Cyber-Awareness: A User-Centric Holistic Approach in practice!

Eleni Klaoudatou

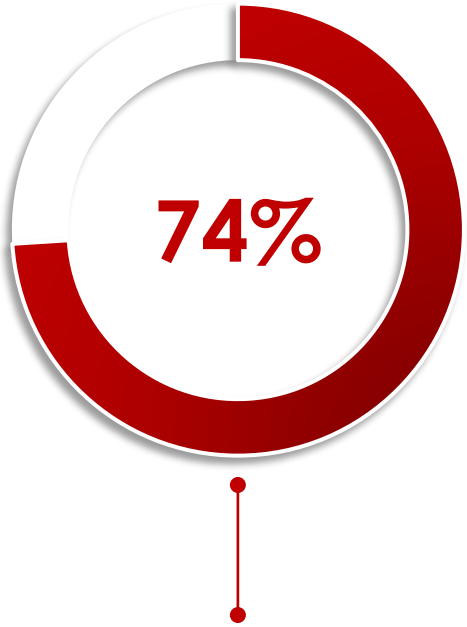
Cybersecurity Professional Services Manager

Katerina Gounari

Capacity Building Manager

Infocom Security 2024 – 11/04/2024

Current reports (Y-2023) show....

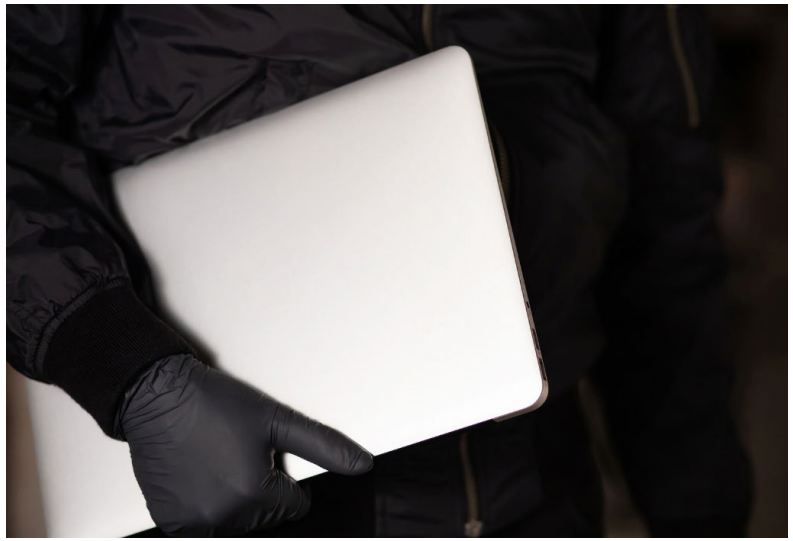


of breaches involved the **human element,** which includes social engineering attacks, errors or misuse.

Verizon's 2023 Data Breaches Investigations Report

In the future Organizations will have to deal with….

INCIDENTS…



But we have an established Cyber awareness training….

Generic training material that does not reflect corporate strategy

Undefined or unclear training objectives

Ignoring user's perception of the training activities

Relying on typical KPIs to evaluate the outcomes of training activities

LIMITATIONS

- **Customization is time consuming**
- **Security Teams are understaffed**
- **Budget is spent on technology**

Behavior change is an ambitious (and necessary) goal!

- Learning in the correct context.
- Repeating actions to embed knowledge.
- Continuous evaluation to adopt strategy.
- Rewarding staff to encourage new habits.

What should we make differently ?

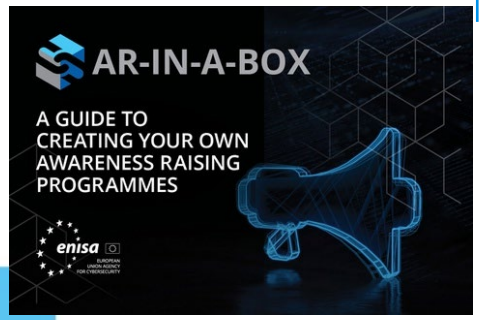
- **Different forms** of education for **different learning types**
- **Different forms** of education for **different roles**
- Promote **local security culture**
- Performance **evaluation** with **appropriate KPIs**

Cyber Noesis ©2024

TOWARDS BUILDING A USER CENTRIC TRAINING APPROACH!

