**CS 5601 Exam 1 Modules 1 through 7**

**Adam Hoffmeister**

1. **The NIST Computer Security Handbook approach to computer security has eight major elements. What are they and briefly describe what each one does? (tell me in your words) (5 pts)**

* Security should protect the organization
  + Protects information, hardware, and software through safeguards. Allows physical and financial resources to be guarded.
* Security is an asset of proper management
  + Computers are critical to an organization’s workflow.
* Security should be cost-effective
  + It should be proportionate to the value and the amount of reliance of the system.
* Security roles and accountability should be specific
  + Users of the computer systems need to adhere to responsibilities or polices.
* Security should be discussed to system users
  + System owners should let users know that the proper measures are in place.
* Security requires a thorough and in-depth approach
  + Environments require specific setup for every piece of software. Documentation and manuals need to be read. Training for system users may also be needed.
* Security should be reevaluated periodically
  + Systems rapidly change as do the threats and risks associated with it. Software, policies, training, etc. may need to be updated.
* Security can be limited by social issues
  + Measures need to be put in place, but they should be balanced to not interfere with the end user.

1. **An employee is using your organization's servers to host books that are in the public domain. According to your security program you are writing for class, would this be in violation of any policy, if so, please describe. If not, would your security program require a new policy? (Your answer will be compared to your security program to date) (5 pts)**

This would not be in violation of any of my current policies. As the material is open for the public, it may be hosted on the organization’s servers.

1. **Explain why computer security should be periodically reassessed. (5 pts)**

Computer security needs to periodically reassessed because technology rapidly changes. As machines update and the organization uses more software, polices and training need to be reevaluated. New malware and threats can cause harm if patches and updates are not installed.

1. **When writing a security policy, what 5 questions should writers ask themselves to ensure they will end up with well written policies? (5pts)**

Who, What, Where, When, and Why

1. **There are three foundational principles that form the basis for most security plans and controls. Name them and describe each one. (5pts)**

* Confidentiality – only allows authorized users to view information
* Integrity – only allows authorized users to modify information
* Availability – ensures that authorized users can access data, or system, when needed

1. **If the cost of controls to deal with a risk associated with a specific asset are greater than the value of the asset, what is the appropriate risk management decision? Explain why. (5pts)**

The asset should be done away with if it the cost of controls is greater than its worth. It would cost too much to protect or mitigate the risks, so the asset should just be removed.

1. **In regards to information classification, why is it important to establish a classification scheme to classify an organization’s information? (5pts)**

Establishing a classification scheme provides an organization a basis to secure their information. It is important because they need to maintain the schemes for their documents, ensuring they are storing them on the proper systems and folders.

1. **Why is it considered inappropriate to include how to do something within a policy? (5pts)**

Polices are meant to be broad to cover the subject to avoid having to re-write them often. Further details can be defined by standards and guidelines.

1. **What are assets and some risks? Provide a few examples of the asset and risks. (5pts)**

Assets: inventory, buildings, cash, information, data, hardware, software, services, documents, etc.

Risks: treasury, revenue, contract, fraud, environmental, regulatory, technology, etc.

1. **Your supervisor is very busy and asks you to log into the HR Server using her account ID and password to retrieve some reports. Describe what you would do. (5pts)**

I would follow the security policy to see how I should proceed. It should point to the guideline or standard telling me how to approach the situation.

1. **Why are Human Resource security policies dealing with terminations important? There are quite a few attributes to this questions so be thorough as you can with the information provided during the class and reading. (5pts)**

HR security policies for terminations are important because situations dealing with employees getting fired or let go can get intense. The employee could abuse their previous permissions, leak sensitive information, cause physical threat, or steal company secrets. If the situation is handled correctly, the employee’s tasks can be handed off to other employees while their permissions get revoked. Otherwise, they need to be escorted out of the building with their access revoked.

1. **When deciding on a risk assessment design, there are two standard methods for an organization to determine what is at risk and by how much, and deciding which is the highest priority. Describe what you would design and why you would choose the method(s) including reasons why one is preferred over the other. (5pts)**

The risk management model should be chosen with the organization’s objectives and strategies in mind. In summary, the two standard models are similar in their goals, but vary a bit in their steps. General risk management model is more inclusive to an organization’s entire design. It includes asset identification, threat assessment, impact definition and qualification, control design and evaluation, and residual risk management. While the software engineering institute model is more for the development of individual programs. Unlike the general risk model, it doesn’t contain asset identification. It includes identify, analyze, plan, track, and control.

1. **When designing a training program, would it be sufficient to create one single training program for the entire organization? Explain your answer. (5pts)**

No, there are at least two audiences that need different information: generalized users and specialized users. General users are everyone and includes the common practices. Specialized users are everyone who needs advanced training, such as management and system security. This ensures that all employees are sufficiently trained for their respective duties.

1. **Hackers and cyber criminals usually perform their activities according to a well structured plan. Please describe what these steps are. (5pts)**

* Reconnaissance – gather easily found public data
* Probing – ping and probe sweeps, figuring out OS, etc.
* Attempt to exploit vulnerabilities – such as the latest 0day attacks
* Attempt to gain access through login credentials – through brute force or social engineering
* Physical theft – robbing storage drives, systems, etc.

1. **What is the confidentiality model and property that ensures that a classified object can only be read/written by a subject with the same classification label? (5pts)**

The Bell-LaPadula Security model’s strong \*-property ensures that an object can be read/written by a subject with the same classification.

1. **What are the three primary integrity goals of the Clark-Wilson Security model? (5pts)**

#1 Stop unauthorized users from making modifications

#2 Stop authorized users from making unauthorized or invalid modifications

#3 Keep internal and external consistency

1. **Describe Least Privilege and its importance. (5pts)**

Least privilege is a form of access control that says an individual should only have the needed permissions to perform their tasks and no extra privileges should be granted. This is important because it limits possible damage that could affect the organization.

1. **Explain why a constrained data object cannot be modified by a subject with the Clark-Wilson Security model. (5pts)**

Constrained data objects are subject to integrity controls. The integrity verification process has to ensure that the data meets integrity constraints. This means that data cannot be modified directly by the user. The transformation process must be used, so multiple individuals are required. This maintains separation of duties for critical functions.

1. **Which of the Access Control Methods (Access Controls.pdf) would be best suited for a business that has thousands of employees, hundreds of thousands of files/applications/devices that need appropriate access controls and there is a high turnover rate of employees? Explain your answer. (5pts)**

Role Based Access Control (RBAC) should be used in the case where there is a high turnover rate. Employees can be assigned and unassigned to a group in order to get their set of permissions. This skips the daunting task of assigning permissions on a per user basis.

1. **List the possible forms that can be used in multifactor authentication (5pts)**

In addition to passphrases, additional forms of authentication be instilled, such as:

Mutual authentication – each communicating party is verified by the other party through a mechanism.

Tokens – uniquely generated, time-based pin to respond to a Challenge and Response authentication.