CIDM 6341-70 : Cybersecurity

Final TAKE HOME Exam, Summer 2021

Total points: 200

Answer Only FIVE from the following SIX Problems [5 x 40 = 200 points], and please delete the extra ONE

N.B: This is a TAKE HOME exam to assess your competency on current topics in cybersecurity management, especially on with Ch#7 -12. You need to work only yourself for this exam. No group/teamwork are allowed. Handwriting or drawing is acceptable, for example - images/figures answers, you can hand draw and take photo and attach within the exam script. Please try to **make all-in-one file***, do not upload different files.*

Q2. Ch#8 [40 points]

a. [10 points] What is access control and what are the essential processes? Identify at least two approaches used to categorize access control methodologies and list the types of controls found in each.

   a. Access control is the methodology that specifies which resources that an individual may access and use them. Some essential processes of access control are:

      i. Identification
      ii. Authentication
      iii. Authorization
      iv. Accountability

   b. Approaches to categorize access control methodologies are

      i. Controls by characteristics:

         1. Directive
         2. Deterrent
         3. Preventative
         4. Detective
         5. Corrective
         6. Recovery

      ii. Operational impacts are based on their effect on the organization

         1. Management
         2. Operational
         3. Technical

b. [20 points] Briefly explain NIST security control assessment process. [Hint: see figure 8.2]

   a. Organization Preparation – One of the first steps in the process

      i. Implement security controls and notify officials that an assessment is imenant
      ii. Create and implement a communication plan with stakeholders
      iii. Identify and obtain the assessment resources and assemble the team to use them
      iv. Collect artificats necessary for the assesment

   b. Assessor Preparation – This is the second step, it leads to the security assessment plan which then leads to the organizational approval

   i. Collect points of contacts
   ii. Review organization to understand: mission, functions, processes, system structure, and current security controls
   iii. Create a security assessment plan and obtain any artifacts needed to complete the assessment

c. Organizational approval – The third step
   i. Present an appropriately tailored plan to senior leadership that has a balanced schedule, performance, and cost.

d. Assessment – This step is where assessment procedures are developed, and the overall assessment is completed. It will lead to a security assessment report.
   i. Procedure development
      1. Establishes objectives
      2. Sets methods, objects, depth and coverage attributes
      3. Custom procedures and test cases created for the organization and its systems
      4. Schedule and milestones established
   ii. Assessment
      1. Implements the plan and executes the procedures to achieve the objectives
      2. Report findings impartially and objectively
      3. Make specific remediation suggestions and create the draft security assessment reports

e. Organization Oversight – This step leads to a plan of actions with milestones in addition to a security plan
   i. Reviews findings with leadership and identifies actions needed to be taken by the organization
   ii. Creates a plan to address issues
   iii. Updates the security plan (as well as risk assessment)

c. [10 points] Compare two security management models with principles "no read up, no write down" vs. "no write up, no read down".

   a. "No read up, no write down" means that the classification system implicitly negates individuals from reading the output. For example, one could think of it as specific directives that are written from a higher to a lower level. Those directives should not be visible to the lowest level, only as translated from an appropriate level. Similar to the chain of command, a General does not command Privates. The General commands Colonels, who commands Majors, who commands Captains, who commands Lieutenants who then commands the non commissioned officers (e.g., Sergeant) who then communicate the appropriate orders for the privates. The private will only have a piece of the overall plan that he needs to do his part. For example, the private maybe instructed to converge on point alpha and dig in defenses. He would not know that the general plans for another unit to be forcing the enemy towards that position so another unit can ambush the enemy. This way, if that single private is captured, he can only communicate a small part of the overall plan. The "no write up, no read down" could be viewed as a CEO telling all employees about a new product that they will be launching since that information will be disimanted the most accurately without filtering down through multiple levels.

Q3. Ch#9 [40 points]

a. [10 points] What are the critical actions that a management must consider taking when dismissing an employee? Do these issues change based on whether the departure is friendly or hostile?

a. When dismissing an employee, it is critical that management:

i. Disable their access to internal resources (not only lockout their users, but be sure to change master config passwords and do an audit of admin-level accounts to ensure they did not leave a backdoor). This includes logins and keycards.

ii. Have them return any property that belongs to the organization (data, tech, etc.)

iii. Data drives should be secured (not only on the computers but also on the cloud)

iv. Keys to filing cabinets they had access should be changed

v. All personal items should be removed

b. Management should take the same steps regardless of the nature of the termination. Reminders of legal action for retaliation may be called for in cases of involuntary termination; however, at the end of the day, all the same, security precautions need to be taken.