ISAWARE

ENISA – AR IN A BOX



Our Approach... ISAWARE

SURVEILLANCE AUDITS

INTERVIEWS WITH EMPLOYEES

REVIEW PREVIOUS AWARENESS ACTIVITIES

BASELINE PHISHING EXERCISE

Step 01

Analyze Current Status

Cyber Noesis ©2024

RAISE CYBER AWARENESS

PROMOTE SECURITY CULTURE FOR SPECIFIC TOPICS

COMMUNICATE POLICIES

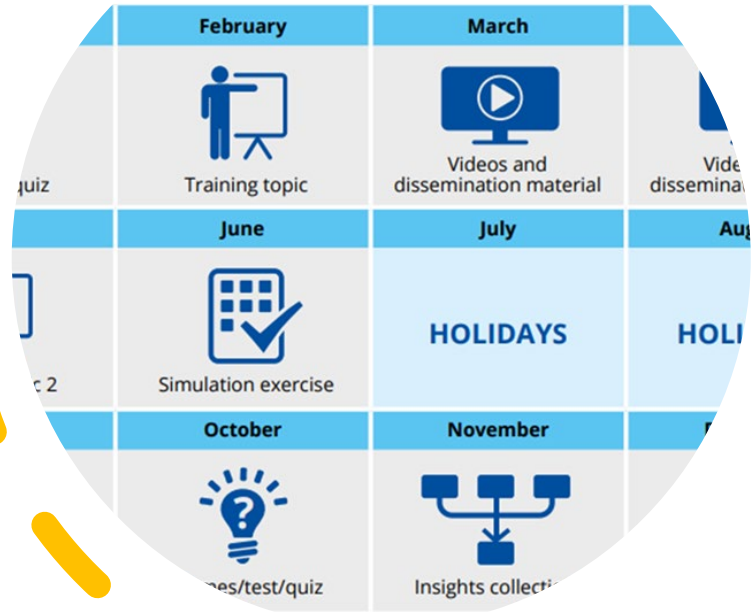
IMPROVE USERS' PERCEIVED CONFIDENCE IN RECOGNIZING SECURITY THREATS DURING THEIR DAILY ACTIVITIES

Cyber Noesis ©2024

SPLIT USERS INTO GROUPS

CHOOSE THE RIGHT MEANS DELIVERY METHODS FOR THE VARIOUS GROUPS & / LEARNING TYPE

SET A TIME PLAN



Cyber Noesis ©2024

S	Specific
M	Measurable
A	Achievable
R	Relevant
T	Time-bound

PHISHING SCORE (%)

PHISHING REPORTING SCORE (%)

SECURITY CULTURE
(Policy Awareness, Physical Security Issues, Information Handling, Perception Of Everyone's Responsibility For Cybersecurity, Passwords, etc.)
(Knowledge Questions – Audits)

USERS' PERCEIVED CONFIDENCE IN RECOGNIZING SECURITY THREATS DURING THEIR DAILY ACTIVITIES (Surveys)

Step 05 Evaluate Program

Cyber Noesis ©2024

WHEN FOCUSING ON USERS' NEEDS, THERE ARE SEVERAL PARAMETERS THAT WE NEED TO CONSIDER...

