Slide No.:

1. Welcome to this presentation. It is about a solution to human factor related issues in cyber security.
2. Let us quickly go through those human factors to better understand why the solution proposed within this presentation was chosen.
3. One human factor is the lack of understanding of employees of any organization. By not knowing how the major attacks take place and how they typically work it is almost impossible to defend against those.
4. Another human factor is ignorance about the risk. Sometimes people are aware of potential ways hackers might attack, but some might simply still not know, that he information they are dealing with is actually very valuable to a hacker. Without the knowledge of the value, it comes as no surprise, that some might not sufficiently safeguard this information.
5. Another human factor worth mentioning is the privacy paradox. Many people are giving away personal information, that can be helpful for a phishing attack for relatively small rewards on social media.
6. The knowing doing gap is when people do know that their behavior is not correct, but they still are doing it. This has several reasons, one being the fact that for example in western culture you are trained to be primarily productive and that it is socially acceptable to cut corners such as not taking care of security in order to achieve maximum productivity.
7. Lastly insider threat whether if accidental or on purpose is a human factor that needs to be considered, when designing a secure system.
8. What can be a solution to those human factors? – But before we discuss this, let me also talk about the social and ethical constraints we must consider.
9. Many social constraints are collected in laws …
    a. such as the US computer accessibility law, which was created to eliminate barriers in IT for people that are for example blind or in any other way impaired.
    b. Another law that needs to be followed, when designing a solution that resolves human factors, is the GDPR. The organization for example must get consent, if data is collected in order to improve corporate IT security or the organization must take care that only relevant data for those tasks is stored.
10. Ethical constraints for example would be …
    a. that a person needs to be respected.
    An example for this would be, that participation in any work group improving security needs to be voluntary. Forced participation is simply not respectful and should not be done.
    b. It is also important to follow beneficence, which simply means that no harm may done to any human or user. This can be achieved by maximizing benefits such as for example a salary bonus and minimizing potential harm by for example anonymizing names of participants wherever possible.
    c. Each person should also be treated equally. The selection of participants must therefore be fair.
    d. Laws and relevant public interest must of course also be followed, and results should always be transparent
11. But what is the solution?
12. The solution to address human factors in cyber security is an effective security culture. It is a balance of multiple items. But before I explain them in detail, …
13. let me tell you that effective security culture is not only a balance of three items, but also an iterative process. An organization must constantly go through the steps

a. Analyze
b. Plan
c. Implement
d. Evaluate and iterate

This is because not only does an organization continuously change - hopefully grow. It is also because the technology evolves on a rapid pace as well as the tactics and tools of cyber criminals.

14. Let us discuss the three elements of an effective security culture now.
15. The first item I would like to discuss is the organizational part of an effective security culture.
16.
    a. An organization must have security policies and procedures in place. Security, where necessary, always must fit into a workflow.
    b. Another organizational tool is to create self-reported surveys, which can be used by anybody within an organization, to flag cyber security issues. “see something – say something”
    c. Additionally, skilled superiors could monitor security behavior.

    All those three items listed here as well as the following may or may not be used by an organization, since some elements sometimes simply do not fit. This proposal is not a solution to all organizations. This proposal is a guidance which can be adapted to fit to any organization. Some organization might for example not be capable of installing focus groups.

17. Let us move on to the individual / behavioral part of an effective security culture.
    It is key that awareness is initially created, but also maintained.
    Also education must be conducted on a regular basis and should talk about
    a. The value of company assets
    b. current threats for the organisation
    c. Typical attack methods & vectors

    This will for example ensure, that human factors mentioned at the beginning of this presentation are properly addressed.
18. Additionally, an organization could conduct trainings / simulations such as
    a. (Phishing) simulation
    b. Security games
    c. Physical access entry simulations

    Those simulations perfectly show that an effective security culture is an iterative process, since those simulations can be used to analyses the security awareness of an organization for example.
19. When the afore mentioned is well implemented and truly conducted by an organization, it is safe to say, that employees don’t lack any motivation to perform security tasks as they should. But this isn’t enough
20. Let us talk about the B-MAT Model.
    a. On the y- axis we have “motivation”
    b. On the x-axis we have “ability”
    c. The more motivation and ability an employee has, the more likely it will become that an employee does perform a certain task or behavior.
21. If you for example have high motivation
    a. But low ability to perform a given task
    b. The result will be that it is not likely that you perform the task
22. If on the other hand

a. You do have high motivation
b. And the organization has given you the right tools
c. It is very likely that you will perform this task. But how do we improve a person's "ability"?
d. We make it easy, measured in time or effort it takes, for a person to do a given task by providing the right technological means.

