137123/EU XXV. GP
Eingelangt am 17/03/17

Council of the
European Union

**Brussels, 17 March 2017
(OR. en)**

6142/17

**CYBER 16
MI 249
FREMP 32
TELECOM 63
JEUN 36**

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	CM 1124/17
Subject:	Prevention and Cyber Awareness across the EU among its citizens and its SMEs - Detailed Report on the Outcome of the Questionnaire

Delegations will find in the Annex the detailed Report on the outcome of the Questionnaire:

Prevention and Cyber Awareness across the EU among its citizens and its SMEs.

ANNEX

Detailed Report on the Outcome of the Questionnaire (CM1124/17): Prevention and Cyber Awareness across the EU among its citizens and its SMEs

1. Introduction

Cyberspace is increasingly forming an integral part of how individuals, organisations and governments across the globe, communicate and conduct business. It allows for a paradigm where everyone may easily and rapidly be able to connect to an intricate web of connected individuals, devices, businesses, processes and data, anytime and anywhere. Unfortunately, such an opportunity comes at a cost; with inherent collective vulnerabilities at a technical and at a human level, leading to various security and trust related issues.

On a pan-European level the latest Eurobarometer survey on cybersecurity indicates that more than half of European citizens access the Internet on a daily basis through various means and for a variety of purposes. The trends also indicate an increased concern for the misuse of personal data and security in the conduct of electronic commerce. Such concerns could undermine the level of trust needed to ensure the success of the Digital Single Market across the European Union. Furthermore, the survey indicates that just under half of EU citizens believe that they are well informed about the risks of cybercrime. The notion of cyber risk is also of particular importance to European businesses, including SMEs which make up the majority of the EU economy. Thus, it needs to be ensured that citizens and businesses are aware and can recognise the risks to their online security and safety, whilst exploiting cyberspace to its full potential.

The Presidency believes that such challenges can be addressed by focusing on a cyber secure culture brought about by an ongoing cybersecurity awareness campaign that focusses on the various sectors of the European society and economy.

The inculcation of a cyber secure culture calls for a holistic and concerted Pan-European effort to ensure that the most vulnerable citizens and SMEs which are often resource constrained, are alert and prepared for any potential compromise to their security in cyberspace. It is within such understanding that the Presidency has affirmed the need to establish an overview and assess the cybersecurity awareness activities carried out across the European Union.

2. The Process

The Presidency has obtained feedback from Member States on their coverage, challenges and expectations of any cyber security awareness campaigns on a national level. In parallel it has sought to establish an overview of cybersecurity awareness activities undertaken on a Pan-European level by the EU Agencies particularly, ENISA and EUROPOL. The aim was to develop on that basis a course of action, leading to a holistic and effective cyber awareness campaign that engages all relevant EU bodies and Member States in reaching out to citizens and organisations, focussing on SMEs in the case of the latter.

3. The Questionnaire

The Presidency circulated a Questionnaire (CM1124/17) to all Member States so as to assess the current cybersecurity awareness campaigns including any future plans, challenges, lessons learnt and requirements. A total of 20 Member States replied to the questionnaire and provided valuable insight in the process.

The Questionnaire focussed on obtaining information on the following points:

(1) The Member States' approaches to national cybersecurity awareness campaigns, including the current and envisaged means, methods and outreach as well as the envisaged cyber threat scenario that the campaign is addressing.

(2) The metrics used to measure the success of the deliverables, milestones and lessons learnt.

(3) Any coordination with EU bodies and their current input to national campaigns.

(4) The Member States’ challenges and requirements within a context of prevalence of security incidents and other difficulties in conducting their campaign(s).

4. The Questionnaire Findings

4.1 Summary

The replies from Member States indicate that the conduct of a cybersecurity awareness campaign in most cases entails the involvement of various entities, with some focussing on a specific audience. In such a scenario, ongoing collaboration and coordination is key to ensure a successful coverage of a cybersecurity awareness campaign across a Member State. The findings also reveal that cooperation needs to be extended on a pan-European scale to harmonise learning and support in a complex scenario dominated by a rapid evolvement of cyber challenges including resource availability and preparedness requirements for an ongoing cyber awareness campaign.

