
Of the gathered initiatives by the GFCE, 20 initiatives were on professional training and development. Many initiatives were government-sponsored, on public-private partnerships, and had a regional focus rather than a national focus.

The recommendations of the white paper were to (1) broaden the reach of the survey, and to (2) establish a means of measuring program effectiveness.

Based on the initiatives, it was apparent that there is:

- No shared taxonomy around the cyber security workforce
- A cyber security skills shortage, and
- A lack of differentiation between traditional and multidisciplinary cyber security professional training and development.

2. Presentation on initiatives and written report - Ian Wallace (New America)

We would like to thank Laura Bate (New America) for contributing to the Task Force white paper. Ian Wallace presented the outcomes and policy guidance on her behalf.

Based on the outcomes, it is important to define the key elements that are needed for successful initiatives. These include the needs, resources, research tools and collaborators. Furthermore, there is a need for the GFCE to measure the effectiveness of initiatives, to broaden the mapping exercise, and to keep changing technology in mind. Furthermore, connecting new initiatives to a community of practice remains important for both the GFCE as for national governments.

Report: ‘New Ways To Bring Women Into And Up Through Cybersecurity Careers’ - Laura Bate (New America)

Ian Wallace presented this report, co-written by Laura Bate (New America), on women in the workforce. The project consists of the convening of experts and written resources, with the goal of creating implementable strategies to bring women into and up through cyber security careers.

3. Presentation of ‘Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions’ – Tommaso de Zan (University of Oxford)

Tommaso de Zan’s report was presented to the Working Group members. It highlights the cyber security skills shortage in both entry level opportunities as well as professional experience, and focuses on public policy interventions. The results and analysis fit well in the overall discussions of the Task Force.
4. Presentation Palo Alto Networks – Dan Myers

Dan Myers, on behalf of Palo Alto Networks, presented three initiatives that are focused on the cyber security skills gap that exists around the world.

1. Cybersecurity Academy: a free program that equips students with next-generation cybersecurity knowledge and skills. The curriculum maps learning objectives to the U.S. NIST/NICE framework and cybersecurity work roles.
2. Cybersecurity Specialization (Coursera): a career-focused 5-course curriculum made to prepare for entry-level careers in cybersecurity.
3. NCWIT Partnership to Increase Women in Cybersecurity: an initiative that helps women focus on careers in cybersecurity. This is done by training school counselors around the US to advise their students on cybersecurity careers.

5. Presentation World Economic Forum – Francesca Bosco

Francesca Bosco discussed PPP cooperation on cyber training initiatives within the WEF Centre for Cybersecurity. The WEF Centre for Cybersecurity focuses on two main aspects: building and developing human capital, and driving diversity and inclusion.

There are three areas to work on:

1. Building a global network of sustainable cyber security hubs
2. The need for a definition of roles and skills
3. Driving diversity and inclusion

6. Presentation Futureskills (NASSCOM initiative) – Vinayak Godse

Futureskills is a platform-based approach on the Education & Training program. It builds on the development of digital talent in a multi-stakeholder response. The Futureskills platform contributes to the GFCE members in its leverage, contribution and collaboration.

ACTIONS

- Expand the initiative dataset and identify the needs of the initiatives
- Finalize the white paper, based on feedback
  - For any feedback, kindly send an email to contact@thegfce.org
- Build on the internationalization of the NICE Framework as a Workshop idea during the Annual Meeting 2019

Save the date

- GFCE Working Group D session during Tel Aviv Cyberweek – Thursday June 27 2019
  - Please find the registration link here: https://cyberweek.tau.ac.il/2019/
- GFCE Annual Meeting 2019 – in the week of October 7th 2019
Report GFCE Working Group D meeting – Task Force Awareness

GFCE Working Group Meetings 2019 – April 4th 09:00 – 10:30, The Hague
Task Force Leader: Folake Olagunju Oyelola

1. White paper on Cyber Security Awareness – Folake Olagunju Oyelola (Task Force Lead / ECOWAS)

We would like to thank Laura Bate for contributing to the Task Force white paper. Of the gathered initiatives by the GFCE, 18 were focused on cyber security awareness. Many initiatives were government-sponsored, on public-private partnerships, and had a regional rather than a national focus.

