Cybersecurity Principles – 6%

Domain Scope

1. A computing-based discipline involving technology, people, information, and processes to enable assured operations.
2. A focus on implementation, operation, analysis, and testing of the security of computing technologies
3. Recognition of the interdisciplinary nature of the application of cybersecurity including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.
4. The practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.
5. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Domain Competencies

A. Evaluate the purpose and function of cybersecurity technology identifying the tools and systems that reduce the risk of data breaches while enabling vital organization practices. *(Cybersecurity functions)*
B. Implement systems, apply tools, and use concepts to minimize the risk to an organization's cyberspace to address cybersecurity threats. *(Tools and threats)*
C. Use a risk management approach for responding to and recovering from a cyber-attack on system that contains high value information and assets such as an email system. *(Response and risks)*
D. Develop policies and procedures needed to respond and remediate a cyber-attack on a credit card system and describe plan to restore functionality to the infrastructure. *(Policies and procedures)*

Cybersecurity Principles Subdomains

01 Perspectives and impact
(Level 1 minimal degree of engagement)
Competencies:

a. Make sense of the hard problem areas in cybersecurity that continue to make cybersecurity a challenge to implement.
b. Describe how a significant cybersecurity event has led to increased organizational focus on cybersecurity.
c. Tell a story of a significant cybersecurity advance.
d. Evaluate when the Confidentiality, Integrity and Availability (CIA) of information has been or could be violated with regards to providing trust of information.
e. Compare and evaluate different approaches/ implementations of digital currencies.

02 Policy goals and mechanisms
(Level 1 minimal degree of engagement)
Competencies:

a. Recognize when an organization focus is on compliance with standards vs. state of the practice vs. state of the art.
b. Be aware of multiple definitions for the word "policy" within a cybersecurity context.
c. Consider vulnerability notification and the issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities.
d. Contrast the implications of relying on open design or the secrecy of design for security.
e. Express why cybersecurity is a societal imperative.

03 Security services, mechanisms and countermeasures
(Level 2 medium degree of engagement)
Competencies:

a. Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability).
b. Make sense of the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security).
c. Document an example of "countermeasures" for specific threats.
d. Produce a list capabilities and tools that identify cybersecurity risks on an ongoing basis.
e. Show the concept of identity management and how it is important.
f. Make meaning of the concepts of authentication, authorization, and access control.
g. Argue for the benefit of multi-factor authentication.
f. Explain the concepts of authentication, authorization, and access control.
g. Explain the benefit of two-factor authentication, including the use of biometrics.
h. Define application 'whitelisting'.
i. Identify the costs and tradeoffs associated with security that a company implements into a product.

04 Cyberattacks and detection
(Level 2 medium degree of engagement)
Competencies:

a. Define the roles of prevention, deterrence, and detection mechanisms.
b. Identify password guessing, port scanning, SQL injection probes, and other cyberattacks in log files.
c. Discuss the role and limitations of signature-based and behavioral-based anti-virus technology.
d. Explain two differences between host-based and network-based intrusion detection systems.
e. Create three rules for a network-based intrusion detection system that will protect against specific known attacks.
f. Discuss the use of deception by malware to evade security mechanisms.

05 High assurance systems
(Level 2 medium degree of engagement)
Competencies:

a. Make sense of the concepts of trust and trustworthiness.
b. Describe how the principle of least privilege and isolation is applied to system design.
c. Describe how the principles of fail-safe and deny-by-default fit high assurance systems.
d. Describe how mediation and the Principle of Complete Mediation apply.
e. Make sense of the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
f. Describe how commercial approaches to delivering high-assurance services, including SE Linux, Security Enhanced hypervisors, role- based access systems, and digital signatures are applied to code and data.
g. Document the role of formal methods in creating high assurance software and systems.
h. Describe how Trusted Platform Modules (TPMs) are used in creating high assurance systems.

06 Vulnerabilities, threats and risk
(Level 2 medium degree of engagement)
Competencies:

a. Express the differences between vulnerabilities, threats, and risk.
b. Describe how security mechanisms can contain vulnerabilities.
c. Use a risk management framework.
d. Use penetration-testing tools to identify a vulnerability.
e. Derive several benefits of defense in depth, e.g., having multiple layers of defenses.
f. Describe how security issues arise at boundaries between components.
g. Use the National Vulnerability Database to determine if software installed on a server or network component has a known vulnerability.
h. Recognize vulnerabilities, threats and risks that are distinct to network infrastructure, cloud computing servers, desktop computers, and mobile devices.
i. Use a buffer-overflow attack against a server that reads an unbounded data into a fixed-size data structure.
j. Use a cross-site scripting attack against a server that does not properly sanitize user input prior to displaying the results in a browser.

