



# AR-IN-A-BOX

## How to Build your Custom Awareness Program

Evangelos Kantas, Cybersecurity Expert, ENISA

BE THE STRONGEST LINK  
BREAK THE KILLCHAIN



# CYBER AWARENESS PROGRAM

*“An (internal) marketing strategy designed to raise **cyber security awareness**.”*

- ✓ Teaches employees **how to mitigate the impact of cyber threats**.
- ✓ A plan encompassing multiple awareness-raising activities over a long period of time following the organisation’s strategy for cybersecurity.
- ✓ It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target group.

# WHY HAVE ONE?

- New threats are emerging.
- Organizations can no longer just rely on their technological defenses to be safe.
- Cybercriminals use sophisticated social engineering techniques to by-pass defenses.
- All it takes is one employee to click on a malicious link and it's game over!
- Your employees are your first line of defense.

**A comprehensive Cyber Security Awareness program is the best way to educate staff and create a security-first culture.**

# STILL NOT SURE?

## ISO 27001/2 & Information Security Awareness Training

For ISO 27001 compliance, it is essential to comply with **clause 7.2.2**.

The ISO 27001/2 clause 7.2.2 states:

*'Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function'.*



# AR-IN-A-BOX REVIEW



# DESIGNING A CYBER-AWARENESS PROGRAMME



# SETTING OBJECTIVES

1



Identify objectives



Overall goals for awareness and learning



Definition of SMART awareness objectives



Selection of specific material, tools, methods

## Awareness-raising objectives stem from the risk assessment of the organization and help:

- ✓ To promote cybersecurity education and culture
- ✓ To be prepared for incidents.
- ✓ To develop an understanding of emerging cybersecurity threats and landscape
- ✓ To promote cybersecurity culture and hygiene
- ✓ To test policies and procedures

# FINANCIAL RESOURCES



## MANAGEMENT:

- Plays a critical role.
- Make sure they are involved in the design and the objectives-setting phase of the awareness programme from an early stage.
- Budget allocation depends on their support.

## TIPS:

- ✓ Try to identify the must-do topics of your programme and the must-train employees who will minimise the risk for your organisation when trained.
- ✓ Reuse or update existing material or resources.
- ✓ Select open-source material or create it in-house.
- ✓ Exploit synergies in the community where available.



# HUMAN RESOURCES

3



Ensure human  
resources

- ✓ **Management**
- ✓ **Cyber Security Officer**
- ✓ **Public Relations & Communications**
- ✓ **ICT**
- ✓ **HR**
- ✓ **DPO / Legal**
- ✓ **Content Developers**
- ✓ **Instructors**



# TARGET GROUPS



**Table 1. Employee target groups**

Audience groups		Clustered audiences
1	Generic employee	Generic employee
2	Contractor	
3	HR	
4	Communications and marketing	
5	Legal	
6	Operations and research and development	C-level, decision-makers, handling budgets
7	Finance and procurement	
8	Managers, officers	
9	Heads of unit, directors	
10	Cybersecurity professionals	Professionals / horizontal implementors of cybersecurity measures and users of cybersecurity solutions, working for organisations and/or individuals
11	Information technology (ICT) professionals	

# SELECTING THE RIGHT TOOLS

5



Choose the right means



## Infographics - Posters

Easy to deploy physically, e.g. in elevators, common spaces



## Ads - Videos

Able to hold and convey a lot of information



## TOOLS FOR AWARENESS RAISING



## Puzzles - Quizzes

Ensure and test understanding of concepts



## Live presentations

Direct interactions with participants

# HEALTHCARE SECTOR CAMPAIGN

## Cyber Health Week 2022

Welcome to the official page of the Cybersecurity Healthcare Week 2022!



**6 – 12 JUNE IS**  
 Cybersecurity Healthcare Week 2022  
 #CyberHealthWeek  
 #BoostYourCyberVitals

Join us for CyberHealthWeek  
 #BoostYourCyberVitals

**Ensure the continuity of clinical services – Information availability:**

Make your healthcare organisation resilient to cyber incidents

In other words, make sure your clinical services are always available and patients have continuous access to them!

