about it. A lot of well known companies have been under cyber attacks. In the meantime, it is possible to buy insurance for cyber attacks, but the insurance companies demand a lot of protection activities.
The value chain is seen as a big “troyan horse” and companies have to make sure their suppliers are not a threat to the system. A solution for this is white-listing, where the system is only allowed to communicate with know assets (IP address,….). This creates very safe networks, but it is also a lot of expense and effort which is often a hurdle for smaller businesses. It was stated that safety is expensive but it also brings safety.
Bringing this into agriculture: as farmers are the suppliers for the food processing industry, farmers should also operate in safe IT systems. Via e-mails or logins into a system (farm delivers goods to buyer) the system is open
Digital passports: are like a digital license plate. E.g. if a farmer brings a load of wheat to the buyer, pictures are taken of the whole load (incl. tractor etc.). That way a charge gets a digital passport, which can be encrypted. This is important for the traceability within the food system!

What can we do?
Keeping up the awareness about cyber security via employer training, etc.
In a company: find out about your Internet of Things (IoT) – which assets can communicate within the system?

Take home message: We have to learn how to life with and handle these challenges!
There is technology that helps you stay safe!

NORTH MACEDONIA

The experiences with cyber crime and security breaches vary widely among individuals and organizations, ranging from no experience to regular trainings. The most frequent challenges reported include spam and strange emails. Fortunately, there haven't been any instances of cyber crime or security breaches yet. In the context of digitalization in the bioeconomy, North Macedonia's relevant experience lies in metrology and protecting agricultural lands from hydro-meteorological disasters, with the presence of Macedonian software and tools for early warning and crop protection. The IT department is primarily responsible for resolving these challenges, but employees often lack information on these matters.
The presentations covered various aspects of dealing with cybercriminals, highlighted the perceived complexity of relevant EU directives, emphasized the availability of cyber security insurance, and underscored the vulnerability of precious data, noting its potential for easy loss.
The key takeaway is to prioritize learning about the important topic of cybersecurity and then implement that knowledge into practical measures. This includes the establishment of security measures, regular backups, and the adoption of licensed software in the field of bioeconomy with integrated data storage and protection. Additionally, the message encourages the use of drones to enhance agricultural land planning for optimal crop planting based on land types.

POLAND

During the discussion, participants shared their experiences of encountering phishing emails aimed at their personal and work-related accounts.

Some participants also mentioned instances of malware infections on their devices. They suspected these infections might have resulted from unsafe browsing practices or downloading files from untrusted sources.

Additionally, one participant recounted a security breach at their workplace, where sensitive information was compromised due to inadequate cybersecurity measures.

Overall, the participants agreed that cyber threats are widespread and pose a significant risk to individuals and organisations.

During the event, Wolfgang Siegel's keynote speech on understanding cybersecurity in the bioeconomy was highly appreciated by many participants. They found the speaker's insights on internet security and data protection within bio-based systems particularly enlightening.

Aneta Łobodzińska's case study on the digitalisation of agriculture generated a lot of interest among the participants. They were fascinated by the challenges and innovative solutions presented in this field. The participants expressed their pride in having an expert from our region working closely with the European Commission and being able to learn from such experts.

The presentation by Volker Kromrey on navigating the bioeconomy amid a cybersecurity breach was alarming and informative for the attendees. They were astonished by the real-world implications of such breaches and the lessons they could learn.

The main message that the participants took away from the meeting was the critical role of cybersecurity measures, particularly in the bioeconomy context. They emphasised the need for robust strategies to protect digital infrastructure and sensitive data.

Participants expressed a renewed commitment to implementing proactive measures to reduce cyber risks within their organisations and communities. Moreover, there was a consensus on the importance of collaboration and knowledge-sharing in collectively addressing cybersecurity challenges. Overall, the webinar reinforced that cybersecurity is not merely a technical issue but a complex challenge that necessitates continuous vigilance and adaptation.

SPAIN

In the Spanish breakout session, the discussion centered on the critical importance of raising awareness about cybersecurity throughout the entire value chain of the bioeconomy. It was emphasized that every stakeholder, from primary producers using digitalized technology to distribution and commercialisation, has a role in protecting the integrity and security of the bioeconomy. The potential operational and reputational damage that a cyberattack can cause was highlighted, with examples illustrating both immediate and long-term effects on organizations. Such incidents not only disrupt operations but can also erode trust and competitive advantage, leading to significant financial losses.