07 Anonymity systems
(Level 1 minimal degree of engagement)
Competencies:

a. Compare the limitations and strengths of anonymous communication and payment systems currently in use.
b. Propose legitimate and illicit uses of anonymity systems.
c. Model policies for prohibiting or using anonymity systems within an organization.
d. Use an anonymity system (e.g., Tor).
e. Document the kind of information not protected by an anonymous communication system.
f. Evaluate the impact of search queries on maintaining anonymity.
g. Evaluate the implications of DNS queries on maintaining anonymity.

08 Usable security
(Level 1 minimal degree of engagement)
Competencies:

a. Describe how the concept of "psychological acceptability" and the importance of usability impact security mechanism design.
b. Make sense of research studies that consistently demonstrate that a trust-oriented interface design can facilitate the development of more trustworthy systems.
c. Design a user interface for a security mechanism.
d. Analyze a security policy and/or procedure to show where it considers, or fails to consider, human factors.
e. Critique the ability of complex password policies to achieve the desired goal of preventing unauthorized access to sensitive systems.
f. Recognize the differences between erasing pointers to information and overwriting the information as they apply to file systems, databases, and cloud storage.
g. Judge the effectiveness of an authentication mechanism from the perspective of a person who is visually impaired.
h. Design and develop software suite for a new digital currency.

09 Cryptography overview
(Level 1 minimal degree of engagement)
Competencies:

a. Exhibit comprehension of the terms encryption, decryption, key, public key cryptography, symmetric cryptography, algorithm, key length, key escrow, key recover, key splitting, random number generator, nonce, initialization vector, cryptographic mode, plaintext, cipher text, S/MIME, PGP, IPsec, TLS.
b. Contrast encryption, digital signatures, and hash functions.
c. Compare encryption for data at rest and data in motion.
d. Make sense of block-level encryption, file-level encryption, and application-level encryption for encrypted storage.
e. Argue for why it is preferred to use validated, proven algorithms and implementations rather than developing new ones.

10 Malware fundamentals
(Level 1 minimal degree of engagement)
Competencies:

a. Tell a story of how malware is concealed and the impact that malware might have on a system.
b. Use signature-based or behavior detection malware countermeasures to address malware infection mechanisms.
c. Propose where within the architectures of organization's information systems it might be most effective to provide protection from malware.
d. Debug a system (network, computer, or application) for the presence of malware.
e. Use techniques for safely isolating malware samples from infected systems and classifying the sample.

11 Mitigation and recovery
(Level 1 minimal degree of engagement)
Competencies:

a. Discuss a risk mitigation and incident recovery plan.
b. Perform a mitigation of a malware infection on an enterprise client and an enterprise server.
c. Document the managerial and forensic steps for recovery after detecting a hostile insider.
d. Contrast backup and recovery plans designed to protect against natural disasters from those designed to protect against hostile actors.
e. Document examples of the steps taken after a credential is lost or compromised.
f. Describe how supply chain risks could be reduced.

12 Personal information
(Level 1 minimal degree of engagement)
Competencies:

a. Make sense of the terms Personal Information, Personally Identifiable Information, De-Identification, Anonymization, Pseudonym, Masking, and Unmasking.
b. Describe how the Fair Information Practices apply to personal information and how online entities collect and use personal information.
c. Classify several categories of personal information according to privacy and disclosure risk.
d. Contrast policies for collecting, processing, storing, sharing, and disposing of personal information.
e. Illustrate the role and limitations of encryption for protecting personal information.
f. Make sense of policies and technologies for isolating personal data from enterprise data.
g. Analyze approaches for controlling access to personal information.

13 Operational issues
(Level 2 medium degree of engagement)
Competencies:

a. Show how one determines the exposure and plans for the recovery of a lost laptop and mobile device.
b. Document standards that apply to an organization's information security posture.
c. Evaluate potential vendors with respect to their security offerings.
d. Make meaning of emerging threats, vulnerabilities, and mitigations.
e. Design a continuing education program.
f. Make sense of the challenges of recruitment and retention of security personnel.
g. Suggest and implement digital currency extensions using relevant scripting techniques (colored coins paradigm).

14 Reporting requirements
(Level 1 minimal degree of engagement)
Competencies:

a. Document legal and regulatory requirements for sharing of threat and breach information.
b. Contrast different vulnerability disclosure policies, including "full disclosure," and "responsible disclosure."
c. Make sense of the concept of privacy breach versus security breach and the governing rules that apply to both types of breach.

Note: Level L1 (L1) used within a subdomain indicates a minimal degree of engagement associated with the learning proficiency of the fundamentals of the subdomain.

Levels 2 (L2) and 3 (L3) used within a subdomain indicate medium and large degrees of learning engagement associated with the application and transferring of learning to complex problems and situations.