IC3 GS4 Cyber Security Objective Domain

1. **Demonstrate an understanding of basic security concepts.**
    a. Distinguish between vulnerability and a threat.
    b. Discuss the different types of attacks (e.g., active, passive).
    c. Define written security policy and explain its role in cyber security.
    d. Describe the basic methods of authentication (e.g., password, biometrics, smart cards, multifactor, mutual).
    e. Describe the various types of encryption and how they can be effectively used to protect the confidentiality of data.
    f. Describe hash functions and their role in authentication.*
    g. Describe various method of access control used in computer security (e.g permissions, domain vs. workgroup, homegroup).*
    h. Identify common security tools (anti-virus, screen saver settings, etc.)
    i. Describe risks relating to peer-to-peer file sharing and media shares
    j. Explain what is meant by risk assessment and describe, in general terms, what factors are considered during a risk assessment.
    k. Explain what is meant by risk mitigation.

2. **Demonstrate an understanding of legal and ethical issues in cyber security.**
    a. Define cyber-crime
    b. Identify the key legislative acts that impact cyber security.* (Localization concerns)
    c. Describe the Federal criminal code related to computers and give examples of cyber-crimes and penalties, particularly those involving inappropriate access. (Localization concerns)
    d. Discuss digital forensics and its role in cyber security. (keep basic from the perspective of the end-user))
    e. Distinguish among the Intellectual Property Rights of trademark, patent, and copyright. (Localization concerns)
    f. Explain digital rights management and the implications of the Digital Millennium Copyright Act. (Localization concerns)
    g. Describe the implications of social media (e.g., Facebook, Twitter, et al) on the safeguarding of personal or sensitive information. (This could be expanded)
    h. Describe various safeguards that can be employed to help ensure that sensitive or confidential information is not inadvertently divulged or obtained.

3. **Understand security concerns and concepts of the following types of devices.**
    a. Firewalls

b. Routers
c. Switches *
d. Wireless
e. Modems *
f. RAS (Remote Access Server)
g. VPN (Virtual Private Network)
h. h.IDS (Intrusion Detection System)*
i. Network Monitoring / Diagnostics *
j. Workstations
k. Servers *
l. l.Mobile Devices
m. m. Removable drives (Thumb drives, removable storage devices)
n. n. webcam
o. o. game consoles
p. p. proxy servers
q. q. printers
r. r. Bluetooth accessories

4. **Demonstrate an understanding of common information and computer system security** vulnerabilities.
    a. Describe the basic categories of vulnerabilities associated with cyber security (i.e., hardware, software, network, human, physical, and organizational).
    b. Describe the ways in which social networks such as Facebook, Twitter, Google+, instagram, Pinterest, LinkedIn, Blog platforms, and MySpace are cyber security targets.
    c. Describe footprinting and explain how it is used to reveal information an attacker can use to gain access to a company's network.
    d. Explain the trade-off between usability and security with regards to default settings and technical controls.
    e. Describe the information that can be obtained by port scanning and how to protect against port scanning.
    f. Describe what is meant by password strength and explain its relationship to vulnerability.
    g. Distinguish between a weak and a strong password.
    h. Describe some of the ways in which intruders are able to cover their tracks.
    i. Describe the circumstances under which a computer system is vulnerable to a denial of service attack.

5. **Demonstrate an understanding of common cyber-attack mechanisms, their consequences,** motivation for their use, and mitigation strategies.

a. Describe spoofing as an attack mechanism and discuss its consequences mechanisms, their consequences, motivation for their use, and mitigation strategies.
b. Describe the introduction of malware or spyware as an attack mechanism and discuss its consequences , motivation for their use, and mitigation strategies.
c. Describe the use of grayware as an attack mechanism and discuss its consequences, motivation for their use, and mitigation strategies.
d. Describe the use of computer viruses or worms as an attack mechanism and discuss its consequences , motivation for their use, and mitigation strategies.
e. Describe Logic Bombs as an attack mechanism and discuss its consequences and , motivation for their use, and mitigation strategies.
f. Describe botnet and rootkit as an attack mechanism and discuss its consequences, motivation for their use, and mitigation strategies.
g. Describe the introduction of a Trojan Horse as an attack mechanism and discuss its consequences, motivation for their use, and mitigation strategies.
h. Describe DNS poisoning and pharming as an attack mechanism and discuss its consequences, motivation for their use, and mitigation strategies.
i. Describe buffer overflow as an attack mechanism and discuss its consequences, motivation for their use, and mitigation strategies.
j. Describe SQL injection as an attack mechanism and discuss its consequences, motivation for their use, and mitigation strategies.
k. Describe QR codes as an attack vector, its consequences, motivation for their use, and mitigation strategies.
l. Describe peer-to-peer file sharing services as an attack vector, its consequences, motivation for their use, and mitigation strategies.
m. Identify common openings for attacks, data entry forms, Web sites, blogs, etc.