The session also underscored the necessity of having preventive protocols in place that are specifically tailored to the context of each organization within the bioeconomy. These protocols are crucial for preventing disruptions, protecting critical infrastructure, and maintaining public confidence in the bioeconomy's products and services. The importance of these measures in safeguarding against cyber threats cannot be overstated, as the bioeconomy is increasingly reliant on digital technologies that are vulnerable to cyberattacks.

Finally, the importance of staff training was discussed in detail. Properly trained employees are essential for recognizing and responding to cybersecurity threats effectively. Training programs should be comprehensive and designed to equip staff with the knowledge and skills needed to identify potential cyber threats, such as phishing and malware, and to respond appropriately. The session concluded with a call to action for organizations to invest in cybersecurity training as a critical component of their overall cybersecurity strategy, transforming employees from potential weak links into strong defenders against cyber threats.

INTERNATIONAL

There was a general sense of confidence regarding the safety of the IT infrastructure within participants' organizations, but at the same time concerns were shared about the increasing frequency of phishing emails aimed at gathering sensitive information. Additionally, it has been reported that in some countries, drones become distracted due to the current geopolitical situation. This highlights the need for ongoing training to ensure that employees remain aware of potential threats.

One recent example was shared regarding phishing in the context of the European Research and Innovation Funding Programme Horizon Europe. Project coordinators and grant beneficiaries got fake phishing emails requesting a bank account for the (pre-)payments. The email address used looked very similar to the real one, and the Commission reacted very fast by informing all beneficiaries through various channels. Participants also emphasized the importance of regulations in cybersecurity, noting that they often lag behind technological developments and need to be updated regularly to address emerging threats effectively.

Regarding the second questions, all presentations were perceived as highly interesting and relevant. The presentation on the digitalization of agriculture, which focused on drones, was well-received due to its direct relevance to the bioeconomy but also due to some interesting aspects mentioned such as challenges regarding data storage and collection, and the broader geopolitical implications affecting drone use in agriculture and having impact on public acceptance.

Finally, there was consensus on the significance of awareness campaigns regarding data protection, recognizing phishing emails, understanding drone application fields and benefits to increase public acceptance, and investing in preventative measures for IT security.

Cross-regional conclusions/learnings

What can we do?

- Establishment of security measures, regular backups, and the adoption of licensed software in the field of bioeconomy with integrated data storage and protection.
- Implementation of proactive measures to reduce cyber risks within their organisations and communities.
- Prioritize learning about the important topic of cybersecurity and then implement that knowledge into practical measures.
- Invest in cybersecurity training as a critical component of an overall cybersecurity strategy transforming employees from potential weak links into strong defenders against cyber threats.
- Keeping up the awareness about cyber security via employer training, etc.
  In a company: find out about your Internet of Things (IoT) – which assets can communicate within the system?

Take home messages

- We have to learn how to life with and handle these challenges!
  There is technology that helps you stay safe!
- Cybersecurity is not merely a technical issue but a complex challenge that necessitates continuous vigilance and adaptation.
- The critical role of cybersecurity measures, particularly in the bioeconomy context, emphasising the need for robust strategies to protect digital infrastructure and sensitive data.
- Importance of collaboration and knowledge-sharing in collectively addressing cybersecurity challenges.
- Awareness campaigns regarding data protection, recognizing phishing emails, understanding drone application fields are significant and help to increase public acceptance, and investing in preventative measures for IT security.

Participant feedback

At the end of the training session, the participants were asked to fill in a short survey to evaluate the training session. In the end, 9 participants responded to the survey, of which 3 from Poland, 2 from Spain, and 2 from Macedonia. Additionally, 2 participants answered the English survey. This gave the following results:

