**Unit 2: Fitting the Task to the Human**

Welcome to Week 2. This unit focuses on approaches to designing security solutions to fit human capabilities and limitations. You will apply the knowledge gained in the first unit to identify appropriate design solutions based on the ISO usability criteria: effectiveness, efficiency and satisfactory.

**In this unit we shall:**

* + Cover the four key principles to designing security to fit to humans.
  + Identify specific user groups and appropriate security design solution for such groups.
  + identify available techniques and technologies to facilitate the design.

**On completion of this unit, you will be able to:**

* + Develop the awareness to fit security design to humans.
  + Evaluate available techniques and technologies for a given design solution.
  + Develop the capacity to evaluate usable security design.

This week builds on the knowledge gained in week one content by discussing the human capabilities and limitations and how usable security design solutions need to fit these limitations. The available technologies and techniques are discussed within the context of usable security.

**Reflection:**

In the current predicament, the security of the system should be the priority for any organization. Protecting one's data from being stolen or otherwise compromised should be the primary focus of any organization GeeksforGeeks. (2020, February 13). The major which have to cover by each of the organization describes as follow.

1. **Confidentiality:** The degree to which the information is kept private determines its level of secrecy. The principle dictates that only the sender and recipient will have access to the information that is communicated between them. When an unauthorized third party can read a communication, the secrecy of the message is compromised (IT, M. C. M. C., (2019, October 10)).
2. **Authentication:** Authentication is the procedure through which a user, system, or object is verified as being who or what it claims to be. To ensure that the user is who they say they are, it checks their credentials. Most of the required security is provided via a login and password. Confidential information is only accessible to the authorized individual whose identification has been previously registered TechWeb. (n.d.).
3. **Integrity:** If you have integrity, you may rest assured that the information you receive will be accurate. When a message's content is changed after it has been delivered but before it reaches the recipient, it may be said to have lost its integrity in transit (Chang, R. (2021, November 5)).
4. **Availability:** The resources must be always available to the authorized user, as stated by the availability principle. At all times, this must be the case. Without the ability to share this data with the right people, it serves no purpose (Chang, R. (2021, November 5)).

Here we are defining the security training program, that all the employees need training in every field but specially in the IT systems, Technologies, and smart products. Here we are defining how we will conduct training for the employees and what are the pros and cons and what things we must keep in mind while we make training sessions.

### Training Basics

Training basics includes the following set of points against each dimension that is presented in maturity model which are given below in the table.

|  |  |
| --- | --- |
| Dimensions | Trainings Needed |
| Knowledge | Must know about company infrastructure.  Must have knowledge of company portfolio. |
| Strategy and Leadership | Must know about the strategic plans.  Know which person leads to them and what type of work will do. |
| Employee | How employee will be sincere.  Must listen the employees’ obstacles.  Give preference to their employees. |
| IT System | What type of work they will do?  If an attack come how, IT team behave.  How to overcome these IT related issues. |
| Smart Product | Introduce them with the smart product. Even most of employee do not know what type of smart products they are using. |
| Phishing Awareness | Made a phishing awareness campaign to train your employees. |
| Hire Security Team | Must hire the security team and train them. |

Workshop for the Executive Teams.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dimensions | Listener | Time | Training period | Agenda |
| Knowledge | Workers, Executive | 15 minutes | Once a year | For employee well understanding about organization. |
| Strategy and Leadership | Executives | 30 minutes | After 6 months | To know and familiar with the company goals. |
| Employee | All Employees | 15 minutes | Once a year | Must listen the employee’s obstacles and difficulties. |
| IT System | IT team | 30 minutes | Every month | Very special case:  Familiar with the work.  What to do in which condition. |
| Smart Product | All Employees | 15 minutes | Once a year | At least employee knows the functionalities of products. |
| Phishing Awareness | All company Employees | 30 minutes | After 6 months | Make for the well understanding to employee about phishing. |
| Security Team | Security team | 15 minutes | Once a year | Must know about the technologies that is utilizing by the companies. |

For making your organization and business secure you must consider these following steps (Solutions, V. (2018, August 18)).

1. Create a Security Policy
2. Educate Your Employees on Business Cybersecurity
3. Use Secure Passwords
4. Keep Software Up to Date
5. Secure Your Networks
6. Back Up Your Data
7. Control Access to Device
8. Cybersecurity Training

**References:**

GeeksforGeeks. (2020, February 13). Cryptography and Network Security Principles. Retrieved from GeeksforGeeks website: <https://www.geeksforgeeks.org/cryptography-and-network-security-principles/>.

IT, M. C. M. C. is associate teaching professor of, analytics, & Dame, operations at the U. of N. (2019, October 10). Security, Privacy and Confidentiality: What’s the Difference? Retrieved from Technology Solutions That Drive Education website: <https://edtechmagazine.com/higher/article/2019/10/security-privacy-and-confidentiality-whats-difference>.

TechWeb. (n.d.). Understanding Authentication, Authorization, and Encryption: TechWeb : Boston University. Retrieved from www.bu.edu website: <https://www.bu.edu/tech/about/security-resources/bestpractice/auth/>.

Chang, R. (2021, November 5). Confidentiality, Integrity and Availability in Cyber Security. Retrieved August 20, 2022, from Kobalt.io website: https://kobalt.io/blogpost/confidentiality-integrity-and-availability-in-cyber-security/.

Solutions, V. (2018, August 18). Eight Cybersecurity Tips to Keep Your Organization Secure. Retrieved from Vector Solutions website: https://www.vectorsolutions.com/resources/blogs/8-cyber-security-tips-to-keep-your-organization-secure/