**CS362 Exam #1**

1. People, as a whole, are statistically the weakest link in security measures. Of these, insiders are where most security breaches originate from. These people already are allowed access to at least a limited portion of the system that data thieves intend to steal from. The most dangerous thing about these insiders is that they may do this unwittingly. Most common of that sort of trickery is social engineering, such as phishing. These threats may be mitigated through policies, procedures, training, and monitoring by the security personnel for the system.

Ref. Lesson 1 ppt. Slide 33

2. As currently, my security policy does not have a policy regarding outside content. That will need to be remedied. Hosting unnecessary content should be against policy. Public works, while not in any way worth anything to the company, still take up space and could provide an exploit for hackers. Also, public works, since they are not worth anything, can be acquired by anyone for free, so any cost spent by the company to host them is inherently flawed logic which costs the company money.

3. A way for a thief to gain access to a system can happen somewhat easily. First, research: Find out as much about the company and system as you can. Who has access? Is it a tiered system? What ways can you contact the system? Do they have a firewall? What can you steal? How do you use it and get it out? One way to do so is targeted phishing. An email saying something to effect of “Your account has been compromised; please send back the answer to your security question to verify your identity.” I give this example on the basis that there is a security question. If no one was to fall for that, I’d find someone’s Facebook, and grab a family picture. I’d put it as an attachment saying something to the effect of “Give me the password or this picture is gonna change. No police.” After I got an account password, I’d poke around the system quietly, seeing what there is to access. If need be, I’d find a way to elevate my privileges. After finding everything I would want, I’d wait till there was few personnel on site, and break into/attack the sensitive areas and get the information I wanted. This all can be avoided through a robust spam filter and training to not respond to phishing under any circumstances.

4. Who? What? Where? When? Why?

Ref. SANS Institute InfoSec Reading Room, page 1

5. Confidentiality – Only authorized individuals can access Information

Integrity – Only authorized individuals can edit Information

Availability – System is accessible when authorized user wants

Ref. Lesson 2 ppt. Slide 9

6. The appropriate measure for risks that cost more to protect than they are worth is to define them as acceptable risk. These risks should not have the security measures placed on them since it’d be simply easier to replace them. An example of overkill protection would be a firewall, encryption, and premium virus scans on a digital copy of “Frankenstein”. It doesn’t make sense to spend hundreds of dollars to protect something that realistically worth next to nothing.

Ref. Lesson 3 ppt. Slide 13

7. It is important to establish a classification system so that you can identify which assets need the most protection. Appropriate levels of security would be taken with the appropriate assets. Assigning too much or too little security to assets is bad in either direction.

Ref. Lesson 3 ppt. Slide 24

8. A policy is brief, high level, and broad statement that rarely changes. A description of how to do something does not belong in a policy since that description may change yearly, whereas the policy needs to last as long as possible. A description of how to implement a policy belongs in the standards or guidelines, since those do not require the formal review that policies do.

Ref. Lesson 2 ppt. Slides 20-25

9. The first process in risk management methodology is to identify risks. Once you identify risks, you can begin to classify their severity and properly plan to protect them. By doing this, we can deter any sorts of loss to the company, allowing more profit for the company and trust from employees and customers.

Ref. Lesson 3 ppt. Slide 13

10. In an organization that heavily relies on Information Technology, everyone is responsible for security of information, assets, intellectual property, etc. Everyone from the CEO to the mice in the walls plays a part in keeping secure the protectable assets. This is because everyone is a potential target, thus everyone needs to be on their guard.

Ref. Lesson 2 ppt. Slide 2

11. Human Resource policies dealing with termination are serious because they deal with a permanent and, if necessary, forced solution to a problem. Terminating an employee can leave some ill will, which may be acted upon. A terminated employee should have their role in the system changed to ‘Terminated’, should you be using a role based classification system. This changes their access to the system to very little, so as to protect the company from any malicious intent on the terminated employee’s part. Termination also needs to be taken seriously since if there was a misunderstanding, you would lose at the very least your employee’s trust, if not the employee themselves. Having termination as a common security measure for minor infractions causes demoralization and a sense of ‘Us vs Them’ with the security officials.

Ref. Lesson 6 ppt. Slide 18, Lesson 8 ppt. Slide 64

12. The 2 standard models of assessing risk are to qualitatively assess the risk or to quantitatively assess the risk. I would design a system that qualitatively assesses the risk to the system, since you can’t purely determine an asset’s quantitative value without determining its quality to some degree. Some of the value into an asset is not purely dollar value. For example, having automated birthday messages to employees doesn’t do anything for profits so, at best, it costs nothing for the company to do. However, it fosters goodwill with employees, allowing them to feel that the company does indeed value them. That is something that could not be easily described quantitatively.

Ref. Lesson 2 ppt., Lesson 3 ppt. Slides 35-51

13. It is not enough to design one training program since there are different levels of security to a system. A standard employee does not need to know how to build a robust firewall, for example. You also need to change up your security training so that people will not get bored and eventually tune you out, thinking they know everything already. This also helps you introduce new security topics.

Ref. Lesson 8 ppt. Slide 50

14. The requirements for building a robust training program are as follow. First, you need to identify your assets. This is part of risk management. Once you’ve identified your assets, figure out how you’re going to go about protecting them. Determining which users are using which assets. Design your program to train your employees on how to mitigate these risks. Have guidelines and rules posted in an easily accessible location. Re-train periodically on old concepts and introduce new ones when appropriate. Knowing is half the battle, so you need to make sure your employees know what they’re responsibilities are, and how they may be affected.

Ref. Lesson 2 ppt.

15. The model and property that ensures that a classified object can only be read/written by user of the same classification label is the Bell-LaPadula model using the Strong \*-Property.

Ref. Lesson 5 ppt. Slide 9

16. The primary integrity goals of Clark-Wilson are:  
i. Prevent unauthorized users from making modifications  
ii. Prevent authorized users form making un-authorized or improper modifications  
iii. Maintain internal and external consistency

Ref. Lesson 5 ppt. Slide 20

17. Least Privileges means to grant access to as few areas of a system for a user while not impeding their ability to do their job. If a user does not need access to a portion of the system then it only distracts them. It also creates a hole where a security breach may happen. (e.g. The custodian does not need access to the financial delegation of the system)

Ref. Lesson 7 ppt. Slide 16

18. A constrained data object cannot be modified by a subject in the Clark-Wilson model because that would violate the 2nd integrity goal of the model. Constrained data objects can only be modified by a trusted transformation process, which have restricted access on them. This makes sure that only authorized users will makes changes through a process that is recognized by the system. The integrity of the system is preserved while still being usable.

Ref. Lesson 5 ppt. Slide 23