The recommendations of the white paper for the GFCE were:

- To expand the dataset
- To develop metrics for evaluating effectiveness of campaigns
- Promote and implement working initiatives that are scalable

Furthermore, recommendations for GFCE members were the following:

- Use a multi-stakeholder approach
- Localize specific content and range of purpose so to tailor to specific needs
- Key leader engagement is essential for awareness initiatives

2. Discussion outcomes

- Most GFCE Members/Partners have methods in which cyber security awareness is promoted, but there is a difference in focus and priority
- There is no clear categorization of cyber security awareness in terms of stakeholders, behavior, and areas where to build awareness. Suggestions have been made to create a clear matrix
- Metrics on the impact of awareness campaigns are of importance
- The Cyber Security Awareness Month in October is a target of opportunity in which GFCE Members/Partners can collectively commit to cyber security awareness raising

ACTIONS

- Expand the initiative dataset and identify the needs of the initiatives
- Develop metrics and categorization for evaluating effectiveness of awareness campaigns
- Finalize the white paper, based on feedback
  - For any feedback, kindly send an email to contact@thegfce.org
- Coordinate a Working Group D wide campaign for cyber security awareness during the Cyber Awareness Month in October

Save the date

- Working Group D meeting during Cyber Week in Tel Aviv, Israel – Thursday June 27 2019
  - Please find the registration link here: https://cyberweek.tau.ac.il/2019/
- GFCE Annual Meeting 2019 – In the week of October 7th 2019
Report GFCE Working Group D meeting

GFCE Working Group Meetings 2019 – April 4th 16:45 – 18:15, The Hague
Chair WG D: Deborah Housen-Couriel

1. Insights from the Task Force meetings

Based on the Task Force Education & Training and the Task Force Awareness meetings, the following insights have been gathered:

- The dataset on initiatives needs to be expanded. The collection of initiatives needs to be continued, and the needs and priorities need to be defined
- The two white papers are to be finalized, based on the given feedback
- Two workshops need to be created for the GFCE Annual Meeting in October 2019

2. Next steps towards the Annual Meeting

- Provide feedback on the white papers (kindly send this to contact@thegfce.org), after which these will be finalized
- Workshops GFCE Annual Meeting 2019:
  - Task Force Education and Training: idea of a NICE framework workshop during the Annual Meeting
  - Task Force Awareness: coordination of an awareness campaign during Cyber Awareness Month in October + a workshop during the Annual Meeting (TBD)
- Provide a list of conferences, meetings, and get-togethers of each Working Group Member/Partner

Save the date

- Working Group D meeting during Cyber Week in Tel Aviv, Israel – June 27 2019
  - Please find the registration link here: https://cyberweek.tau.ac.il/2019/
- GFCE Annual Meeting 2019 – In the week of October 7th 2019
- NICE Conference in Phoenix, Arizona – November 18 - 20 2019
- NICE K12 Cybersecurity Education Conference in Garden Grove, California - December 9-10 2019
<table>
<thead>
<tr>
<th>Working Group Agenda Elements</th>
<th>GFCE Working Group D</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. Mapping</strong></td>
<td><strong>Achievements until April 2019</strong></td>
</tr>
<tr>
<td>Overview on actors, projects, events on respective theme and topics.</td>
<td>• Working Group D split in two Task Forces</td>
</tr>
<tr>
<td></td>
<td>• Mapping of initiatives on Education &amp; Training and Awareness</td>
</tr>
<tr>
<td></td>
<td>o Distribution of questionnaire to WG Members/Partners</td>
</tr>
<tr>
<td></td>
<td>o Mapped data for both Task Forces</td>
</tr>
<tr>
<td></td>
<td>o Total of 40 initiatives mapped, about half-and-half for each Task Force with some overlap</td>
</tr>
<tr>
<td></td>
<td>• Expand the dataset of initiatives via the GFCE questionnaire</td>
</tr>
<tr>
<td></td>
<td>• Identify the needs and priorities for the initiatives that the GFCE and Members/Partners need to focus on for cyber capacity building</td>
</tr>
<tr>
<td></td>
<td>• Promote and implement working initiatives that are scalable, while taking into account cultural relevance</td>
</tr>
<tr>
<td></td>
<td>• Explore how metrics could be developed for evaluating effectiveness of initiatives</td>
</tr>
<tr>
<td><strong>II. Products</strong></td>
<td>Two draft white papers, mapping the gathered initiatives along with recommendations for the GFCE and its Members/Partners</td>
</tr>
<tr>
<td>Existing products, lessons learned and (new) GFCE products.</td>
<td>o Cyber Security Education &amp; Training</td>
</tr>
<tr>
<td></td>
<td>o Cyber Security Awareness</td>
</tr>
<tr>
<td></td>
<td>• Working Group joint learning sessions on scalability of the NICE Cybersecurity Workforce Framework and adaptability to other countries</td>
</tr>
<tr>
<td><strong>III. Clearing House</strong></td>
<td>Discussion on what the Working Group and its members have to offer, on the basis of the initiative database</td>
</tr>
<tr>
<td>Match needs with knowledge/expertise/resources.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use available data from the expanded dataset to identify actors that might need assistance</td>
</tr>
<tr>
<td></td>
<td>Create a document outlining the needs and interests of involved stakeholders</td>
</tr>
<tr>
<td></td>
<td>Proactively help GFCE members find partners that support their cyber capacity building through the GFCE clearing house mechanism</td>
</tr>
<tr>
<td></td>
<td>Explore ways to support the clearinghouse with ongoing research on initiatives and their impact</td>
</tr>
</tbody>
</table>