УДК 159.9:681.3

Mescheryakov D.S.

PhD in Psychology, Institute of Psychology named after G.S. Kostyuk,

NAES of Ukraine

E-mail: meoldom@gmail.com

http://orcid.org/0000-0001-6831-8654

Key psychological factors of the cybersecurity.

The cybersecurity depends not only on the technical solutions, the humans behavior, activity and their psychology also matters in development of the safe environment, including virtual. We are proposing next key factors, which needs take to consideration in cybersecurity complex organization.

Organizational:

- providing and keeping the right values and traditions (which update to current and upcoming challenges);
- designing and modeling of processes before implementing;
- the balance between actual goals and its realization;
- detailed rules and standard procedures (protocols): normal and force major;
- incidents response and feedback system;
- security policies;
- job duties and their limitations;
- dividing of cross duties;
- optimal management and auditing system;
- motivational system (including punishments and rewards);
- recruiting effectiveness;
- ongoing skill and reflexes training;
- corporate culture based on the optimal organization model.

Educational and developmental:

- incorporate the organization values into work environment;
- informing about new threats;
- actualizing the knowledge of ongoing cyber safety threats and methods of countermeasure;
- training of actual skill and behavior (reflexes);
- providing of up-to-date security threats mental model: also provide and support of security conception.

Personal:

- informed decision making;
- integrate and develop the right values: personal, team and corporate;
- pro-security personal and corporate position;
- safe behavior: “safety thinking;
- reflexes, habits;
- motivation;
- culture: work, lifestyle etc;
- following rules, policies and corporate culture;
- constant self-development and self-improvement;
- being a subject, which means responsibility of own actions, critical thinking, prognostication of own actions and situations consequences, goal setting, designing of activities etc.

We can consider the values that important to security are: safety; safe environment; information; privacy; confidentiality; integrity; vigilance; wellbeing of the organization, property and members etc. Traditions are based on the values and keeps the working environment running according to them and maintaining the corporate culture. For the informational safety is necessary to have traditions of organization with respect, delicate attitude to the information and cybersecurity. All the members of the company including owners and managers should follow traditions without exceptions to have an appropriate safety level. Until that, traditions will not work on safety and security will be under risk.

Thereby, the organizational function here is establishing of effective cooperation with use of psychology and other knowledge. The educational and developmental function is providing complex learning system and learning environment to that cooperation. And personal function is being a subject of that cooperation, learning and development.

References

1. Мещеряков, Д.С. (2019). Розвиток суб'єктної активності дорослих користувачів соціальних мереж: дис. ... канд. психол. наук: 19.00.07. НАПН України, Ін-т психології імені Г.С. Костюка. Київ.
2. Mcalaney, John & Taylor, Jacqui & Faily, Shamal. (2015). The Social Psychology of Cybersecurity. 10.13140/RG.2.1.1275.6961.
3. Poteete, Paul Wyatt. (2020). Psychometric Modelling of Cybersecurity Roles. ICCWS 2020 15th International Conference on Cyber Warfare and Security. DOI:10.34190/ICCWS.20.103
4. Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. Psychology of Popular Media Culture. Advance online publication. https://doi.org/10.1037/ppm0000247
5. Wiederhold, Brenda. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyberpsychology, behavior and social networking. 17. 131-2. 10.1089/cyber.2014.1502.