b. [20 points] How can you measure information security management performance? Briefly describe how to design and implement information security measures. [Hints figs. 9.3, 9.4]

a. One can measure security management performance by performance targets. A performance target provides the ability to define what success looks like in a security program. Performance targets are essential to a measurement program because they offer the ability to measure what has been achieved (e.g., have 100% of employees attended security awareness training?). The fields in an adequately defined performance method can include:

i. Measurement Id

ii. Goal

iii. Measurement

iv. Measure type

v. Formula

vi. Target

vii. Implementation evidence

viii. Frequency

ix. Responsible Parties

x. Data source

xi. Reporting format

b. Once the targets have been established, one must continually monitor and act upon the observed results. This usually involves getting developing a business case to obtain the resources needed to address any items that need correction. Then the cycle starts again.

c. [10 points] What are six areas of PCI/DSS Recommended Practices for security management.

a. "Build and maintain a secure network and systems"

b. "Protect cardholder data"

c. "Maintain a vulnerability management program"

d. "Implement strong access control measures"

e. "Regularly monitor and test networks"

f. "Maintain an information security policy"

Q4. Ch#10: [40 points]

a. [10 points] What do you mean by disaster recovery and crisis management?
    a. Disaster recovery is the plan that has been established to deal with any sort of disaster (which could be artificial or acts of God). Crisis management is how an organization deals with the human side of a disaster (e.g., injuries obtained during the disaster). Typically, it is focused on reacting to a disaster and recovering from it to resume normal business operations.

b. [20 points] What strategies can be used to test contingency plans (CPs)? Explain (with proper diagrams/figures) the seven-step contingency planning (CP) process recommended by NIST. How can we implement a CP?
    a. Strategies
        i. Desk Check
        ii. Structured walk-through
        iii. Simulation
        iv. Parallel testing
        v. Full interruption
    b. NIST CPs
        i. Create contingency planning policy
        ii. Conduct the BIA
        iii. Identify any preventative measures that can be done
        iv. Create recovery strategies
        v. Create a contingency plan for IT
        vi. Plan training, exercises and testing
        vii. Maintaining the plan
    c. Implementing a CP

c. [10 points] What is incidence response (IR) plan? "It is important to understand that IR is a reactive measure, not a preventative one, although most IR plans include preventative recommendations." – Explain.
    a. Incident Response Plan – Determines how incidents are handled in near real-time. Any unexpected event is classified as an incident until it is determined to be a disaster.
    b. When an incident has occurred, that usually means you are reacting to something that has happened already. For example, let's look at the old expression about the horse and the burning barn. The horse has left the burning barn (reaction), and all you can do is (react) try to put the fire out and catch the horse. If proper maintenance had been maintained (preventative) on the electrical system in the barn, then the fire would not have occurred.

Q5. Ch#11: [40 points]

a. [10 points] List and define the factors that are likely to shift in an organization's information security environment.

   i. Change in assets (either acquiring new ones or getting rid of)
   ii. New vulnerabilities of assets discovered
   iii. Change in business priorities
   iv. Change in partnerships (either adding new or dissolving)
   v. Personnel changes

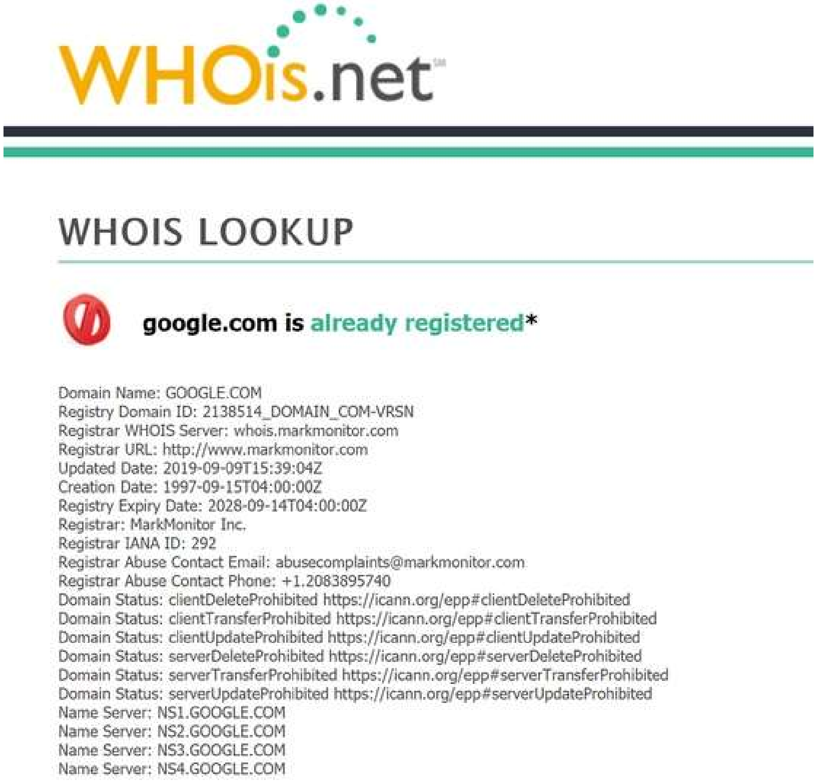
b. [20 points] The Security Maintenance Model is designed to focus organizational effort on maintaining systems. Explain a security maintenance model with five subject areas: External monitoring Internal monitoring Planning and risk assessment Vulnerability assessment and remediation Readiness and review.

