EUROPEAN CYBER SECURITY ORGANISATION

BUILDING THE FUTURE OF EUROPEAN CYBER SECURITY AWARENESS CAMPAIGNS

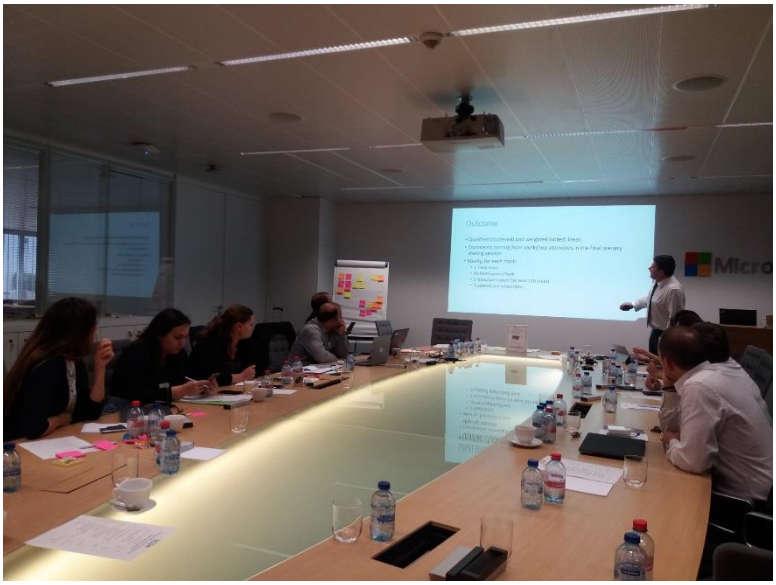
Outcome paper from ECSO workshop

Context

The aim of the ECSO Cyber Security Awareness Workshop which took place in Brussels on 20th June was to offer a full day of presentations, breakout sessions, and networking with professionals and decision-makers from industry, academia, SMEs, governmental and EU officials in order to:

- Provide a solid idea about how to design a cyber security awareness campaign strategy
- Present several tracks with experiences focusing on relevant challenges and opportunities
- Coach to ideate solutions and build new ideas
- Enhance skills mastery and personal development
- Stimulate cooperation between stakeholders

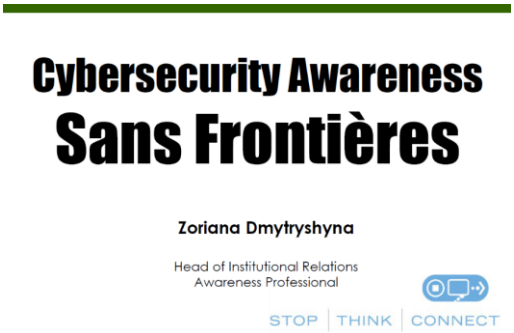
The workshop engaged target audiences with various perspectives about awareness campaigns, piloted by the ECSO SWG5.3 members, in order to support the production of more targeted events and materials to c-level executives.



ECSO members best practices

The workshop focused on 4 tracks, each piloted by ECSO members who shared their best practices:

