The Human Factor at the Center of a Cyber Security Culture

Sorana Campean
University of Luxembourg
sorana.campean.001@student.uni.lu

Abstract

With the issuing of the Resolution of 3 October 2017, on the fight against cybercrime, the European Parliament stressed once again that although the awareness about the risk posed by cybercrime has increased, "precautionary measures taken by individual users, public institutions and business, remain wholly inadequate, primarily due to lack of knowledge and resources". (own emphasis) Consequently, there is a vital need to enable the end-users with easy-to-understand technical terminology, so that the goal becomes to maximise to the greatest extent feasible the human-factor as the strong link at the end of an IP address. Considering also the recent guidelines issued by ENISA on this topic, the paper proposes a simple, easy-to-implement model of a cyber-savvy digital user, as a possible way to approach the overall (mis)interpretation of "the human as the weakest link of cyber security". Cyber security is often perceived as either belonging to the State or to organizations who can afford to implement it, or it is poorly put in place by small and medium size businesses due to financial constraints. This is, de facto, what is fuelling the perception of human as the weakest link of cyber security. Consequently, cyber security needs more recognition and increased visibility in the European Union. This paper proposes that the best manner to address this is via a human-centered approach to learning, trainings and awareness raising initiatives, tailored to suit all levels of digital literacy and regardless of demographics such as age or level of income.

Index terms: cyber security, end-users, digital skills education, cyber security awareness, privacy, EU legislation

References:

[1]. 'Cyber Security Intelligence Index', IBM 2014, retrieved from https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks.

[2]. e.g.von Gavrock, E. ; 'Here are the biggest cybercrime trends of 2019' ; March 2019 for World Economic Forum, available at https://www.weforum.org/ agenda/2019/03/here-are-the-biggest¬cybercrime-trends-of-2019/ ; also: Joint Communication to the European Parliament and the Council : Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels,

September 2017, available at https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cybersecurity_ec.pdf.

[3]. According to 'Human Capital and Digital Skills' Report 2018, available at https://ec.europa.eu/digital-single-market/en/human-capital.

[4]. European Parliamentary Research Service, Scientific Foresight Unit (STOA); Cybersecurity in the EU Common Security and Defence Policy; May 2017; available at http://www.europarl.europa.eu/stoa/.

[5]. European Union Agency for Network and Information Security (ENISA); Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity; December 2018, available at www.enisa.europa.eu.

[6]. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2106 concerning measures for a high common level of security of network and information systems across the Union (The NIS Directive).

[7]. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[8]. 'The Directive on security of network and information systems (NIS Directive)' in European Commission, Strategies, Digital Single Market Policies, available at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive last update August 2018.

[9]. Stalla-Bourdillon, S. et al; Privacy vs Security; Springer, 2014, p. 3.

[10]. Georgieva, L.; The First EU -Wide Legislation on Cybersecurity, European Energy Journal, vol.6, issue 3, December 2016.

[11]. See ENISA, National Cybersecurity Strategies, Overview in the EU; available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

[12]. Bourke, E.; A War without Bullets: Protecting Civilians in the Technology Trenches; Alb. L.J. Sci & Tech, vol. 28, issue 2, 2018, p. 18.

[13]. Georgieva, L.; The First EU-Wide Legislation on Cybersecurity, 6 European Energy Journal; vol.6, issue 3, December 2016.

[14]. See recital (5), NIS Directive.

[15]. See Article 1 (1), NIS Directive.

[16]. Article 7, 1 (d), NIS Directive.

[17]. Stalla-Bourdillon, S. et al; Privacy vs. Security; Springer, 2014, p. 2.

[18]. Idem, p. 62.

[19]. European Parliament resolution of 3 October 2017 on the fight against cybercrime, adopted text.

[20]. 'General considerations' in the European Parliament resolution of 3 October 2017 on the fight against cybercrime, adopted text.

[21]. See points 28, 30, 31 of 'Prevention' in the European Parliament resolution of 3 October 2017 on the fight against cybercrime, adopted text.

[22]. Popescu, A.; The Right to Information and Cybersecurity, Journal of Law and Public Administration, vol. 3, issue 6, 2017, p. 106.

[23]. Pawlak, P. (ed.) Riding the digital wave: the impact of cyber capacity building on human development; Report 21, December 2014; EU Institute for Security Studies; Pawlak in Introduction, p. 6.

[24]. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, ENISA, December 2018, p. 18.

[25]. 'Cyber Security Index'; 'the Index of Cyber Security is a measure of risk. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite'; available at: www.cybersecurityindex.org.

[26]. See Introduction to Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, March 2017; available at https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cybersecurity_ec.pdf "Unless we substantially improve our cybersecurity, the risk will increase in line with digital transformation", p. 2.

[27]. Grimes, R.; Ten topics every security training program should cover; Sep. 2018, available at https://www.csoonline.com/article/3298961/10-topics-every-security-training-program-should¬cover.html.

[28]. Jardine, E.; Sometimes Three Rights Really Do Make a Wrong: Measuring Cybersecurity and Simpson's Paradox; Paper presented to the 16th Annual Workshop on the Economics of Information Security, CA, 2017.

[29]. e.g. using antivirus, antimalware software, use strong, separate passwords, back-up important data; https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online.

[30]. "from 2008 when the IoT entered the sample until the end of 2017, the IoT grew some 1631 percent, naïve users grew by 310 percent and savvy users grew by only 34 percent" in Jardine, 2017, p. 11.

[31]. see: Digital skills and jobs coalition, under the European Commission 'Digital Single Market' policy, available at https://ec.europa.eu/digital-single-market/en/policies/digital-skills.

[32]. see 'Upskilling pathways - New opportunities for adults' under the European Commission's Policies and activities available at https://ec.europa.eu/social/main.jsp?catId=1224&langId=en.

[33]. Coventry, L.; Briggs, P.; Blythe, J.; Tran, M.; Using behavioural insights to improve the public's use of cyber security best practices. Project Report. Government Office for Science; 2014, p. 8; Retrieved from http://nrl.northumbria.ac.uk/23903/.