   i. Externa Monitoring: Focuses on monitoring threats to organizational information systems from the outside. Intelligence can originate from Vendors, CERT Orgs, public network sources, and membership sites,
   ii. Internal Monitoring: Monitoring of the internal network, assets, defenses and keeping them documented. This can be done by building an inventory of assets, governance, and real-time monitoring systems.
   iii. Planning and Risk Assessment: Continual process of identifying area's to improve and conducting re-assessments. Also is responsible for creating projects to address any identified risks. Should work to establish formal IS program, project management and encourage everyone throughout the organization to evaluate risks.
   iv. Vulnerability Assessment and Remediation: Focus is to identify any vulnerabilities and address them. Should use identified vulnerabilities and brief management to decide if the risk is palatable or if it needs addressing.
   v. Readiness and Review: This is where readiness is assessed, and policies are reviewed at defined intervals. This ensures that the previously established policies, programs, and plans are still effective.

c. [10 points] What is penetration testing? Explain the figure below in terms of vulnerability assessment and penetration testing.

   i. Penetration testing is the process by which an outside party will attempt to penetrate the companies network in the same fashion as an actual attacker. Highly skilled individuals usually do penetration testing with customized attacks. While there are similarities to vulnerability assessments, the fact that these are outside consultants who do penetration testing full time provides a level of attacks that most internal infosec pros don't like to be seen. Additionally, since they are external, they are more likely not to be blinded by possible assumptions that those who build the systems might have.
   ii. The image below shows how vulnerable the domain is too bad actors. Since it is locked down, this means that it is unlikely to be vulnerable from that perspective.

It does list the name servers (which are hosted on the same domain), which is generally considered bad practice in my experience. If the domain does get upset for some reason, the same servers that should be providing the correct information about how to get to the domain are a part of the same domain (thus, it's a circular issue). Pen testing could be done based on trying to take over the name servers and see if there are any vulnerabilities that can be taken advantage of.



WHOis.net

WHOIS LOOKUP

google.com is already registered*

```
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
```

Q6. Ch#12: [40 points]

a. [10 points] Access control encompasses four processes: Identification (I), Authentication (A), Authorization (A), and Accountability (A). A successful access control approach always incorporates all four of these elements (IAAA). Briefly explain what do we mean by IAAA?
   a. Identification – The person or entity that should have access to a system. Usually identified by a user name of some sort but can take other forms (e.g., an access keycard)
   b. Authentication – This is how the entity being identified is able to validate that they are whom they say they are. There are three types of authentication mechanisms:
      i. Knows – e.g., password
      ii. Has – (e.g., One Time Password like Duo)
      iii. Produce (e.g., biometic)
   c. Authorization – What the entity can "do" or "access" after they have been authenticated (e.g., system admins can install software onto a PC; however, normal users cannot)
   d. Accountability – Documentation of what has been done (e.g., audit log)
   e. When combined, these aspects are powerful in maintaining a secure environment. Having multiple layers of defense (especially when it comes to authentication, I'm a big fan of requiring at least 2 forms of authorization) is always ideal.

b. [20 points] Write notes on any two of the following:

   i. Firewall – A firewall is a system that separates an internal network from the outside. It is usually responsible for routing inbound traffic from external sources internally. It can be advanced by doing packet-level inspection to determine if there might be an attack being done. Firewalls are generally considered the first line of defense for a network to prevent bad actors from accessing data within the LAN.
   ii. Biometrics authentication mechanism – Biometrics can be used as an authentication mechanism so one can prove that they are themselves. This can be fingerprinted, facial or retinal. They should not be a primary mechanism in authentication because they cannot change (well they could, but usually, that requires disfigurement). They could also be fooled by some mechanism (you used to be able to fool fingerprint scanners with superglue and an imprint of the victim's fingerprint). I typically look at biometrics as a secondary authentication method. For example, you must provide a password (or pin) in addition to the biometric. This way the biometric authentication is used to supplement something that can be changed in case of compromise.

d. [10 points] List some ways of managing cryptographic controls.
   i. Here are some ideas on manage cryptogratic controls:
      1. Controlling and securing keys, this ensures that you will always be able to access the data. Making sure the keys are secure (e.g., locked in a physical vault, and never recorded electronically after their initial conception). Keys can be changed later on; however, it requires one to decrypt the data first!
      2. Ensure that keys are exchanged with the intended party, and not with someone pretending to be them. The book recommends always verifying public keys in a public key exchange.
      3. Have plans in place to mitigate any weaknesses that a particular system has. These should be regularly reviewed to ensure that they continue to be as secure

as you believe them to be. TLS 1 and 1.1 are good examples of protocols that are old and out of date with vulnerabilities. Keeping apprised of such things ensures that you are able to stay ahead of the attack curb.