1.1 Quality

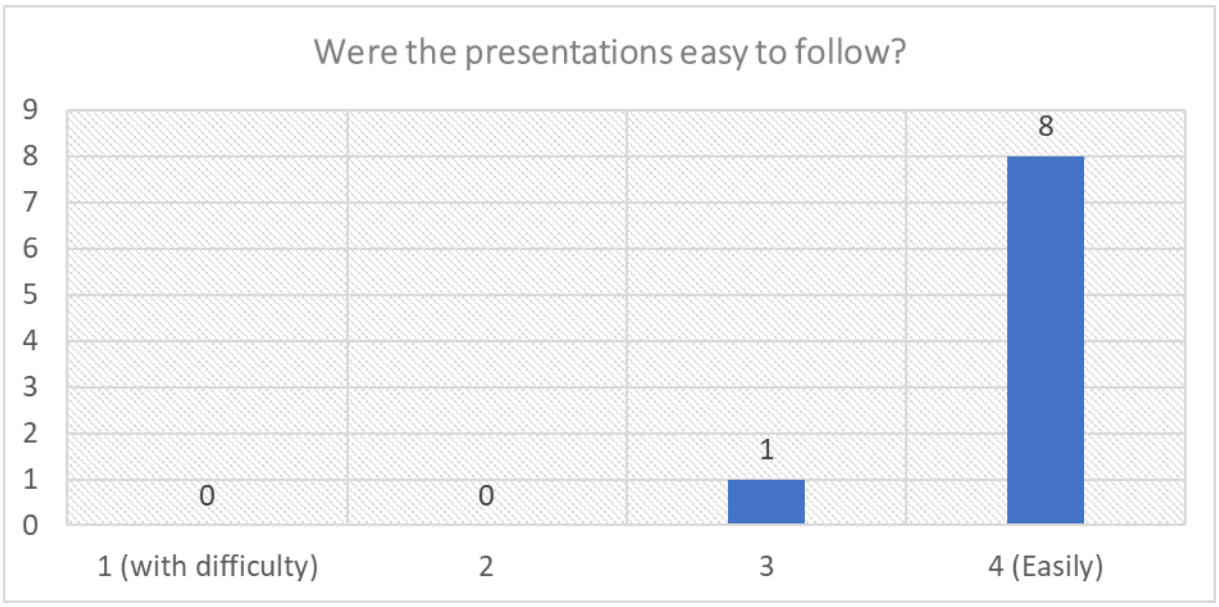
The participants were asked to rate the quality of the training session on a scale from 1 (poor) to 4 (excellent). Almost all of the participants (7) responded with a 4, meaning they found the training session to be of excellent quality. The other 2 participants responded with a 3.

The participants were then asked what went well during the session. Multiple participants answered that they very much liked the presentations, they had lots of interesting information and concrete examples. The participants also liked the contents, program, and discussions. They also mentioned that the session went smoothly and the time management was better compared to previous sessions.

Next, the participants were asked what could have gone better. Here, the few answers mostly answered that there were no points of improvement. Two comments were made: better communication, and expand cybersecurity.

1.2 Understandability

The participants were also asked whether the presentations were easy to follow. They were asked to rate this on a scale from 1(with difficulty) to 4 (easily). Out of the 9 participants, 8 gave this a score of 4 (easily), and 1 participant a score of 3, meaning that the presentations were relatively easy to understand.



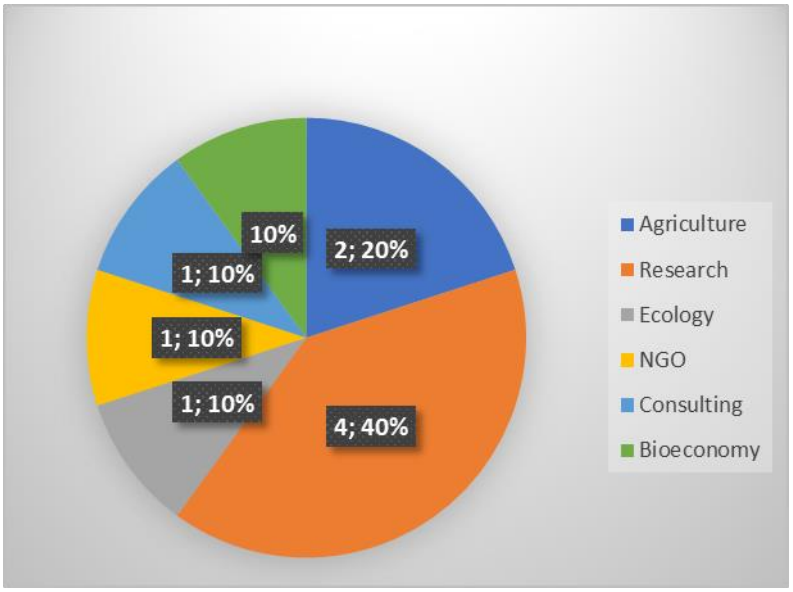
1.3 Topics

When asked which topic was most interesting, we received the following answers:

- All of them
- How AI can effectively be used fort he decelopment and protection of projects in the bioeconomy.
- Being hacked
- Cyber security in organizations
- Use of drones
- Presentation by Aneta Łobodzińska

1.4 Field of occupation

The survey concluded with an optional question regarding the participant's field of occupation. The participants came from different areas: 4 from research; 2 from agriculture; and one from ecology, an NGO, consulting and the bioeconomy.



Participants:

If you wish to get in touch with one of the participants from this session, please contact someone in the SCALE-EP consortium.