AR-IN-A-BOX

HOW TO RUN THE CYBER-AWARENESS GAME

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu
website: www.enisa.europa.eu

AUTHORS

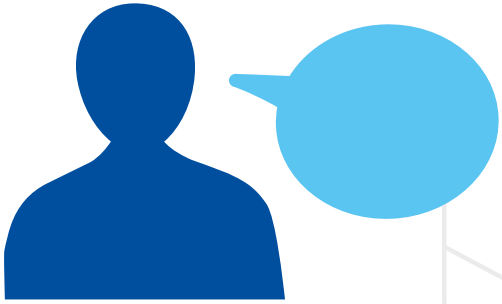
Alexandros Zacharis, Dimitra Liveri, Georgia Bafoutsou, Marianna Kalenti (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-09-22-594-EN-N
ISBN: 978-92-9204-595-1

FOREWORD



The AR-in-a-Box (awareness raising in a box) cyber game is an off-the-shelf, tabletop, mini awareness exercise. Participants will be introduced, through a gamified awareness scenario, to a number of realistic threats against a fictitious company. Their task is to analyse the attacks, identify the threats and mitigate them, ultimately identifying the root cause and the malicious actors behind them.

Through a hands-on, interactive session, participants are exposed to cyber incidents that could potentially affect their organisation and taught how to react to them', preparing them for a real life scenario.

Through this gamified approach, ENISA provides a fun way to introduce cyber awareness in team-building activities while focusing on topics such as:

- phishing and spear phishing
- ransomware
- supply chain and insider threats
- physical security
- fake news.

AR-IN-A-BOX: THE CYBER GAME

CONTENT

The AR-in-a-Box cyber game consists of the following customisable folders/files.

Style 1:

- 01. Cyber Awareness MiniGame Generic
- 02. Cyber Awareness Game Generic Style 01
- 04. Cyber Awareness MiniGame Energy
- 05. Cyber Awareness MiniGame Energy Style 01

Style 2:

- 03. Cyber Awareness Game Generic Style 02
- 06. Cyber Awareness MiniGame Energy Style 02
- 07. Cyber Awareness Quiz

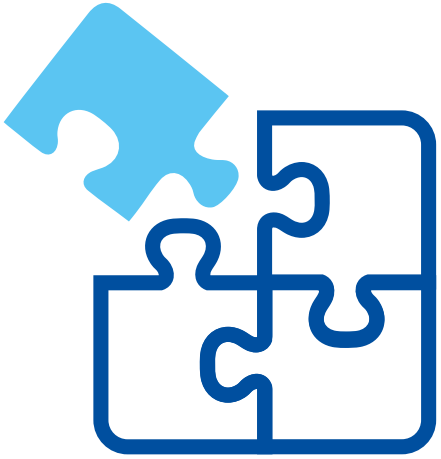
The files can be used as they come to execute the game by following the instructions in the FAQs section and all of them include hints and possible solutions.

Execution modes

The game can be executed following two different styles. These styles differ based on the scope and the set-up of the event in which the game will be conducted.

- For **team-building events** and **collaboration** between groups of people, choose style 1.

- If you are mostly interested in evaluating the cyber-awareness levels of **individuals**, use style 2.



STYLE 1: team building and collaboration

Below are the characteristics and the actions needed to execute the cyber awareness game following style 1.

Event type: team building and collaboration (physical or hybrid location).

Ideal number of participants: 50.

Ideal number of teams: 10 teams of 5 people per team, with 1 team leader per team.

Room set-up: separate round tables per team.

Resources: printouts, laptop, projector, microphone.

Preparation time: 2 to 3 hours, for preparation of room, printouts and materials.

Execution time: 1.5 hours, for explanation of game mechanics and game execution.

Reporting time: 1 hour, for presentation of solutions and reporting.

STEPS FOR CONDUCT

Preparation

Step 0: identify number of participants (e.g. 50) and split them into equal teams of 5 people. Give names to the teams or let the teams decide their names. Identify 1 person per team to be the team captain.

Step 1: download and print all the contents of the style 1 folder. You should print off enough copies for each participating team. Categorise the contents in folders using different colours.

Step 2: ask teams to sit at their dedicated table.

Execution

Step 3: explain the rules of the game to all participants.

Step 4: hand out the printouts to all team captains (3. 'included in the hints folder').

Do not provide the solutions!

Step 5: assign tasks to captains (they have 15 minutes to prepare the teams).

1. Split the team and assign tasks.
2. Team awareness and exchange of info.
3. Submit solution (answer sheet + hints folder).

Step 6: the game starts. Teams now have 45 minutes to resolve the tasks and return the answers sheet to you.

