Working Group D: Cyber Security Culture and Skills

White Paper: Task Force on Cyber Security Awareness

Date: 21st March 2019

Editors: Laura Bate, Deborah Housen-Couriel, Tamar Berenblum, Marjo Baayen, and Folake Olagunju Oyelola.

Background

Malicious behaviour online - whether theft of personal property, compromise of sensitive information, cyber bulling, harassment, or real-world crime enabled by online activity - is increasingly costly and notoriously difficult to stop. Wide-scale protection against such activities relies, in part, on cultivating awareness of cyber security basics among entire populations, and the development pathways to educate future cyber security experts. In line with this, one of the prioritised themes of the Global Forum on Cyber Expertise (GFCE's) Delhi Communiqué is the development of cyber security culture and skills.

I. Data Collection Effort

Within Working Group D's larger theme of cyber security and skills, two task forces undertook a project to learn more about (i) cyber security awareness programmes (CA) and (ii) programmes for the development of professional education and training (PET) in cyber security. This paper expands on the first of these two subjects.

The goal of this work is to promote comprehensive awareness across all stakeholders' subject to cyber-related threats and vulnerabilities, and empower them with the knowledge, skills and sense of shared responsibility to practice safe and informed behaviours i.e. such as in the use of information communication technologies (ICTs).

As governments, private sector entities and other key ICT stakeholders are developing their cyber security strategies, now is the ideal time for the GFCE to pool insight and coordinate on resources/best practice. To enable this sharing process, the GFCE's Working Group D gathered information on both CA and PET programmes in operation.

The working group conducted the information gathering effort via a survey (annex 1) with fourteen questions about specific aspects of the programmes. The

GFCE secretariat and working group members distributed the survey to GFCE members, partners, and their wider networks. The survey was conducted across the public and private sectors to see how stakeholders are raising cyber awareness and incorporating it into daily business.

The survey presented no standard definition of cyber awareness; however, its initial results concluded that awareness programmes should encompass a change in attitude and behaviour, and the acquisition of knowledge, that will safeguard the use of valuable data and information towards the end of increasing cyber awareness on a broad scale.

Sections II and III of this paper will present the results of that process and recommend ways that cyber awareness can help promote a positive change/impact in tackling cyber security issues.

II. Results and Analysis

Of the 41 initiatives received covering both cyber security awareness and cyber security professional education and training programmes (see Annex 2):

- 15[1] initiatives focused specifically on cyber security awareness education and training
- 4[2] initiatives cut across both cyber security awareness and professional education and training
- Fewer programmes were reported in Asia and South America;
- More government-sponsored than Non-Government Organisations (NGO) -sponsored activities were reported
- More activities with a national focus, rather than with a regional focus, were reported

[1] U.S. Department of Homeland Security's (DHS) STOP. THINK. CONNECT.™ Campaign, STOP aux violences faites aux femmes sur Internet" - Campagne de sensibilisation sur les violences faites aux femmes sur Internet, ICT for Peace Foundation, Les Samedis du Numérique, The Gambia Cyber Security Alliance (GCSA), National Cybersecurity Career Awareness Week, Cyber Defence East Africa (CDEA) conference, The Cyber Surakshit Bharat Initiative, US CERT National Cyber Alliance, ENISA's European Cyber Security Month, US National Cyber Security Alliance (NCSA) – StaySafeOnline, AlertAfrica, Cyber Aware, Cyber Readiness Institute, Safe Internet week and Isoc-IL – Netica.

[2] CyberPatriot, National Youth Cyber Education Program, Collegiate Cyber Defense Competition, Technology Update Workshops; Internet Safety Campaign for youths, Senior Citizens and House Wives and *Magshimim* -Rashi Foundation.

Of the results received, *twenty-two* efforts focused on cyber security awareness and training, which includes the *four* initiatives that cut across both cyber security awareness and professional education and training. *Twelve* of these programmes were government-driven efforts in cyber security awareness, and ten were from NGOs.[3] *Six* were in Africa, *nine* were in North America, *three* were in the Middle East, *two* were in Europe, *one* was in Asia, and *one* was global in nature.

Variance in focus: The programmes reported varied significantly in the core issue they were designed to address. Many programmes focused on developing habits that encourage personal safety and security for entire populations, while others campaigns were targeted at vulnerable populations like women and children, who experience specific types of harassment and threats online. Other programmes were not focused on individuals at all, but rather were designed to connect businesses of all sizes with the resources needed to secure their operations.

In some cases, the mandates for awareness programmes expanded beyond cultivating good internet usage habits. For example, some programmes have the secondary goal of engaging youth in the study of cyber security in order to encourage them to consider cyber security careers. Meanwhile, some programmes focused on enabling internet users to report cybercrime rather than—or in addition to—encouraging good cyber security hygiene.

Variance in approach: In addition to the issue they address, programmes varied in their underlying theory of change. While most programmes focused on educating the general public—relying on 'bottom-up" style change, others engaged with high-level leaders like policymakers and chief information officers, demonstrating a "top-down" approach to building greater cyber security awareness. One programme even connected with media (in addition to other audiences) in an attempt to educate influencers.

Commonalities between Programmes: Despite these variances, the programmes all shared core similarities. All were designed for scale. Even those that started with a small group of leaders are ultimately targeted at changing behaviour among a wide population. Another similarity is that many, although not all, reported

[3] In some cases, NGOs and governments were operating in partnership, so not all cases exhibit a clear delineation between NGO and government.

resource constraints as a barrier to expansion. A lack of budget, time, and commitment were reported in hindering the growth or continuance of many programmes. Perhaps in response to this, many programmes also exhibited reliance on partnerships between various combinations of NGOs, government entities, and private companies.

III. Recommendations

There is no standardised formula for a cyber-security awareness programme that will suit all global contexts. Effective programmes will and must adapt to fit local systems of education, economic circumstances, and stakeholder ecosystems. Nevertheless, the survey results do point to recommendations both for the GFCE as an organisation and for GFCE members that may be considering or in the process of developing domestic cyber security awareness programmes.

Based on the findings of this survey, the task force recommends that the GFCE:

- Seek opportunities to further expand the data set, as the survey data is likely subject to some sampling bias. That is to say, because GFCE members, the task force, and the secretariat were the primary mechanism for distributing the survey, programmes and regions with which those members are connected are likely to be more thoroughly represented than other regions.
- Develop metrics for evaluating effectiveness of campaigns. It is very useful to see the range of possibilities for emerging programs, but a better understanding of which are effective and under what circumstances would enable dedicating limited resources on the campaigns that have a history of greatest effectiveness.
- Promote and implement initiatives that work regardless of the jurisdictional environment (organisation, country, region or global) and are scalable.

Based on the findings of this survey, the task force recommends that GFCE Members:

- Utilise (i) a multi-stakeholder approach in the development of future efforts in cyber security awareness and (ii) ongoing involvement to encourage sustainability in future efforts.

- Promote the use of local content in the dissemination of information. Awareness campaigns that resonate with the local population will gain access to a larger audience through contextualisation.
- Consider the range of purposes, platforms, and audiences for awareness campaigns and tailor campaigns to specific needs.
- Encourage key leader engagement and commitment to ensure awareness campaigns are visible and impactful.

As a final point recommendation to both the GFCE and members, information sharing amongst countries belonging to the same regional blocs/communities will continue to be a critical mechanism for building greater awareness and education on cyber security globally. The effort described in this paper has been a first step, and the task force encourages future work of this kind.

Annexes

1. Survey
2. Spreadsheet of initiatives