Track 1: Communication and content sharing strategies – APWG



STOP.THINK.CONNECT CAMPAIGN

We need a label just as common as a no-smoking or biohazard label

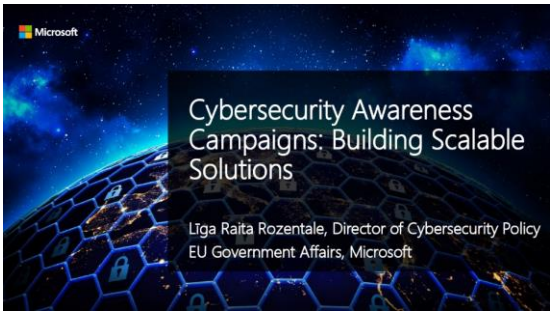
STC messaging free for all users

To use STC kit, it is best to sign an MoU

20 national campaigns deployed worldwide

→ https://www.stopthinkconnect.org/

Track 2: Scalable Solutions – Microsoft



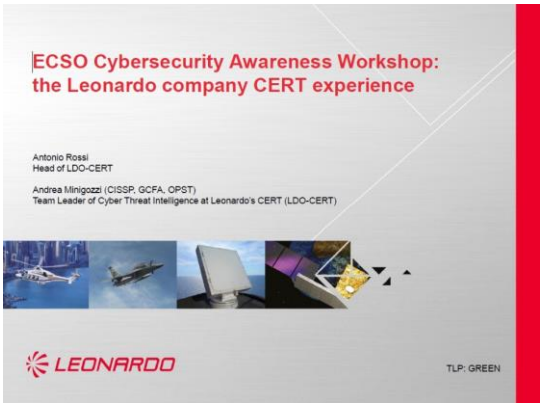
Focus on cyber hygiene, commercial measures, and political and diplomatic responses

Election security – Campaign security – Advertising transparency – Disinformation defense

Train the trainers (Microsoft's training has reached around 1000 people involved in EU elections across 28 MS)

→ Take advantage of the ecosystem

Track 3: Security processes and technologies – Leonardo



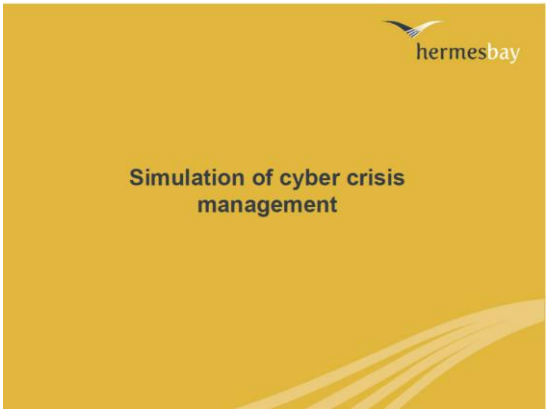
The weakest chain in the link is between the keyboard and the chair – most vulnerable system is the human brain

Leonardo-CERT approach to cybersecurity awareness – Induction – Maintaining – Assessment – Improvement

Internal trainings

Cybershield 2018 (CTF War Room and "Proxy Bar")

Track 4: Metrics on cyber security awareness – Hermes Bay



Simulation - organisation of role play

Four steps: Warming up – Action – Cooling off – Analysis

Involves managers, experts…everyone

You need a stage (crisis committee table, CERT/SOC infrastructure, "attacker" hacking station), actors (performing all the main corporate roles), and narrator (underlining causes and consequences of choices throughout)

Awareness campaign concept designs

Workshop attendees split up into 4 groups to further ideate and discuss the challenges & opportunities for each track, in order to come up with an "awareness campaign concept design":

Design 1: Communication and content sharing strategies

Name of concept		
"IoT: I Own Technology"		
Description		
Campaign to raise awareness about risks & opportunities associated to IoT		
What problem is it solving		
Lack of understanding and awareness of IoT risks (privacy, security,…)		
Value for citizens	**Value for companies (private)**	**Value for Institutions (public)**
Enable informed choices (aware about privacy & security risks)	Improve business & processes	Trigger to produce basic regulatory framework
Key features for public and private		
IoT pervasive and new: needs PPP, media interaction, continuous campaigning (ex: ENISA and Europol/EC3)		
How do people learn about this?		
Citizens: game "find the IoT in your house", video/tv ad, poster Companies: game ("find & use IoT in your company") Institutions: workshops/roundtables, policy briefs		
How do companies and Institutions interact?		
Workshops/roundtables, online platform or forum, dedicated events		
What technology is involved?		
Website, app, social media, live events, demos		

- **Clustered ideas**:
  1) IoT, phishing, cyber hygiene, spyware, ebanking, personal information, ransomware
  2) Security by design, develop common standards, cyber security basics for SME's
  3) Cyber basics for the older generation
  4) Gamification, use ambassadors ("influencers"), unique advertising, social, viral, human element
- **Key takeaway**: Just like cyber hygiene, this type of campaign should be continuous so it becomes a habit. Awareness starts at the basic level. Ex: NotPetya (Maersk): there was no "hand washing" – we haven't reached the point yet where everyone is washing their hands as a habit/automatism

