4.6 6 Knowledge Area: Human Security

The Human Security knowledge area focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity.

4.6.1 Knowledge Units and Topics

Humans have responsibility to ensure the confidentiality, integrity, and availability (CIA) of their organizational and personal computer systems, while that responsibility is dependent upon each of the Human Security knowledge units outlined below. The following table lists the essentials, knowledge units, and topics of the Human Security knowledge area.

HUMAN SECURITY		
Essentials - Identity management, - Social engineering, - Awareness and understanding, - Social behavioral privacy and security, and - Personal data privacy and security.		
Knowledge Units	**Topic**	**Description/Curricular Guidance**
Identity Management		
	Identification and authentication of people and devices	This topic provides an overview of various access control methods to demonstrate the benefits and challenges of each. Topics include an overview of Network Access Control (NAC), Identity Access Management (IAM), roles, multi-method identification and authentication systems, biometric authentication systems (including issues such as accuracy/FAR/FRR, resistance, privacy, etc.), as well as usability and tolerability of the methods.
	Physical and logical assets control	This topic covers various access controls to physical assets including system hardware, network assets, backup/storage devices, etc. Examples are Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), Roles- based Access Control (RBAC), inventory tracking methods, and identity creation methods (what type of user ID helps increase security with access control, for example, abc1234, first name and last name, first initial and last name).
	Identity as a Service (IaaS)	This topic cover identity management as a service (e.g., Cloud identity) brings forward issues such as the system being out of the user's control with no way to know what has happened to the information in the system, auditing access, ensuring compliance and flexibility to quickly revoke permissions.

	Third-party identity services	This topic provides an overview of the authentication infrastructure used to build, host, and manage third- party identity services. Topics include on-premises, cloud, centralized identity services/password management tools, end-point privilege management, etc.
	Access control attacks and mitigation measures	This topic provides an overview of various types of access control attacks to steal data or user credentials, and mitigation measures for combating them. Topics include password, dictionary, brute force, and spoofing attacks; multifactor authentication; strong password policy; secure password files; restrict access to systems; etc.
Social Engineering		
	Types of social engineering attacks	This topic provides an overview of the different ways that cybercriminals or malicious groups exploit weaknesses in organizations, systems, networks, and personal information used to enable a later cyberattack. Proposed topics included: phishing and spear phishing attacks, physical/impersonation, vishing (phone phishing), email compromise, and baiting.
	Psychology of social engineering attacks	This topic provides an overview of the psychological and behavioral factors related to individuals falling for social engineering attacks. Proposed topics include adversarial thinking, how emotional responses impact decision-making, cognitive biases of risks and rewards, and trust building.
	Misleading users	This topic provides an overview of message systems' and browsers' interfaces and/or user interaction that can be exploited to mislead users. Proposed topics include spoofing message senders, misleading URLs, how users judge and trust webpages and emails, as well as user behaviors with phishing and other browser warnings.
	Detection and mitigation of social engineering attacks	This topic provides scenario-based, hands-on activities via simulation or virtual tools to create an environment of various social engineering attacks. Hands-on experience on the use of tools and technical approaches to detect and/or mitigate different social engineering threats. Proposed tools such as email filtering, blacklist, security information and event management (SIEM) tools, and IDS/IPS.

Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms [*See also Societal Security KA for related content*]		
	System misuse and user misbehavior	This topic provides overview of intentional and unintentional system misuse, cyberbullying, cyber hacking, naive behavior, and ethical dilemmas related to system security decisions.
	Enforcement and rules of behavior	This topic provides an overview of methods and techniques to get people to follow the rules/policies/ethical norms (e.g., driving!). Topics include consequences for not following cybersecurity rules/policy/ethical norms, documentation and audit trail (evidence of compliance to prove that the cybersecurity rules/policy/ethical norms were followed), and knowledge of accountability for not following security rule/policy/ethical norms. Incentives to keep the job (especially after being educated and trained for the proper rules/policy/ethical norms, individuals are legally liable for not following the rules as an employee), and individuals may lose their identity/access in personal life due to a lack of adherence.
	Proper behavior under uncertainty	This topic provides an overview of the methods and techniques to adhere to when uncertain about how to respond to a cybersecurity situation. Topics include CyberIQ, intellectual adaptability, critical thinking, understanding the right versus wrong choices, how to make those choices under uncertainty, rational versus irrational thinking, ethical thinking/decisions, and behavior when there is no clear process to follow (reporting/point of contact/etc.), and human error mitigation.
Awareness and Understanding [*See also, Organizational Security KA for related content*]		

	Risk perception and communication	This topic covers how users perceive and respond to cybersecurity risks, cognitive biases in judging risks, metaphors for communicating particular security risks, and how to frame messages regarding risks. Definition of a mental model, how mental models impact user behavior, as well as common mental models (folk models) of cybersecurity and privacy.
	Cyber hygiene	This topic provides a discussion and activities focused on the individual responsibilities (not the organization) to protect and mitigate against cyberthreats and cyberattacks. Topics include password creation, password storage, mitigation tools, (i.e., anti-virus software), how to identify safe websites, identifying levels of privacy settings, etc.).
	Cybersecurity user education	Methods for educating end-users on various cybersecurity/privacy threats and behaviors. Topics include methods for raising user awareness (PreK-12, employees, public, etc.), delivery methods of cybersecurity education and training (e.g., posters, leaflets, computer-based training, gamification, communication styles, message framing, how to reach different audiences and user communities, individuals with disabilities and/or cognitive impairments), timing and reinforcement of education, as well as impact of training on users' knowledge and behaviors.
	Cyber vulnerabilities and threats awareness	This topic provides an overview of end-user-facing threats as well as Fear, Uncertainty, and Doubt (FUD). Proposed topics include warning signs of internal employee vulnerabilities and threats, awareness of identity theft, business email compromise, threat of free/open Wi-Fi networks, and malware, spyware, and ransomware.
Social and Behavioral Privacy [*See also Societal Security KA for related content*]		
	Social theories of privacy	This topic provides an overview of various theories of privacy from social psychology and social science, emphasizing privacy that involves interacting with other people as opposed to organizations. Proposed topics include privacy tradeoffs and risks in the social context, control and awareness of data consent, personal information monitoring, regulatory protections and concerns on maintaining social privacy.