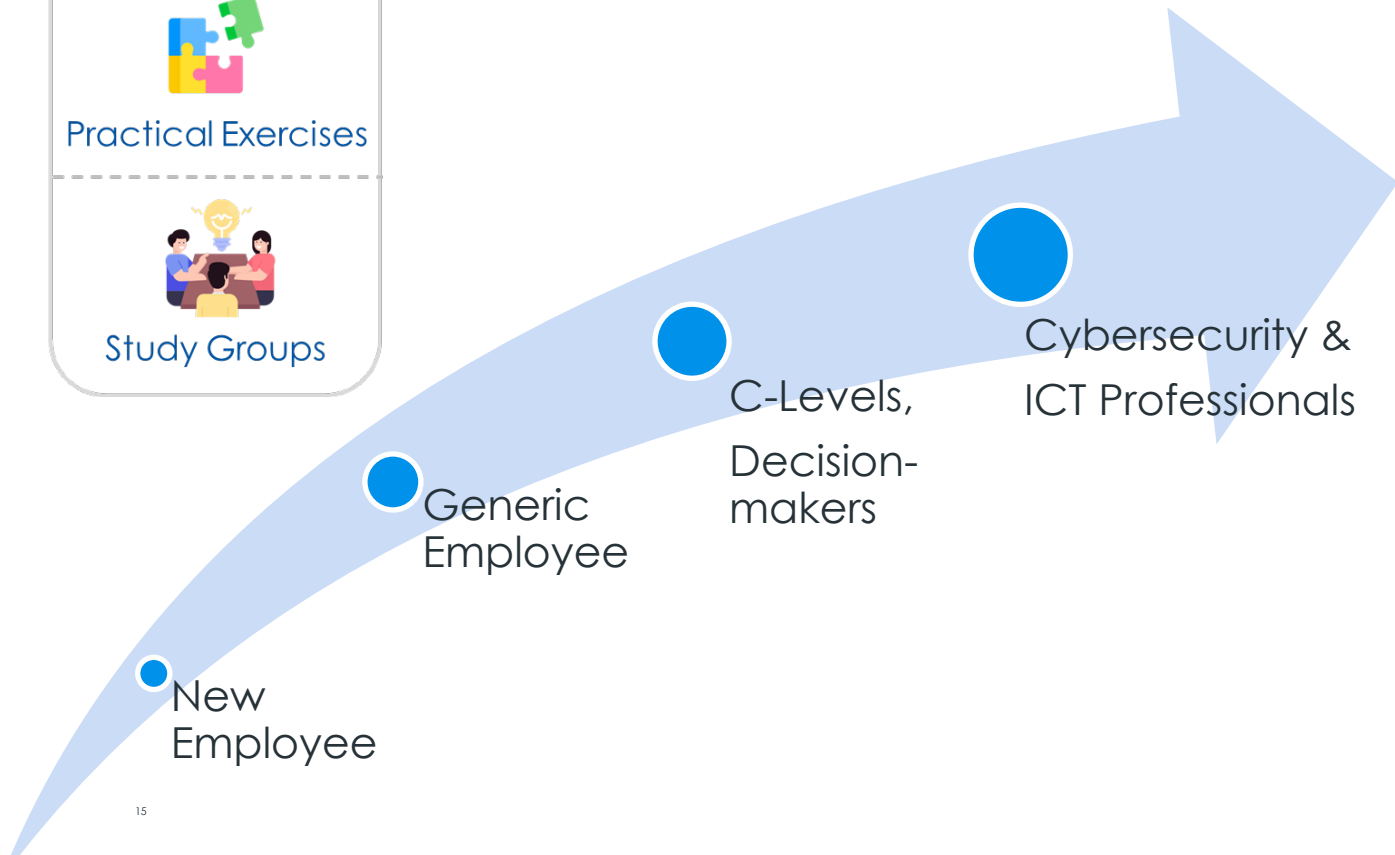
Every individual has its own specific learning profile

Every employee has a different level of knowledge and engagement

ISAWARE

Learning Paths & Topics per Role

	Visual Learner	Auditory Learner	Reading Learner	Kinesthetic Learner
Tactic 1	Color	Recording	List	Practical Exercises
Tactic 2	Diagram	Discussions	Notes & Text	Study Groups



Learning Styles Strategies…

- **Mix instructional methods of delivery**
  - Videos with audio and captions
  - Slide presentations and verbal instructions
  - Flyers
  - Exercises & role-playing assignments
- **Use custom material**
  - Customize training material based on corporate culture and processes
- **Offer choices to learn**
  - Set clear learning objectives
  - Allow selection of learning paths and methods
  - Feedback through user surveys
- **Assess learners often**
  - Define KPIs in a way that they provide measurable and qualitative insights

Cyber Awareness is more than training.

Cyber Noesis ©2024

Cyber Noesis

Thank you!

ISAWARE

www.cybernoesis.com