6. Be able to identify and explain the following different kinds of cryptographic algorithms.

a. Hashing Functions
b. Symmetric Keys
c. Asymmetric Keys
d. Kerberos

7. Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation.

a. Define intrusion.
b. Describe the classes of intruders (i.e., masquerader, misfeasor, and clandestine user).
c. Describe what is meant by a hacker and discuss their role in cyber security.
d. d. Compare and contrast the “black hat” and “white hat” hacker cultures (i.e., computer criminal versus computer security expert).

e. Describe various techniques used by hackers to achieve intrusion and identify steps you can take to mitigate the risk of an attack.

8. Demonstrate an understanding of Intrusion Detection Systems (IDS).

a. Describe the three logical components that comprise an IDS (i.e., sensors, analyzers, and user interface).
b. Explain how user behavior relates to the detection of an intruder.
c. Describe the essential requirements for any IDS.

9. Demonstrate an understanding of firewalls and other means of intrusion prevention.

a. Describe the purpose and limitations of firewalls.
b. Describe the four types of firewalls (i.e., packet filtering, stateful inspection, application-level gateway, and circuit-level gateway).
c. Describe the use of honeypots as an intrusion prevention technique.
d. Explain how written security policies are used to prevent intruders.
e. Explain how Access Control Lists (ACLs) are used to prevent intrusion.
f. Demonstrate and understanding of network and host firewalls

10. Demonstrate an understanding of vulnerabilities unique to virtual computing environments.

a. Describe the limitations of traffic monitoring within virtual networks.
b. Discuss the primary vulnerability of virtual operating systems.
c. Describe the "hypervisor" and explain its role in securing a virtual environment.
d. Discuss the ramifications of allowing a virtual machine to communicate on a network.
e. Explain incentives for using virtual machines.
f. Describe the security benefits of using Virtual Desktop Interface.

11. Demonstrate an understanding of social engineering and its implications to cyber security.

a. Define social engineering and describe its role in cyber security.
b. Discuss common mechanisms that constitute social engineering (e.g., phishing, baiting, quid pro quo, pretexting, et al).
c. Describe the variety of attacks targeting the human element.
d. Describe countermeasures that can be used to counter social engineering attacks.
e. Identify potential opportunities for social engineering in facilities and physical environment.

12. **Describe various cloud-based services and their implications on security.**
    a. Describe the basic functionality of cloud computing.
13. **Explain how shadow IT can present a security risk to a company.**
14. **Explain the security and compliance risks associated with storing data on the cloud.**
15. **Explain the security and compliance risks associated with synchronizing data using a cloud-based service.**
16. **Identify risks relating to cloud-based backups and remote data storage**
17. **Describe risks relating to consumer cloud services (Dropbox, etc.)**

18. **Describe considerations related to ensuring the confidentiality and integrity of personal and company data.**
    a. Explain why data should be classified (i.e. all data does not require the same level of security.)
    b. Describe what is meant by personally identifiable information.
    c. Explain the challenges of data discovery and its implication on compliance.
    d. Identify the concerns in managing and maintaining encrypted data.
    e. Explain the need to understand where and how data is stored and warehoused.
    f. Describe mechanisms for protecting data on mobile devices (encryption, remote wipe, etc.)

19. **Describe the security vulnerabilities associated with mobile devices and the steps you can take to mitigate the risk**
    a. Explain the risk of geolocation and sharing location data with apps.
    b. Explain how app permissions impact the security of mobile devices.
    c. Explain the ramifications of installing Android apps from sources other than the marketplace.
    d. Describe precautions you can take to protect the data on your mobile device (remote wipe, local wipe, locking the device).
    e. Describe the security ramifications of using an on-screen keyboard.
    f. Describe the security ramifications of using your smartphone as a wireless hotspot.

20. **Describe the security issues associated with common applications.**
    a. Explain the risks of enabling macros.
    b. Describe browser security settings and how they impact functionality and security (i.e. cookies, scripts, safe browsing, certificates, phishing and malware protection)

c. Describe email security settings and how they impact functionality and security (i.e. antispam, attachment safety, phishing, digital signature, encryption).
d. Discuss how you can protect against application attack vectors by keeping applications updated.
e. Discuss how you can prevent unauthorized users from modifying a document.
f. Describe, in general terms, the advantages to code signing and the risk of executing unsigned applications and drivers.