

Why Do National Cybersecurity Awareness Programmes Often Fail?

Eva NAGYFEJEO¹, Basie Von SOLMS²

¹ Global Cyber Security Capacity Centre, University of Oxford, UK

eva.nagyfejeo@cs.ox.ac.uk

² Academy for Computer Science and Software Engineering, University of Johannesburg, South Africa

basievs@uj.ac.za

Abstract

Nowadays, many cyber users do not understand how to protect themselves and their information within cyber space. One reason is that cyber users are unaware of possible cyber risks and threats that may occur within cyber space. The second reason is that citizens, businesses and users within the public sector may be aware of relevant cyber risks but do not really understand the seriousness of such risks and the consequences if they do realise. Therefore, cybersecurity awareness campaigns are an integral part of improving cybersecurity awareness. Based on in-country reviews conducted as part of the Global Cybersecurity Capacity Centre (GCSCC) programme, we observed that the campaigns to raise cybersecurity awareness throughout the country are often led by different 'owners' without co-ordination and adequate resources therefore creating fragmentation in the national cybersecurity awareness raising programme. This paper suggests that the development of a coordinated and coherent national cybersecurity awareness program is critical for building a basic level of awareness at the national level. We will examine the requirements needed to develop a coordinated national awareness raising programme by reviewing the existing literature, best practice approaches and the role of different stakeholders such as the government, private sector and civil society. We will draw conclusions on the main obstacles to ensure overall coherence between the actions of stakeholders and the efforts countries should prioritise in order to increase awareness of cyber risks at the national level.

Index terms: cybersecurity, awareness raising, national frameworks

References:

- [1]. Gutwin, C., Greenberg, S. A Descriptive Framework of Workspace Awareness for Real-Time Groupware. *Computer Supported Cooperative Work (CSCW)* 11, 411–446 (2002). <https://doi.org/10.1023/A:1021271517844>.
- [2]. Endsley, M. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, vol. 37, no. 1, pp. 32–64. (1995).

- [3]. German Ministry for Economic Co-operation and Development (BMZ) and the OECD De-velopment Centre. Global Education, Public Awareness- Raising and Campaigning on Development Issues, (2007) <https://www.oecd.org/development/pgd/38405962.pdf>.
- [4]. Sieber, U. Legal aspects of computer-related crime in the information society. University of Würzburg. COMCRIME - Study Prepared for the European Commission. (1998) <http://www.oas.org/juridico/english/COMCRIME%20Study.pdf>.
- [5]. Brenner, S. W. Cybercrime: criminal threats from cyberspace. Santa Barbara, CA: Praeger. (2010).
- [6]. Cybersecurity Tech Accord, Cybersecurity Awareness in the Commonwealth of Nations. (2020) <https://cybertechaccord.org/new-whitepaper-cybersecurity-awareness-in-the-com-monwealth-of-nations/>.
- [7]. de Bruijn, Hans, and Marijn Janssen. Building cybersecurity awareness: The need for evi-dence-based framing strategies. *Government Information Quarterly* 34, no. 1 (2017): 1-7.
- [8]. BitSight Report, The Secret to Creating a Cyber Risk-Aware Organization, <https://info.bitsight.com/the-secret-to-creating-a-cyber-risk-aware-organization-ebook>, last accessed 2020/06/24.
- [9]. Ibid.
- [10]. Global Cyber Security Capacity Centre, Cybersecurity capacity maturity model for nations (CMM): Revised edition, (2017) <https://cybilportal.org/tools/cybersecurity-capacity-ma-turity-model-for-nations-cmm-revised-edition/>.
- [11]. Lithuania, CMM report (2017) <https://www.nrdcs.lt/en/press-releases/lithuania-s-cyber-se-curity-capacity-are-we-cyber-ready-to-embrace-digital-era-/80>.
- [12]. Cyprus, CMM report (2017) http://www.ocecpr.org.cy/sites/default/files/cmm_cyprus_re-port_2017_final.pdf.
- [13]. North Macedonia, CMM report, (2018) https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf.
- [14]. Bosnia and Herzegovina, CMM report, (2018) http://mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=7650&langTag=bs-BA.
- [15]. Samoa, CMM report, (2018) <https://mcit.gov.ws/2019/04/03/cyber-security-capacity-re-view-2018/>.
- [16]. The Gambia, CMM report (2018) http://www.pura.gm/wp-content/uploads/2019/07/CMM-report_Gambia_2019.pdf.
- [17]. Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing national cybersecurity aware-ness in Africa: An empirical study. <https://www.repository.cam.ac.uk/bitstream/handle/1810/293742/Bada.et.al.pdf?sequence=3&isAllowed=y>.
- [18]. ITU. Measuring digital development. Facts and figures. (2019) <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>.
- [19]. UNESCO, Literacy Rates Continue to Rise from One Generation to the Next. Fact Sheet No. 45. (2017) <http://uis.unesco.org/sites/default/files/documents/fs45-literacy-rates-con-tinue-rise-generation-to-next-en-2017.pdf>.
- [20]. Hammergren, Linn. Political will, constituency building, and public support in rule of law programs. Center for Democracy and Governance Fax 202, 216-3232 (1998).

- [21]. Malena, C. (Ed.). From political won't to political will: Building support for participatory governance. Kumarian Press (2009).
- [22]. Brinkerhoff, D. W. Unpacking the concept of political will to confront corruption. U4 Brief. (2010).
- [23]. Kukutschka, R. M. B. Building political will: Topic guide (2016).
- [24]. GFCE, Report on the “Next steps Cybil – the CCB knowledge portal” Session. <https://thegfce.org/report-on-the-next-steps-cybil-the-ccb-knowledge-portal-session/>, last accessed 2020/05/16.
- [25]. Cybil, The Knowledge Portal for Cyber Capacity Building, <https://cybilportal.org/>, last accessed 2020/05/16.
- [26]. Get Safe Online, <https://www.getsafeonline.org/about-us/>, last accessed 2020/05/30.
- [27]. STOP. THINK. CONNECT. <https://www.stopthinkconnect.org/about> last accessed 2020/05/25.
- [28]. APWG. <https://thegfce.org/wp-content/uploads/2020/06/APWG-GFCE-V-Meeting-26-May-2020-Cyber-Security-Awareness-Campaigns.pdf>, last accessed 2020/05/30.
- [29]. GFCE. Report on the “Cyber Security Awareness Campaigns” Session. <https://thegfce.org/report-on-the-cyber-security-awareness-campaigns-session/>, last accessed 2020/05/29.