Design 2: Scalable solutions

Name of concept		
"Scalability: Find the Right Message"		
Description		
Quality, quantity, targeting		
What problem is it solving		
Match behavioural change with limited resources		
Value for citizens	**Value for companies (private)**	**Value for Institutions (public)**
Reachability	Reduce costs	Increase trust
Key features for public and private		
Train the trainers Mix media Rewards		
How do people learn about this?		
Legislation, social media, and traditional media		
How do companies and Institutions interact?		
PPP (ECSO), best practices, info sharing, cooperation		
What technology is involved?		
Mix communication means: Video, ads, true story, news		

- **Clustered ideas**:
  1) Train the trainers, mix communication and media, awards
  2) Legislation, right message and info, real life stories, ambassadors, in-company differentiation
  3) Change the behaviour, match target and complexity
  4) Learning by doing, alert campaigns (texts and videos)
- **Key takeaway**: Public-private partnership/collaboration is key: sharing content, best practices, and cooperating with the ecosystem. eLearning should be combined with face to face learning and you must prioritise what you want to teach. Stay close to the human level (awareness, not technical)

Design 3: Security processes and technologies

Name of concept		
"Cyber driving license"		
Description		
Cyber driving license (with a points system), hands on training		
What problem is it solving		
No technical language		
Value for citizens	**Value for companies (private)**	**Value for Institutions (public)**
Open their eyes: better understanding of risks Better security	Awareness: security is not only an IT matter	Maintain a good level of awareness
Key features for public and private		
Tracking awareness level Isolate risks Track training effectiveness		
How do people learn about this?		
Company policy Public campaign Schools Market incentives		
How do companies and Institutions interact?		
Ratings Autonomous access when a license is owned		
What technology is involved?		
Cyber range Public database record Standard to authorise the various licences		

- **Clustered ideas**:
  1) Proactiveness, capture the flag, cyber ranges, all things that can be automated should be automated
  2) Eliminate process gaps, simplicity, relevance, adaptive, feedback loop
  3) Transparent MFA, push content periodically, live demos
  4) Use social profiling capabilities to address awareness, use location to push more relevant content
- **Key takeaway**: The advantage of a cyber driving license is that it can be used to test the effectiveness of your campaign. To succeed, it will need scalability, communications, and content.

Design 4: Metrics for cyber security awareness

Name of concept		
"Metrics for Cyber Security Awareness"		
Description		
Macro indicators for success in cyber awareness, reaching 4 dimensions: outside validation, security, "channel", behavioural, through dedicated sub-indicators		
What problem is it solving		
How to measure a campaign in an objective way, monitoring the situation before and after the campaign		
Value for citizens	**Value for companies (private)**	**Value for Institutions (public)**
Have more focused and more effective campaigns	Cost-effective campaigns Easy to monitor Comparable offers to evaluate More transparency	Transparency Accountability made possible
Key features for public and private		
Analytics, dashboard, general agreed methodology		
How do people learn about this?		
Public stats by Institutions		
How do companies and Institutions interact?		
Shared objective framework		
What technology is involved?		
Big data architecture		

- **Clustered ideas**:
  1) Impact of social networks, return rate
  2) Feedbacks and reports on scams, perception shift, test group
  3) Criminal stats impacting company, website built for awareness, partners/stakeholders
  4) HR stats, customer panels, effectiveness
- **Key takeaway**: With a metrics framework, it would be possible to build a standardised and quantitative approach for cyber security awareness in Europe (leveraging on work done by ENISA, ECSO, etc.)

TIPS FOR YOUR NEXT AWARENESS CAMPAIGN

- ✓ Focus on basic cyber hygiene – use simple labels, like a no-smoking label
- ✓ Take advantage of the ecosystem – scale your initiative
- ✓ Implement measures for monitoring basic cyber security knowledge and skills, such as a “cyber driving license”
- ✓ Focus your awareness initiative at the human level (non-technical)
- ✓ Come up with unique and engaging tools and ads to get people’s attention
- ✓ Use ambassadors to promote your initiative
- ✓ Mix e-learning with face to face learning
- ✓ Implement metrics to test the effectiveness of your campaign, before and after launch

---

Do you have a cyber security awareness best practice that you would like to share with us?

Send an email to **wg5_secretariat@ecs-org.eu**