**Unit 5: Ethical, Societal and Organizational Issues**

Welcome to Week 5. This unit focuses on the cross-cutting issues which need to be reviewed to achieve optimal usable security solution for an organization and society. It discusses an organizational framework that can be employed to achieve positive security culture. We will also look at various elements of the framework, as well as approaches such as using mental models as risk communication tools within an organization to create awareness. Finally, we will explore the ethical issues around designing a usable security solution.

**In this unit we shall:**

* Discuss cultural, organizational issues and their impact on security.
* Discuss the framework to develop a positive, organizational security culture.
* Cover the use of mental model as security risk communication tool.
* Discuss the legal and ethical requirements and implication when developing usable security.
* Reflect on the current and future research in the various areas of usable security and human factors in cyber security.

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

* Develop the ability to apply and evaluate mental models for risk communication.
* Become the organizational culture and its impact on security.
* Develop the awareness of legal and ethical issues related usable security.
* Understand the usable security issues in current and emergent technologies.

This week builds on the knowledge gained in previous weeks. Previous weeks have focused on the issues related to users and individuals within an organization. This week’s lecture cast focuses on the organizational, legal, and ethical issues within the context of usable security.

**Reflection:**

* **Cultural Organizational Issues:**

When one culture has a difficulty with another culture, a system, or a set of goals, we call this a cultural issue. Culture develops organically because of social interactions and is not predetermined. Uncertainty, poor communication, and inconsistencies are all symptoms of a faulty work environment. These factors may exacerbate the feeling that the workplace is unsafe and unwelcoming, which in turn could lead to problems like harassing, abuse, and high rates of turnover among employees (Impact of Organizational Culture and Security Norms on Security Compliance Pressure: A Competing Value Model Perspective, n.d.).

* **Impact on Security:**

Keeping sensitive data safe is everyone's responsibility in a thriving company culture. Your efforts to shape the company culture will help reduce the risk of an attack from within. In addition, it motivates workers to take initiative in addressing weaknesses and thwarting threats.

* **Using Organizational Culture to Improve Cyber Security:**

Simply stated, the level of security of a firm or government agency depends on the culture surrounding information technology and its use. There will be deeper cross-departmental collaboration when cybersecurity is ingrained in the company's culture (attomus.com, n.d.).

So, it's time to construct an IT infrastructure that is nimbler than ever before. The available cybersecurity expert and the established norms and practices in your organization are the first steps in fostering a more secure environment for your employees.

* [**Security Culture Framework (SCF)**](https://get.clt.re/framework/)**:**

Kai Roer's security culture framework (SCF) is a widely adopted approach to fostering a company-wide commitment to safety, education, and best practices. Companies can use the four pillars of the SCF to reduce cyber risks.

1. **Define Metrics:** Understanding the criteria is the foundation for creating a cybersecurity culture. Organizations need to establish success criteria, establish objectives, and monitor their development.
2. **Involve Your Organization:** It is important for businesses to form a security team, design an employee education program focused on safety training, and implement security-related laws, guidelines, and practices.
3. **Determine Topics:** Wherever employees have the largest gaps in knowledge and skill development should be the focus of training and education programmes. Individuals in non-technical roles are often poorly informed about the company's security standards, rules, and practices.
4. **Review Your Planner:** Developing a strategy document to guide the implementation of your company's new cybersecurity cultural framework is the last phase. A planner's job is to map out the state of the company, key performance indicators, and discussion points so that they may be compared to actual outcomes (Romeo, 2016).

As with a customized algorithm, a person's mental model can influence their behavior and the way they approach challenges and complete activities. Cognitive processes like reasoning and decision-making are thought to rely heavily on mental models, which can be thought of as internal symbols or representations of external reality.

**Legal And Ethical Requirements:**

Principles including anonymity, confidentiality, risk assessment, reporting findings, and communicating with participants are all part of this framework. Privacy, access to data, and online misdeeds are only a few examples of the types of fundamental ethical concerns that arise when using IT over worldwide networks. Encryption methods, Secure Sockets Layer (SSL), digital IDs, and computer firewalls are only some of the technological solutions that have helped alleviate these fundamental problems (Jungermann, Schutz and Thuring, 1988).

**Security Issues in Emergent Technologies:**

Terrorism on a global scale, cyberattacks, piracy, energy supply attacks, and natural and manufactured tragedies are all very serious problems that affect many countries. To successfully guarantee defense against such growing concerns, we will need to adjust existing policy practices (Gunarto, n.d.).

**References:**

Attomus.com. (n.d.). *Using Organisational Culture to Improve Cyber Security*. [online] Available at: <https://attomus.com/blog/2020-using-organisational-culture-to-improve-cyber-security/>.

Gunarto, H. (n.d.). Ethical Issues in Cyberspace and IT Society. [online] Available at: <https://www.apu.ac.jp/~gunarto/it1.pdf>.

Impact of Organizational Culture and Security Norms on Security Compliance Pressure: A Competing Value Model Perspective. (n.d.). [online] Available at: https://facultystaff.richmond.edu/~tmattson/CulturalValuesDraft\_ver2.pdf [Accessed 20 Aug. 2022].

Jungermann, H., Schutz, H. and Thuring, M. (1988). Mental Models in Risk Assessment: Informing People About Drugs. *Risk Analysis*, 8(1), pp.147–155. doi:10.1111/j.1539-6924.1988.tb01161.x.

Romeo, C. (2016). 6 ways to develop a security culture in your organization. [online] TechBeacon. Available at: <https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom>.