4.2 The Conduct of the National Awareness Campaign

4.2.1 The Campaign and the target audience

- The majority of respondent Member States (90%) stated that they are conducting a national awareness campaign and that is an ongoing process. In a number of cases, various entities within a Member States were responsible for targeting specific sectors. Hence, the information provided unless centrally coordinated could reflect only part of the respondent's remit of responsibility.
- **Awareness by the majority of the respondent Member States is aimed at the Public Sector (80%) followed by adults, children, adolescents (70%) and SMEs (60%)**, other private sector organisations (55%), elderly and vulnerable (35%) and Minority Groups (15%). Future awareness raising is expected to remain with a slightly increased majority of MS (85%) towards the Public Sector, children (75%) followed by adolescents, adults and SMEs (70%), other private sector organisations (60%), elderly and vulnerable (55%) and minority groups (30%). Hence whilst there is a retained majority towards adolescents and adults, more **Member States are expected to focus on SMEs, children, elderly and vulnerable, minority groups and other private sector organisations in their future awareness campaigns**. Additionally, in both current and future campaigns targets also include individuals and organisations in occupationally sensitive areas and in managerial roles.

www.parlament.gv.at

The majority of respondent Member States specify that they are conducting a national awareness campaign on an on-going basis. Whilst the Public Sector as one of Member States' largest recipient of sensitive information is understandably one of the primary target of cyber awareness campaigns, a strong focus is equally noted towards citizens and SMEs. Such focus is expected to retain its intensity especially towards vulnerable members of society in the future.

4.2.2 The Communication Channels

- **Events such as conferences and specialist meetings** (63 specific instances), **Social media** (45 instances) and **leaflets and brochures** (31 instances), appear to be the most resorted means to conduct a cybersecurity awareness campaign. This is followed by television (26 instances), newspapers (19 instances), radio (17 instances), webinars (12 instances) and online ads (11 instances). Reference has also been made to other forms not specifically referred to within the questionnaire such as specialised training sessions to students, parents and educators (12 instances), email distribution (7 instances), story books and specialist articles (5 instances), websites and the use of interactive modules, games, social debates (4 instances), adverts on public transport (2 instances) and partnering with trusted organisations having a wide customer/membership base (2 instances).

- More specifically, dedicated **events appear to be the most resorted medium by respondent Member States in the case of children, adolescents, public sector (55%), SMEs and other private sector organisations (45%)**. **Social media is mostly resorted to in the case of adults and adolescents (50%), children (30%), public sector and SMEs (25%), other private sector organisations (20%), minority groups (15%) and elderly (10%). Leaflets and brochures are being applied for adolescents, adults and public sector (30%) followed by private sector organisations (20%), children and SMEs (15%), elderly (10%) and minority groups (5%). Online ads are mostly aimed towards adults (20%) and SMEs (15%), adolescents (10%) and children & public sector (5%).**

- **Traditional forms of media such as television and radio are being applied to reach out to adults (35%), elderly (25%), public sector (20%) and other private sector organisations (15%); Radio in the case of Adults and Public Sector (20%), Elderly and SMEs (15%) and others; Newspapers in the case of Adults and Public Sector (20%), SMEs (15%), Elderly and private sector organisations (10%).** Billboards appear to be minimally applied on a Pan-European level, with their use limited to adolescents, public sector and private sector (5%).

- Consideration also needs to be made to other forms of communication channels identified that are deemed to be effective within specific sectors such as training sessions/programs/interactive workshops/courses/social debates to the public sector, adolescents and children – even as part of the curricula in the latter two audiences; the use of interactive modules, games for children and adults; mass email distribution to the public sector and adults, literature such as books or specialist articles in the cases of children, the public sector, SMEs, private sector organisations and others; use of other forms of online presence – interactive or otherwise, advertisements on public transport and also partnering with trusted organisations having a wide customer or membership base so as to reach more effectively the target audience – particularly in the case of adults and SMEs.

It could be noted, through the responses by Member States, that the most widely used communication channels are those that involve mutual interaction with the audience. Definitely such observation would need to be seen further in light of other promotional aspects that are specific to the audience being targeted.

4.2.3 The Cyber security threat landscape focus of the Campaign

- **The majority of respondents identified ransomware and the compromise of sensitive data (75%) as the top challenges that their campaign is addressing. This is closely followed by malware, social engineering, spamming, phishing, online frauds and scams (70%), cyber bullying and online account hacking (60%) and identity theft (50%).** At a significantly lower extent are sextortion and incitement of hatred & violence (35%), compromise of services (30%), mal-advertising and others (25%).

- It has been acknowledged by some Member States that the cyber threat landscape is continuously evolving and thus the strategy would need to be aligned accordingly. However, **an equal majority of respondents still identify ransomware, compromise of sensitive data, malware, social engineering, spamming and phishing and online frauds as challenges to be tackled.** They are followed, to a lesser extent by cases of cyberbullying and online account hacking (50%). The decrease in the latter is however offset by a **significant increase in respondents intending to focus their awareness on identity theft (70%), compromise of services (50%), mal-advertising and incitement of hatred & violence (45%) and sextortion (40%).**

- Some respondent Member States also project future focus on website vulnerabilities, child pornography, cyberespionage, Internet of Things (IoT) security and hacktivism.