But, how?

By having a recovery plan that will help you:

- Respond swiftly
- Deliver services in abnormal circumstances
- Quickly get back to business as usual

A cyberrip, a day keeps the hackers away!

#BoostYourCyberVitals

**Don't take the bite!**

Immunise yourself from phishing infections!

**THE THREAT**

Fraudulent attempts to steal user data are usually launched through e-mail, appearing to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent URL.

**SOME PHISHING FACTS**

**OVERALL OVERVIEW**

Number of phishing attacks has **TRIPLED** since 2019 (not from) early 2020  
 Phishing attacks hit an **ALL TIME HIGH** in 2021  
 Phishing accounts for **90%** of data breaches

**HEALTHCARE SECTOR OVERVIEW**

Cyberattacks on healthcare sector saw a **71%** increase in 2021

**PHISHING MADE IT TO THE RANKS**

Phishing is found as the most common significant security incident and the most common initial point of compromise

Good news is I have a prescription for phishing immunity.

Let's make some checks looking for a pathogen pattern!

**Cyber-hygiene: a set of simple routines to minimise the risk of cyberthreats and information leaks.**

**PROTECT YOUR HEALTH DATA**

To prevent information leaks and unauthorised access to your devices you must never leave sensitive information unattended. The moment you are not on your workstation, devices, must be locked, and papers must be safely stored. Also, back up your data regularly.

**BROWSE SAFELY**

At work, browse only secured websites (https) related to your duties and never download unauthorised software.

**KEEP YOUR SYSTEMS UP TO DATE**

To keep yourself fully protected, use an anti-malware solution on all your devices and implement all available updates as soon as possible.

**KEEP YOUR DEVICES SECURED**

Choose strong passwords, keep them secret and unique for each service, change them regularly and use a password manager. Use an extra step when you log-in, such as a code sent to your phone or a fingerprint scan (two-factor authentication).

**CONNECT SAFELY OVER PUBLIC WI-FI**

Avoid connecting to public Wi-Fi networks. If you have no choice, verify the network, keep your antivirus enabled, avoid entering credentials or performing financial transactions and ask the IT personnel for Access through VPN.

#BoostYourCyberVitals




# PLANNING

6



Create a timeplan

January	February	March	April
 Baseline quiz	 Training topic	 Videos and dissemination material	 Videos and dissemination material
May	June	July	August
 Training topic 2	 Simulation exercise	HOLIDAYS	HOLIDAYS
September	October	November	December
 Back-to-school training	 Games/test/quiz	 <u>Insights</u> collections	 Report to management

# IMPLEMENTATION

**Cybersecurity training is an ongoing process.**

Ensure that your security posture is as mature as it can be, even as your company and the cybersecurity landscape grows and evolves.

**Three periods are considered relevant for delivering cybersecurity-awareness training to your employees:**

1. when they join the organisation as part of the induction process
2. after an incident, in order to indicate the procedures, roles and responsibilities in place;
3. at regular intervals throughout the year (see calendar)



# EVALUATION

8



Evaluate the program

A KPI is a value that measures a component of an awareness-raising campaign or programme.

There are five reasons why KPIs fail to improve performance:

1. the KPIs are poorly defined;
2. they lack accountability;
3. they are not achievable;
4. they are not specific enough;
5. they are too hard to measure.





# MAGNIFY THE EFFECT

- Quick wins count
- Keep it simple
- Identify strategies to magnify the effects of your program
- Train-a-Trainer
- Cyber Awareness Champions
- Inject Cyber Awareness in other events (Ex. team building events)



# CYBER AWARENESS GAMES

## Gamification helps!

- ✓ Determine how your team will react to a theoretical cyber attack and how effective your plan is.
- ✓ Identify flaws or gaps in the organization's response and make adjustments
- ✓ Testing consequences in a safe environment
- ✓ Coordination between different departments
- ✓ Save money



# QUIZZES



EUROPEAN UNION AGENCY FOR CYBERSECURITY

Which type of cyber-attack is commonly performed through email?

