Cybersecurity Awareness Trainings: A Practical Guide

1. Introduction: Cybersecurity is every manager's responsibility

There is an urgent need to boost digital competences in Europe. According to the Digital Economy and Society Index, 37% of the EU workforce has low digital skills, or none at all. At the same time, cybersecurity experts generally agree that the majority of breaches are the result of human error. Senior leaders have an important role to play in both creating a culture of cybersecurity awareness and in protecting themselves against the threats they are likely to face. On the former, managers are well positioned to create a whole-of-organisation culture of responsibility for cybersecurity. In today's workplace, every employee in an organisation across virtually every industry uses technology in their daily work, making cybersecurity no longer only an IT-department issue. In addition, executives are often the primary target of spear-phishing and Advanced Persistent Threat (APT) attacks, so it is important that they are made fully aware of the techniques used by malicious actors and what they can do to protect themselves and their organisations.

As the heart of policymaking across the EU, the European Commission must be exceptionally prepared for and aware of the cyber threats they may face. To help Commission managers secure themselves and their organisation we offered hands-on training that enabled senior leaders to take actions themselves, and to prepare their teams to deal with the cyber threat landscape. Through a series of workshops, Commission representatives received trainings to build their knowledge and secure processes at work.

This guide is intended to present concrete advice, suggestions and tips on how to best organise cybersecurity awareness trainings.

2. European Cybersecurity Month: ECSO-Microsoft's Engagement

The European Cybersecurity Month (ECSM) is the EU's annual awareness raising campaign that takes place in October and aims to promote cybersecurity among citizens and organisations, provide up to date security information through education and share best practices. Cybersecurity awareness is central to Microsoft's work in promoting trust in technology for all our users everywhere. For ECSM, Microsoft provides practical training and interactive learning opportunities to drive understanding of key cybersecurity issues for EU policy makers.

The theme for week two of the ECSM in 2018 was "Expand your digital skills and education." In partnership with the European Cyber Security Organisation (ECSO), Microsoft offered an in-person training to promote end-user education and improve cybersecurity literacy. The training took place over three 90-minute breakfast series and covered cyber threats, vulnerabilities and countermeasures unique to senior EU policy makers.

3. ECSO-Microsoft Cybersecurity Breakfast Series

The series consisted of three workshops covering the following topics: (1) "Building your Cybersecurity Policy Foundations"; (2) "Building your Cybersecurity Toolkit"; and (3) "Practicing your Cybersecurity Culture".

- "Building your Cybersecurity Policy Foundations", 12 October, 8:00-10:00:

In this foundational course, we provided an overview of the state of cybersecurity and cybercrime today. We covered the most common cyber threats, such as tech scams, malware attacks, phishing and social engineering, but also provided more insight into nation-state attacks and ongoing diplomatic efforts to address cybercrime and cybersecurity threats.

- "Building your Cybersecurity Toolkit", 16 November, 8:00-10:00:

In this course, we provided tools to avoid common security mistakes and protect yourself from different tech scams and online fraud when using technology. We also gave attendees practical solutions to protect themselves.

- "Practicing your Cybersecurity Culture", 7 December, 8:00-10:00:

The final workshop in this series concentrated on incident response – at international, enterprise and individual level – bridging related policy and technical discussions and practicing some cyber skills learned during the previous sessions.

Did you know?

- Between 2017-2018 Microsoft's cybersecurity teams monitored 376 policy developments across 96 countries worldwide. They looked at eight subcategories and found that by far cybersecurity policy, which includes developments such as national cybersecurity strategies or cybersecurity agencies, was the clear front runner at 55% of total policy developments within that period.

- In terms of geographic representation, Europe made up the largest region for policy development at 33%, followed by the Americas at 30%, Asia-Pacific at 23% and Middle East and Africa at 14%.

- Over 90% of successful cyber-attacks begin with a phishing email and from that 4% of people will click on any given phishing campaign. The more clicks, the more likely to do it again.

- The intent of 91% of phishing attacks are to steal a user's credentials!

- There has been a 90% rise in business-targeted ransomware – nearly doubled from 82,000 in 2016 to 159,700 in 2017.

- Since the majority of cyber incidents are never reported, the actual number in 2017 could easily exceed 350 000.

- 2 out of 3 people have experienced a tech support scam.

- $4M is the average cost of a data breach in 2017.

- 99 days is the average number of days between infiltration and detection of a cyber-attack.

- Multi Factor Authentication (MFA) reduces the risk of an attack by 99.9%!

Our tips for future workshops!

Do…

… Organise your workshop during *breakfast or lunch*: this may increase attendance as you won't interfere with people's daily schedule.

… Make it *interactive*: use tools such as Mentimeter and encourage questions to spark lively and interactive discussions.

… Tell a story: people tend to remember *facts over principles*. Explain best and bad practices through real stories. Make it personal to help them understand the direct negative impact of poor security.

… Make it real: *simulate a hack* to show how the most dangerous cyber-attacks work in practice.

Don't…

… Overdo it with slides: keep *slides to a minimum and prioritise visual aids* which will help create an interactive environment.

… Go too technical: if your audience has no technical knowledge, there is no point in going into the technical ways that cybersecurity works. Use *simple language and hands-on practice*. Understanding your audience and tailoring your workshop is crucial.

… Use *open-ended questions* in your feedback survey. People will respond more readily to multiple choice or yes / no questions.

Do you have suggestions? Ideas? Contact us!

For Microsoft, send an email to Simona Autolitano t-siauto@microsoft.com
For ECSO, send an email to wg5_secretariat@ecs-org.eu