Focus of respondent Member States appears to be, among others, in the areas of ransomware and the compromise of sensitive data, which can leave serious consequences to victims. It also indicates an increasing concern on incitement of hatred & violence, sextortion, identity theft, attacks on online services, mal-advertising, all of which may significantly lower online trust, apart from security in online services and transactions.

4.2.4 The Areas of focus

- **Protection is the focus area mostly identified by respondents in their awareness campaign (75%) and it is likely to remain in the foreseeable future (80%)**. Identification and authentication also features high among 60% of Member States, indicating it as an area of focus, although the thrust towards it is envisaged to decline down to 45%. A slight decline is also noted with respect to authorisation from 35% to 25% of Member States. The **focus on confidentiality and on detection is however expected to be retained** at a rank of 50% and 45% of Member States respectively.

- An **overall future increase in focus is also expected on data integrity (from 25%, at present to 40%), response (from 40% at present, to 50%) and significantly from 10% to 30% of Member States, with respect to recovery.** Particular reference has also been made towards a future focus on prevention and deterrence.

Whilst protection from cyber grievances appears to be the most important measure to be tackled among respondent Member States at all times, there appears to be a future shift towards focusing on instances where attacks do occur and wherefore the victims would need to be aware of how to react in such situations. This could possibly reflect an evolving maturity in the awareness campaigning of Member States.

4.3 Evaluation of the National Awareness Campaign

4.3.1 Key performance indicators

- **35% of the respondent Member States stated that they do not apply any form of KPI (key performance indicators) measures; whilst 50% of the respondent Member States refer to their use. In the latter case, whilst half of the respondents refer to the application of KPIs of a quantitative nature, the remaining half refer to a hybrid of quantitative and qualitative measures.**

- Amongst the KPIs applied are: feedback received from participants in events, number of participants or partners in events, number of events and activities delivered, infographics, reach of communication channels, use of statistical tools to track performance of online presences, as well as regular research to assess the level of understanding of cyber security awareness on a national level.

Evaluation of cyber awareness campaign performance through metrics only appears to be conducted by half of the respondent Member States. Furthermore, there does not appear to be standard KPIs among respondent Member States as a metric to measure the outreach and effectiveness of a cyber awareness campaign, although a number of respondents apply forms of indicators that could help in assessing performance effectively.

4.3.2 Achievements

- The following achievements are registered by Member States during the conduct of their campaign:
  - A noted increase in cyber awareness among audiences, following awareness related activities;
  - Adoption of articulated and disseminated guidelines by organisations for their own use;
  - Increase in incident reporting, level of questions asked and related discussions in social media;
  - Increased public -private interaction for awareness-raising activities;
  - Marketing related awards.

As noted by respondent Member States, effective cyber awareness campaigns call for incentives as well as collaboration between the public and private sectors. A noted increase in interest, knowledge and reporting of online grievances by the target audiences are also seen as achievements in the awareness process.

4.3.3 Lessons learnt

- A number of respondent Member States (60%) also shared their lessons learnt to date in the course of their campaign, as noted below:
    - **Emphasising and addressing** the cyber related needs, requirements, challenges and concerns of all target audiences;
    - **Addressing all aspects of cybersecurity albeit focussing on small amounts of cyber related behaviours at a time** to ensure better understanding;
    - Opportunities for **behavioural research studies in cyberspace for better preparedness;**
    - **Trust building-enabled with long-term activities and the application of interactive and hands-on activities** with the intended audience contributing to the success of an effective adoption of a cybersecurity aware culture as especially highlighted in the case of students;
    - **Pragmatism by addressing cybersecurity issues that are topical** to a specific audience or that **impact upon their personal needs; with clear cut measures;**
    - **Cooperation and coordination of effort between all national stakeholders;**
    - Careful **consideration of presentation of content, including use of visual imaging**, **easily understood language, positive messaging** and **appropriateness of the communication channel used** for a specifically targeted audience;
    - Availability of the **appropriate human and financial resources;**
    - **Empowerment of the target audience** to take action;
    - **Partnering with organisations having an established client base as a potential effective way to ensure reachability and credibility to specific target audiences**. Such **relationships take time and a pragmatic approach, starting with mutual collaboration on small tasks,** may help attain success.

