CYBERWISER.eu
Cyber Range & Capacity Building in Cybersecurity

Insights from the Stakeholder Expert Board

The Cyber Training Landscape in Europe: Insights from Peter Meyer, eyeo and member of CYBERWISER.eu Stakeholders Expert Board

Peter Meyer
Public Affairs & Internet Security

Q1 ***Can you briefly introduce yourself and the work you do?***

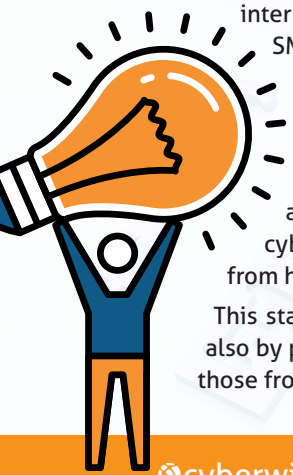
My name is Peter Meyer and I lead the Security and Privacy team at the German tech company eyeo. Part of my work includes the responsibility for our internal awareness measures. I've been into cyber security for almost 20 years now and have worked on several projects since then. This includes fighting botnets, securing websites, detecting malware, or just sharing information about best practices on cyber security awareness.

Q2 ***From your perspective, how has the cyber training landscape evolved in recent years?***

The human factor in IT security has drawn quite a lot of attention during the last few years. The focus has changed from relying solely on technical solutions and has started taking the people behind the computer more into account. The big ransomware outbreaks during the past few years have especially changed the mindset of Management when it comes to dedicating budget to cyber security training. What I am also seeing is that cyber training activities have moved away from pure ex-cathedra teaching to a much more practical approach often including Anti-Phishing simulations, cyber ranges, or the use of gamification elements.

Q3a ***What key role does the private sector make in shaping the cyber training landscape?***

In my opinion, the private sector is the main driver in the cyber training landscape. But it's not just the top dogs of the IT-Security industry that have taken the initiative here. This rising demand for cyber training services has also enabled a couple of new startups to get into this business. These startups have added plenty of innovation to the eLearning and cyber training landscape, especially by providing cyber training solutions for SMEs and by adapting them to regional markets. Many cyber training solutions built by an international corporation seem to be focused on being used by another international corporation, but such solutions often don't meet the needs of a 100 employee SME in Germany or the Czech Republic.



Q3b ***What about governments and EU agencies?***

I see governments or EU agencies more as the counterpart to the private sector by providing a certain kind of basic service for cyber education. Before talking about cyber training, we first have to continue shaping a general and broad culture of cyber security education – addressing the public, but also companies that are still far away from having any kind of cyber security culture in place.

This starts by taking cyber security awareness into schools or universities, starting early, but also by providing free cyber training resources to small companies, such as those from the craft business.

eye/o

CYBERWISER.eu has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 786668

I like the approach of initiating and funding pilot research and innovation projects on a national or European level like CYBERWISER.eu, but I am often disappointed with the situation when the public funding ends.

I see such publicly funded projects as an investment for our society, but the public support usually ends the day a project plan is finished.

Just take a look at a project like CYBERWISER.eu. I wish that the EU would say – "*We asked the best organizations across Europe to build a cyber range and a cyber training resource in a pilot. Now it's ready and we are going to support the operation and further development of this great initiative for the next five years*".

And that's exactly what I meant above by saying why I see the governments or EU agencies as the counterpart to the private sector by providing these kinds of free basic services to the public.

Q4 *What good practices are emerging from the German government (and private sector) in increasing awareness and education on cyber security through national programs?*

The German BSI (Federal Office for Information Security) runs a great initiative called Allianz für Cybersicherheit (Alliance for cyber security). It has almost 5.000 members at the moment, from the private and public sectors, NGOs, and industry associations, but is open to companies from all industries and of all sizes.

The alliance wants to foster synergies in the industry and also to bring some structure into the wide landscape of solution providers, including the public sector and private initiatives. Their claim is: Networks protect Networks.

The alliance organizes a lot of training seminars, networking events, workshops, and best practice papers, where members of the alliance share their knowledge and expertise with other members. And the best thing about it – they are all free and provided in a non-commercial way. Even membership is free.

Q5 *Are there any gaps in the national strategy for cybersecurity and what recommendations would you make to fill them?*

The general ideas and approaches are definitely going in the right direction, but I have the feeling that there are still too many initiatives doing the same things. A bit more structure and coordination would help. Also, a bit less of a "governmentish" take on some things would be good too.

Q6 *Is there anything else you would like to add about cyber training more generally at the EU level?*

I like the idea of the European Union starting something like a campaign asking for "5 minutes for IT-Security". I think that is a suitable and fair amount of time (at the least) that an employer should concede to each employee for IT-Security training. Per week would be great, but I'd already be happy with 5 minutes per month.

CYBERWISER.eu has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 786668