- Phishing
- Smishing
- Vishing
- Ransomware

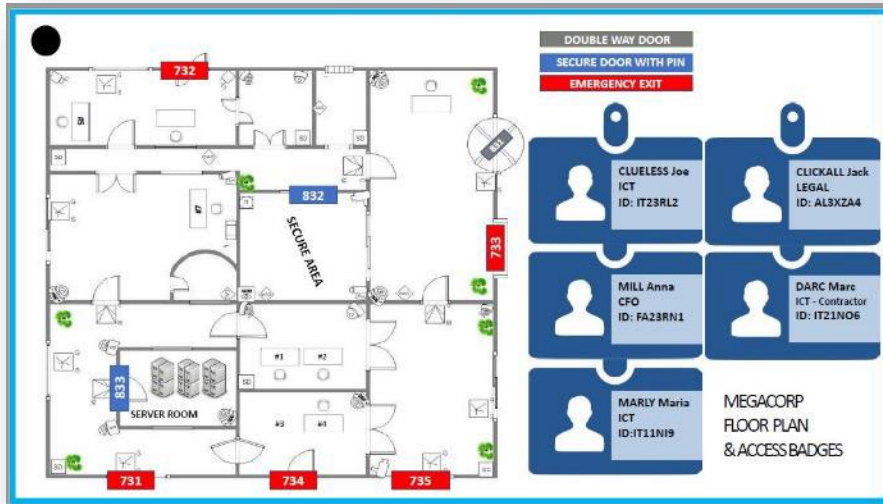


## Phishing

**CORRECT!** The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).

Other choices: **INCORRECT**

# TABLE-TOP GAMES



## SCENARIO - MEGACORP HACKED

**MEGACORP** MegaCorp, a leader in online retail has been hacked based on information leaked on the public Internet.

Attackers appeared to have gained initial access via a successful **PHISHING ATTACK**.

To make matters worse **UNAUTHORISED ACCESS** has been detected in MegaCorp headquarters and a **RANSOMWARE** hit the company the same day.

You are the lead Cyber Security Investigator recruited to provide answers on who is behind the hack and try to stop him/her before its too late.

We gathered as much evidence as possible. Analyze them quickly.

You have 30 minutes left before all our data are wiped out.

**GOOD LUCK!**

## ANSWER SHEET

What is the name of the first known victim of the PHISHING ATTACK?  
 (Name Surname as seen in the Badge with space\*)

Which Badge ID was used to performed unauthorized access?

ENCIPHERMENT KEY

What is the filename of the decrypted file?

# AR-IN-A-BOX: METHODS OF DELIVERY

## 1 Training-at-your-own-pace

**Set Up:** Online access to Material  
**Content:** [AR-in-a-Box — ENISA \(europa.eu\)](#)



## 2 Virtual or Physical Workshop

**Set Up:** 1-2 days Workshop  
**Content:**

- Theory of building an Awareness Raising Program
- Use of Communications dept in real life
- How ENISA supporting tools can be best utilized to deal with cyber crisis.

**Delivery upon Request**

## 3

**PRACTICE MAKES PERFECT**

# THE FUTURE -2023



- ✓ **Crisis Communications guide**
- ✓ **Sector agnostic, editable, customizable material for an AR campaign on phishing and cyber-hygiene (leaflets, posters, videos, quizzes, etc)**
- ✓ **Expansion packs for Game including other kinds of threats/incidents (e.g. BYOD, DDOS)**
- ✓ **Online version of the Game**
- ✓ **Translations**

**GIVE US SOME  
FEEDBACK!**



[EUSurvey - Survey  
\(europa.eu\)](https://europa.eu)



**AR-IN-A-BOX**

Thank you

**BE THE STRONGEST LINK  
BREAK THE KILLCHAIN**

