IGF 2016 Workshop Report

Session Title	WS113: What makes cybersecurity awareness campaigns effective?
Date	8/12/2016
Time	15:00-16:30
Session Organizer	Kerry-Ann Barrett (Organization of American States) Carolin Weisser (Global Cyber Security Capacity Centre, University of Oxford) Carolyn Nguyen (Microsoft)
Chair/Moderator	Carolin Weisser
Rapporteur/Notetaker	Dr Maria Bada/Carolin Weisser
List of Speakers and their institutional affiliations	Dr Maria Bada (Global Cyber Security Capacity Centre, University of Oxford) Jorge Bejarano (Ministry for ICT Colombia) Michael Kaiser (National Cyber Security Alliance) Barbara Marchiori (Organization of American States)
Key Issues raised (1 sentence per issue):	• Risk perception in relation to different cultural environments (e.g. in an individualistic vs. collectivist society), socio-economic situation and demographics (e.g. women, elderly, children); and how risk perception influences compliance with policies and guidelines for cybersecurity. • The reasons why cybersecurity awareness campaigns often have little impact or even fail to change behaviour. • Description of good practices for different target groups and the stakeholders that need to be involved in the planning and the implementation process of awareness campaigns. • The influencing strategies and best implementation approaches to change people's attitudes and behaviours. Behaviour change can lead to creation of a cybersecurity culture which is important for a nation to secure its citizens.

	• The issues which need to be considered when adapting campaigns to other cultural and organisational settings, and different target groups. • The existing metrics to measure the impact of cybersecurity awareness campaigns and possible metrics that could be considered for evaluating their effectiveness.
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	Presentations focused on international and national best practices describing the key elements that characterise them as successful initiatives. The key elements presented are: simple advice provided by the correct messenger, targeted, linked to national goals, and taking into consideration cultural differences. 1. Michael Kaiser described the National Cyber Security Alliance and core campaigns in the U.S. such as Stay Safe Online; Data Privacy Day; and the National Cyber Security Awareness Month. 2. Barbara Marchiori described the Cybersecurity Awareness Campaign Toolkit, developed by the Organization of American States. It is designed to provide governments or organisations guidance and resources for developing a cybersecurity awareness campaign that educates citizens about safe attitudes and behaviours when using the internet, and helps build a national culture of cybersecurity. 3. Jorge Fernando Bejarano described initiatives such as the campaign ‘‘We Protect You’’ in Colombia and ‘‘Cyber Voluntarily’’ in Spain which targets adults and children. 4. Maria Bada described the current national campaign ‘‘CyberAware’’, a UK government initiative which aims to create awareness in organisations and the general public; the South African Cyber Security Academic Alliance (SACSAA); and the campaign CyberSafe in Malaysia, a government initiative tasked with educating and enhancing the awareness of the general public on the risks people face online.
Please describe the Discussions that took place during the workshop session: (3 paragraphs)	During the workshop the speakers discussed how changing behaviour online requires more than providing information about risks online. The panel agreed that people must be able to understand the advice provided, and be able and motivated to apply the recommendations. Often people are

	not aware of the associated risks or do not fully understand what the 'correct' behaviour may be. The discussion evolved and focused on the factors which influence human behaviour and trigger behavioural change such as: (1) the messenger who communicates information; (2) the messages used; (3) the incentives provided; and (4) culture. Furthermore, different influence strategies (e.g. fear invocations), used in existing awareness campaigns and their effectiveness in changing behaviour were discussed. Speakers debated which factors define best practices. The key elements identified as important were resources that will ensure the sustainability of a campaign, being targeted and linked to the national cybersecurity strategy, ensuring multi-stakeholder involvement not only during the planning of a campaign but, in particular, during its implementation. The discussion led to a review of existing metrics for evaluating the effectiveness of cybersecurity awareness efforts. Quantitative data can be measured by collecting information such as the number of visits to a website; time spent on a webpage; number of followers on social media. Qualitative data measure perceptions, attitudes, and the sense of trust in the Internet. The presenters emphasized the difficulty of collecting qualitative data at large scale or at a national level.
Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)	The discussion during the workshop led to suggestions regarding the way forward. Presenters advised that not too much importance should be given to the main message of a campaign but to the sub-messages providing advice on specific issues. These messages are the ones that users will have to remember. Also, the key factors that can lead to a campaign's success were discussed and agreed upon. Factors such as simple advice provided by the correct messenger, targeted, linked to national goals, taking into consideration cultural differences were identified as crucial when planning a campaign. Reporting mechanisms were also identified as important for the effectiveness of awareness campaigns. A key takeaway in this regard is that a more coordinated

	effort is needed from both public and private sector so that users have a clear understanding of who to report to. Another suggestion was related to parenting and the fact that children avoid speaking to their parents but tend to speak to their peers when they have a negative experience online. It is suggested that more coordinated efforts are necessary in schools in order to raise awareness and educate not only children but also parents. Lastly, the need for defined large scale metrics was identified in order to help cybersecurity awareness efforts be evaluated and assessed. A good way, which proved to be successful for approaching this challenge also in other fields and disciplines is marketing analysis and testing messages through consumer research approaches.