23. A great technological mean is to have usable security, which means that
    a. Security must be well integrated in applicable workflows of your organization
    b. That any unnecessary alarm prompts or actions to secure assets are avoided
    c. That security messages are properly emphasized. Be aware that, if you show unimportant alarm messages emphasized, that soon important ones will also be ignored by operators. This is called alarm fatigue.
    d. Make sure that you do have a good structure within for example your security settings. Combine similar items in proximity, make them look the same. Use visual hierarchy.
       On the other hand, separate items by space, that need to be separated
    e. Use pictograms wherever possible. Collect user feedback, that show you have chosen correct pictograms and that the message is understandable by the user.
    f. Keep security text shorts. Studies show, that despite popular belief, information seldomly gets lost, when shortening security texts.
       Avoid using terminology a user does not understand. A nurse for example might not understand the phrase: "Please reauthenticate" a phrase like "Please log in again" would be better.
    g. Use easy and secure authentication wherever possible. "One-time passwords" and "two factor authentication" can ramp up security significantly without taking too much time from an user.
    h. Always do progressive disclosure. Hide advanced functionality until the user needs it.
24. You must keep in mind, when integrating security into software, that the goals "Security", "Functionality" and "Ease of Use" are to some extent in contradiction to each other. By adding more security for example, the "Functionality" and "Ease of use" might suffer.
    You must try to find the correct balance for your software that fits your organization best.
25.
    a. Blockchain is also a great technological element for an effective security culture of some organization, since it can for example be used to flag human errors with little effort.
    b. Artificial Intelligence can for example be used to detect accidental or intentional insider threat with ease, if used correctly.
26. Lastly it is important to conclude one more time, that the afore mentioned items of the effective security culture must be balanced.
    A good statement to keep in mind when balancing is the following: "fitting the task to the human is in the long run proven to be more cost effective than vice versa."
27. The solution to human factor related issues in cyber security…
    a. … is an effective security culture that is well balanced, tailored to the needs of your organisation and iterative.

(ENISA 2018, Fogg 2009, Cox 2012, Johnson 2021, Sasse & Rashid 2019, Yao 2017, Waite 2010. Kokolakis 2015, Sasse 2021)

References:

ENISA (2018) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Available from: https://www.thehaguesecuritydelta.com/media/com_hsd/report/228/document/WP2018-O-3-3-2-Review-of-Behavioural-SciencesResearch-in-the-Field-of-Cybersecurity.pdf [Accessed on 2021-10-29]

Fogg, B.J., (2009). 'A behaviour model for persuasive design'. The 4th international Conference on Persuasive Technology. Claremont, California, USA, 26-29 April. ACM: New York, NY United States, DOI: https://doi.org/10.1145/1541948.1541999 [Accessed on 2021-10-29]

Cox, J. (2012) Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior 28: 1849-1858: https://www.researchgate.net/publication/257252888_Information_systems_user_security_A_structured_model_of_the_knowing-doing_gap [Accessed on 2021-10-29]

Johnson, J. (2021) Designing with the Mind in Mind. Third Edition. Cambridge: Elsevier Inc.

Sasse, A. Rashid, A. (2019) Human Factors Knowledge Area. First Edition. Bristol: CyBOK

Yao, M. (2017) Your Electronic Medical Records Could Be Worth $1000 To Hackers. Forbes. Available from: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/?sh=1c8f72f450cf [Accessed on 2021-10-29]

Waite, A. (2010) InfoSec Triads: Security/Functionality/Ease-of-Use Available from: https://blog.infosanity.co.uk/?p=676 [Accessed on 2021-10-29]

Kokolakis, S. (2015) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Computers & Security DOI: https://doi.org/10.1016/j.cose.2015.07.002 [Accessed on 2021-10-29]

Sasse, M.A & Rashid A (2019) Human Factors Issue. The Cyber Security Body Of Knowledge (1). Available from: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf [Accessed on 2021-10-29]