

# Cyber Awareness Exercises: Virtual vs On-site Participation & the Hybrid Approach

Alexandros ZACHARIS<sup>2</sup>, Eloise JABES<sup>1</sup>, Ifigenia LELLA<sup>2</sup>,  
Evangelos REKLEITIS<sup>2</sup>

<sup>1</sup> European Union Agency for the Space Programme (EUSPA)  
{eloise.jabes}@euspa.europa.eu

<sup>2</sup> European Union Agency for Cybersecurity (ENISA)  
{alexandros.zacharis, ifigenia.lella, evangelos.rekleitis}@enisa.europa.eu

## Abstract

*This paper examines the advantages and disadvantages of executing cyber awareness exercises in two different formats: Virtual vs On-site participation. Two EU Agencies, EUSPA and ENISA have organized in the previous years Cyber Awareness exercises; a very important tool to enhance and test the organization's ability to put up resistance and respond to different cyber threats. The objective of this paper is to compare the outcomes of these awareness exercises, executed on-site through physical attendance prior to 2019 and virtually, in a remote setup in 2020, due to the restrictions posed by the pandemic of COVID-19. ENISA in collaboration with EUSPA have accumulated raw and diverse data from the evaluation reports of the cyber events mentioned above. The comparison of these data will focus on the most important success factors of a cyber awareness exercise such as: participation, cooperation (social interaction/teambuilding), effectiveness, fun, tools and identify how the location of the participants affects them. The aim of this work is to highlight through statistical analysis the benefits of a hybrid approach to the exercise's setup, once combining elements of both virtual and on-site. Depending on the different kind of exercises, such a hybrid setup, will provide more flexibility to an exercise organizer and help maximize effectiveness, while adapting to the fluctuating working regimes of the near future; namely Teleworking. Furthermore, a modular exercise design will be proposed in order to adapt to the location limitations without impacting negatively the rate of the rest of factors analyzed.*

**Index terms:** Cyber Security, Cyber Exercise, Cyber Awareness, Teleworking, Training, COVID-19

## References

- [1]. T. Augustine and R. Dodge. Cyber Defense Exercise: Meeting Learning Objectives thru Competition. In Proceedings of the Colloquium for Information Systems Security Education (CISSE), 2006.

- [2]. A. D'Amico, L. Buchanan, J. Goodall, and P. Walczak. Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships between Cyber Assets, Missions and Users. In Proceedings of the International Conference on Information Warfare and Security, Dayton, Ohio, April 2010.
- [3]. Jason Kick, Cyber Exercise Playbook, The MITRE Corporation, November 2014.
- [4]. ISO 22398:2013, Guidelines for exercises.
- [5]. ENISA, CERT Exercises Handbook.