	Social media privacy and security	This topic provides overview of privacy behaviors and concerns of users in protecting personal information when using social media. Proposed topics include users' online disclosure decisions and behaviors, personas and identity management, determining audience and social access controls, interface and coping mechanisms for managing privacy on various social media sites, challenges of managing time boundaries, as well as personal/workplace boundaries of social media.
Personal Data Privacy and Security [*See also Data Security KA, & Organizational Security KA, for related content.*]		
	Sensitive personal data (SPD)	This topic provides overview of the types of Personal Data (PD), including Personally Identifiable Information (PII), which are especially sensitive due to the risk that such information could be misused to significantly harm an individual in a financial, employment or social way. Proposed topics include examples of data elements of Sensitive Personal Data (SPD) (social security number, social insurance number or other government issued identification number such as a driver's license or passport number; bank account number; credit card numbers; health and medical information; biometric or genetic data, etc.), regulations governing the collection, use and distribution of SPD, and possibilities for inference of SPD.
	Personal tracking and digital footprint	Location tracking, Web traffic tracking, network tracking, personal device tracking, digital assistants recordings (Siri, Alexa, etc.). Topics include users' behaviors and concerns with each of these kinds of tracking, as well as current methods for limiting tracking and protecting privacy.
Usable Security and Privacy [*See also Organizational Security KA, and Societal Security KA, for related content.*]		

	Usability and user experience	Definition of usability and user experience, and the impact that usability (or lack thereof) has on the security and privacy of a system. Topics include examples of usability problems in traditional security systems such as authentication or encryption, usability and security tradeoffs in systems, methods for evaluating the usability of security and privacy systems.
	Human security factors	Students will be able to operate at the intersection of human factors, computer science, and the quality assurance area. This should include a strong core of computing and in-depth human factors and quality assurance. Topics include applied psychology in the context of adversarial thinking and security policies, security economics, regulatory environments, responsibility, liability, self-determination, impersonation, and fraud (e.g., phishing and spear phishing, trust, deception, resistance to biometric authentication and identity management).
	Policy awareness and understanding	This topic provides an overview of regulating policies (e.g., HIPAA, FERPA, PIIs) and the method or technique to take when a security situation arises. Topics include refresher training for policy updates, revisiting of existing threats, and knowledge tests to understand the policy when it comes to data protection. Due to the overlap in topics, also reference the knowledge units in the Societal Security and Organizational Security knowledge areas.
	Privacy policy	This topic provides an overview of privacy policies in social and localized variances. Jurisdictional variance in privacy policy definitions should be explored. The relationships between individuals, organizations, or governmental privacy policies should also be addressed from the users' perspective. Additional topics should include the impact of privacy policy on new tools/software, identifying a need for tools and techniques to be covered in most areas. Moreover, notifications of users of policy on how their data is used so they can make an informed choice as to whether to provide their information.
	Design guidance and implications	Guidelines include reducing user burden and decisions, providing secure defaults, reducing unintentional security and privacy errors, making threats along with risks contextual and concrete, as well as reducing technical language and jargon.

4.6.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Identity Management	
	Explain the difference between identification, authentication, and access authorization of people and devices.
	Discuss the importance of audit trails and logging in identification and authentication.
	Demonstrate the ability to implement the concept of least privilege and segregation of duties.
	Demonstrate the overall understanding of access control attacks and mitigation measures.
Social Engineering	
	Demonstrate overall understanding of the types of social engineering attacks, psychology of social engineering attacks, and misleading users.
	Demonstrate the ability to identify types of social engineering attacks.
	Demonstrate the ability to implement approaches for detection and mitigation of social engineering attacks.
Awareness and understanding	
	Discuss the importance of cyber hygiene, cybersecurity user education, as well as cyber vulnerabilities and threats awareness.
	Describe the major topics within Security Education, Training, and Awareness (SETA) programs.
	Discuss the importance of SETA as countermeasures.
	Discuss the importance of risk perception and communication in the context of mental models of cybersecurity and privacy.
Social behavioral privacy and security	
	Compare and contrast various theories of privacy from social psychology and social science.
	Describe the concepts of privacy tradeoffs and risks in the social context, control and awareness of data consent, personal information monitoring, regulatory protections and concerns on maintaining social privacy.
	Discuss the importance of social media privacy and security.
Personal data privacy and security	
	Discuss the importance of protection of Sensitive Personal Data (SPD) and Personally Identifiable Information (PII).
	Discuss the importance of regulations governing the collection, use and distribution of SPD, and possibilities for inference of SPD.
	Describe the concepts of personal tracking and digital footprint, while understanding the invasiveness of such tools in the context of privacy.