It is noted that the features identified by the respondent Member States with respect to lessons learnt, reflect a drive towards a successful paradigm shift that needs to be attained so as to ensure a cybersecurity sensitive and responsive culture. Such drive is marked with the need to ensure pragmatism, collaboration and trust among all stakeholders as well as a clear but positive message always whilst indicating the potential pitfalls and dangers.

4.3 Coordination with EU institutions and agencies

- 60% of the respondent Member States indicated a form of support received from EU bodies with the majority of attributed ENISA, particularly in consultations and coordination in European Cyber Security Month (ECSM) events on a domestic level.

- European Commission supported activities such as The Safer Internet Day (30%), DG CONNECT and DG GROW (5%); Other EU bodies referred to by respondent Member States include Europol, particularly in terms of content required for the campaign (20%); INSAFE (10%) and Innovation and Networks Executive Agency and the Internal Security Fund for the EU – for co-financing (5%).

- Most of the respondents got to know of such support through the EU bodies themselves (67%), with the rest attributing such information through other Member States or through research.

The findings indicate a good number of respondent Member States availing of support at EU level - mainly of an organisational nature - on short term European cyber events and to a lower extent on the use of any related material provided at EU level. Even lower reference is made to any co-financing options as a form of support at an EU level to Member States on cybersecurity awareness. Promotion of such support is reached mainly through EU institutions although it appears that this is not the case in all instances.

4.4 Issues and Expectations

4.4.1 Prevalence of cyber incidents

- Respondents, in their overall majority, did not prioritise where most cybersecurity incidents occur among the target audience, but only marked them as victims of cyber-attacks reported. Some acknowledged the difficulty in prioritising and attributing it to various actors focussing only on specific sectors and the overall lack of visibility. Of the 2 Member States that indeed prioritised, both gave third placing to SMEs and first to the Public sector in one case and to the citizens in the other.

- Most respondent Member States identified citizens as victims (55%), followed by the public sector (50%) and SMEs (45%). At a significantly lower level were other private sector organisations (20%) and others (10%).

- In both cases, **excluding the public sector, citizens and SMEs appear to be the most likely victims of cyber-attacks reported on a national level.**

Based upon the responses of Member States, it appears that citizens and SMEs, apart from the public sector are among the highest incidence of cyber-attack victims.. This trend may reflect, apart from sensitivity of information and processes dealt with, the vulnerability and need for further preparedness, enabled through awareness amongst such audiences.

4.4.2 Issues

A lack of human and financial resource availability was the issue highlighted by 30% of respondent Member States. In one case, such issue was claimed to attribute to a lack of support from other stakeholders. Other issues, some of which are related to the above mentioned one, include:

- The **need for further research and study** particularly on how people react when confronted by a cybersecurity related problem;

- The need for **synchronisation of activities with those held by EU bodies** as well as **sharing and exchange of best practice** on awareness raising;

- The **need for regular staff training** to ensure currency of expertise within a highly dynamic cyber landscape;

- A **piecemeal rather than a unified approach adopted by various stakeholders** involved in the campaign, possibly leading to conflicting messages to the intended recipient. In one case reference has been made to individuals and SMEs who may find it difficult to prioritise which key behaviours to adapt;

- **Maintaining a balance between conveying information about incidents and threats and minimising the level of fear** could lead to lower trust in the use of online services. The need to find support on an international level such as through campaigns organised on an EU level was also highlighted in one case as a means to meet the related cyber challenges on a national scale.

The issues highlighted by respondent Member States indicate the need for a concerted national effort that calls for ongoing harnessing and availability of financial and human resources that could even be supported at a EU level.

4.4.3 Plans

55% of respondent Member States indicated their mode of conducting cyber awareness through a more focused approach such as on public administration, critical infrastructure providers or SMEs. Among the plans identified were:

- **Training** to public sector employees, to the general public as well as to those occupying managerial roles (20%);

- **The development of an e-learning platform** that focusses on the public administration or on a wider audience (20%);

- Focusing on the Education Sector through the **development of content, modules, courses, gamification** that doesn't necessarily involve students but parents and educators as well (20%);

- **More active engagement with local stakeholders as a means to reach a wider national audience (15%) and membership with international cyber related initiatives** to support their campaign;

- **Organisation of national cybersecurity events in conjunction with EU level cyber activities** such as the ECSM (15%);

- **Promoting a business case for long-term investment in cybersecurity** as a means of ensuring a sustainable business strategy (5%).