Reporting

Step 7: the game is over and all reports have been collected. Evaluate and score.

Step 8: present results and solution.

STYLE 2: self-evaluation and quiz

Below are the characteristics and the actions needed to execute the cyber awareness game following style 2.

Event type: self-evaluation (physical or remote location).

Ideal number of participants: any.

Room set-up: virtual or physical.

Resources: printouts, laptop, projector, microphone.

Preparation time: 1 hour, for preparation of room, printouts and materials.

Execution time: 1.5 hour, for explanation of game mechanics and game execution.

Reporting time: 1 hour, for presentation of solutions and reporting.

STEPS FOR CONDUCT

Preparation

Step 0: identify number of participants (e.g. 50).

Step 1: download and project 'AR-in-a-Box awareness game v.1.0 style 2'.

Step 2: ask participants to take their places.

Step 3: print and provide the empty answers sheet slide to all players.

Execution

Step 4: explain the rules of the game to all participants by presenting the first part of the document.

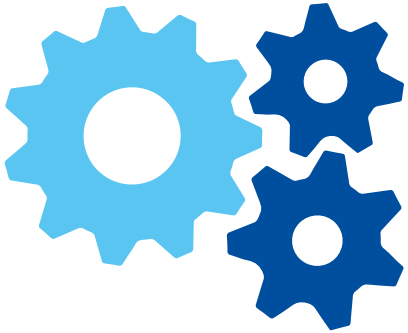
Do not provide the solutions!

Step 5: the game starts. Navigate players through the slides and narrate the content. Players now have to reply to the questions asked, resolve the tasks and return the answers sheet to you.

Reporting

Step 6: the game is over and all reports have been collected. Evaluate and score.

Step 8: present results and solution.



FAQs

Who do I need to invite to the cyber game?

Each game file is self and includes all the materials you would need to prepare for and run it. This will include the participants required for each game – you may want to invite others. Most games will require the participation of those members of staff responsible for making operational and strategic decisions during an incident.

How many people should attend a game?

The ideal size will vary between organisations, but we recommend between 5 and 6 participants per team. The number of teams can be up to 10. Consider who is required and whether individuals attending or not attending will make the game more difficult to run. Too few participants may mean you are not representing the entire organisation; too many and it becomes difficult to moderate, with the risk of overly long discussions.

Where should I run the game?

The game is designed to be best run in a dedicated physical space, so we recommend you use a normal meeting room, or somewhere further afield with fewer distractions. You will also have to consider which participants need to attend, and when. The game is designed in way where hybrid participation (virtual and physical) is also supported.

What materials do I need to run the game?

At various points during the game, you will need to share your screen so that the participants can take part. So, in addition to a laptop/computer with access to the internet, you will need:

- a projector;
- whiteboards or flipcharts with marker pens;
- printouts from the game packs;
- refreshments for your participants so they stay comfortable and productive.

What do I need to do before running the game?

You need to download the game pack for each game and familiarise yourself with the materials. Each pack will contain resources for both the facilitator and the participants. This includes guidance on how each game should be run, as well as how to get the most out of it.

How is the game structured?

The game starts by introducing an event, which could be, for example, 'your organisation's IT is being attacked'. In cyber exercise jargon, these events are known as 'injects'. The game continues by asking a set of questions relating to the inject. The answers can be given straight away or as the game evolves. Do not jump to conclusions as you might be surprised by the evolution of a cyber event. You will often find there is no simple answer.

How should I record the discussions?

The game pack includes scribe sheets for you to make notes on as you go along. In addition, you might want to use a recording device to make sure that you do not miss any contributions (there are numerous voice recording apps available on modern smartphones). The group discussion questions at the end of each game are a further opportunity for participants to reflect and review the discussions.

What happens once the game is completed?

When you have finished a game, we strongly recommend that you complete the associated report to ensure that the game is a learning experience with useful outcomes.

Each game includes a reporting module that:

- gathers all responses;
- suggests areas of improvement;
- provides links to relevant guidance.

Do participants have to be present to produce the report?

No, the reporting section can be completed by the facilitator alone, or with the help of the participants. The most important thing is that it is completed within a couple of days of the game taking place, while the game is still fresh in the mind.

How can I use the report to improve cybersecurity in my organisation?

The final report, generated from the game, should allow you to prioritise the actions your organisation should take. For minor issues relating to a specific IT system, actions could be assigned to that system's manager. More serious issues (that is, issues that present an unacceptable risk to your organisation) should be escalated to an appropriate risk owner or responsible person in your organisation. This may vary in your organisation, and could be a director, company owner or senior IT manager/officer.

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu