Top of FormBottom of Form**Unit 1: Human Factors and Cyber Security**

Welcome to Week 1 of The Human Factor module. We will be setting the agenda by looking at the bigger picture of Human Factors within the context of Cyber Security. The role of Human Factors and why it is critical to pay particular attention to human behavior when designing computing systems as professionals in organizations.

This week’s lesson will focus on setting the context by looking at some data on the major causes of data breaches, type of attacks that are caused by humans and their impact on the organizations. We will then discuss the limitations of human capabilities and factors that influences humans' interactions with computing systems, and the need to design security solutions around these limitations in order to achieve optimum security. The lecture cast also introduces the concept of the ‘malicious insider’, insider threat and their traits, as well as some behavior modelling tools to understand human behavior.

**In this unit we shall:**

* Explore human behavior and its implications in designing computing systems within the context of cyber security.
* Discuss human capabilities and limitations and their impact on usable security.
* Discuss the concept of insider threat and accidental insider and their effect on security.

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

* Develop an understanding of the security issues and risks associated with how people interact with computing systems.
* Appreciate the impact of human factors and activities on security of computing systems in an organization.

This week provides the foundation and context for the entire module. It begins by examining the available evidence to understand the scale and the nature of the security problems caused by human factors. It provides information on the limits on human capabilities as key drivers for designing security solutions that fit human behavior which services the background to the module

**Reflection:**

When studying behavioral analysis in the field of cybersecurity, it is essential to have a clear understanding on both how individuals provide a threat to enterprises and how such threats can be mitigated. Experts in cybersecurity need to study how people act and find ways to teach and train people so they don't make these mistakes. In cybersecurity, "human factors" are any actions or events that can cause a data breach. The main reasons for these problems are lack of understanding, lack of knowledge, or bad access control. (CYDEF, 2021).

Understanding normal behavior is essential for detecting anomalies and mitigating cyberattacks. Behavioral sciences with a focus on user behavior can give significant tools for enhancing cyber security and mitigating the effects of social engineering and cognitive hacking tactics employed by cybercriminals. Human behavior is one of the greatest threats to a secure network, and it is essential to understand human behavior in order to recognize anomalies and prevent cyberattacks (i.e., spreading false information).

But cyber attackers can also manipulate the minds of computer system users instead of the computer system itself. For example, they can use social engineering (e.g., tricking computer system users to get information like passwords) and psychological hacking (e.g., spreading false information) to break into a network or computer system. This can be done with social engineering (e.g., tricking people who use a computer system to get information like passwords) and cognitive hacking (e.g., tricking people's minds to get information) (King et al., 2018).

This change means putting more focus on areas that haven't been studied much yet, like the behavioral aspects of cybersecurity. Since most cyber problems are caused by people, this move means more research is needed. Focusing on social and behavioral problems is more important than ever when trying to change the current situation (Maalem Lahcen et al., 2020).

When a member of an organization's internal community who has been given authorized access uses that access to hurt the organization's important information or systems, this is called an "insider threat." This person doesn't have to be an employee; they could be a third-party vendor, an independent contractor, or a business partner. Unintentional insider threats are not caused by employees who act maliciously. Instead, they are caused by employees who inadvertently pose a significant risk because they don't follow corporate security policies or use company systems or data in a careless way (Froehlich, n.d.).

**References:**

CYDEF (2021). The Human Factor: The Hidden Problem of Cybersecurity. [online] CYDEF. Available at: <https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/>.

Froehlich, A. (n.d.). What is an insider threat? [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/insider-threat.

King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B. and Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. Frontiers in Psychology, 9. doi:10.3389/fpsyg.2018.00039.

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. and Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(1). doi:10.1186/s42400-020-00050-w.