The plans indicate ways of reaching out to specific and/or various economic and social sectors within Member States, through various interactive means – online or otherwise - whilst seeking to attain further collaboration with national and EU stakeholders.

4.4.4 Desired expectations from EU bodies

65% of respondent Member States cited the **need for support to their national awareness campaigns through funding mechanisms** followed by more **guidance at an EU level** (45%). The responses indicate that cybersecurity awareness campaigning is still a new activity where development of ideas, expert advice on the conduct and evaluation of performance of the campaigns and pooling of resources and sharing of best practice is welcomed by Member States. In this respect the implementation for such a need from EU level was proposed as follows:

- **The establishment of regular meetings with other Member States** as a means to share and exchange best practice, ideas, advice, experiences;
- **Stimulate the use of the EU Safer Internet Programme**, which apart from co-financing provided MS with strategic guidance as well as an expert knowledge base;
- **Strengthening the coordinating role of ENISA and Europol in awareness programmes**, including the provision of more funds to such bodies for provision of published content to Member States;
- **Provision of standard awareness deliverables to Member States** e.g. TV, radio, published content, as a result of projects developed at EU level;
- **Clarity and support for an awareness campaign that targets citizens and SMEs**.

25% of respondent Member states also called for the need for a dedicated legislation to ensure the implementation of a coordinated national awareness campaigns across the EU.

Awareness campaigning on cybersecurity is still a new activity that calls for substantial financial and human resource involvement where every Member State can mutually learn and develop further on ideas, good practices, advice and experiences shared. In this regard, as indicated by the responses, the EU needs to take a leading role in finding ways of supporting Member States through funding mechanisms, in reconsidering and/or developing related programmes, in strengthening further its coordinating role, including that provided by its existing bodies such as ENISA and Europol, and potentially in exploring - along with Member States - the possibility of having a dedicated EU legislation.

5. Way Forward

5.1 Preliminary Conclusions

The uncertainty prevailing within the cyber environment due to the rapid evolvement of cyber threats, coupled with the complexity of the issues, calls for a high degree of awareness within Member States as one of the key pillars of security and trust within cyberspace.

The outcome of the questionnaire highlights a strong need among Member States to focus on cyber awareness not solely within the public sector or large organisations, but also on society - children, adolescents, adults, elderly and vulnerable groups and minority groups - as well as SMEs as a crucial economic sector. The key challenges faced by Member States include also the need to:

- Have the necessary resources, as cybersecurity is an ongoing concern that merits continuous awareness, training, research, study and monitoring;

- Ensure a national coordinated approach amongst all stakeholders so as to establish a comprehensive and consistent nation-wide cyber awareness coverage is attained and maintained;

- Exchange, share and have access to experience, with a view that cyber awareness is a pan-European concern;

- Conduct an awareness campaign that increasingly covers the citizens, including vulnerable and minority groups; SMEs, apart from the public sector; and that covers not only protection but increasingly the ways to respond effectively in case of grievances experienced online.

5.2 Discussion Points

Furthermore, the replies of the questionnaire indicate that a wider level of ongoing mutual support and collaboration should help further Member States in their cyber awareness efforts. Hence, the Presidency would like to address and seek delegations' views on the following points:

- How to actively promote and encourage an ongoing nation-wide cyber security awareness in Member States that considers both on-line protection as well as preparedness of all EU citizens and SMEs.

- Should the possibility of a dedicated legislation aiming at establishing a coordinated and strategic approach to cyber awareness across the EU be further explored?

- What national and/or EU channels are there or could be available to fund or to support Member States in their national cyber awareness activities and campaigns?

- How to extend further, and promote activities of EU bodies such as ENISA, Europol and others, within a cooperation framework, so as to support Member States on an ongoing basis throughout the year in content material catering for various forms of intended audiences, knowledge, expertise, advice, participation and collaboration.

- How to support, in close cooperation with Member States and all relevant EU bodies, the establishment of a cybersecurity training platform[1].

- How to further promote the research on behaviour in cyberspace, so as to ensure better preparedness of individuals and organisations on cyber-related grievances experienced.

[1] As highlighted in Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a competitive and innovative cybersecurity industry (doc. 14540/16)

5.3 Next Steps

Further to the discussion on the points outlined above, the Presidency proposes to outline the key features of a common approach towards the consolidation of a pan-European cyber awareness in a set of dedicated Council Conclusions. A draft would be presented at the next meeting of the working party if this approach is shared by Member States.

In addition to that the Presidency would also encourage the continuous exchange of ideas, good practices and experiences among the Member States in the framework of the Horizontal Working Party on Cyber Issues.

www.parlament.gv.at