# ISEC 325 Homework 11

Answer the following questions based on your reading of the text books, the module key points, and the instructor’s presentation this week.

1. [2 points] List and describe the components of contingency planning.

The first component is business impact analysis which will provide information on what needs to be recovered, what is affect, and the threat. The second component is the incident response plan where they will document the actions that should be taken while the incident is in progress. Next is the disaster recovery plan where they determine how bad the threat was and the recovery needed. The final component is the business continuity plan which is when they determine the next steps to take hand how to continue after the attack.

1. [2 points] What is the primary goal of digital forensics?

The primary goal of digital forensics is to take the data from electronics to be able to use it for evidence.

1. [2 points] What are the major steps in a business impact analysis? Briefly describe what happens in each step.

The major steps for BIA are first determine the processes and recovery, then determine the resource requirements, and finally find the recovery priorities for the system resources.

1. [2 points] Name and describe the four steps in collecting digital evidence.

The first step is to identify the sources of the evidence, next is to authenticate the evidence, then collect it, and finally make sure to maintain a documented chain of custody.

1. [3 points] What are the three broad categories of incident indicators? What types of events are considered possible indicators of actual incidents? Probable indicators? Definite indicators?

The three broad categories of incident indicators are possible, probable, and definite. Possible indicators are the presence of unknown files or programs, as well as unusual system crashes or use of resources. The probable ones are when there are activities at unexpected times or new accounts appear without knowledge of them, there are also the reported attacks and notifications sent from IDS. Definite is when there is use within a dormant account or logs have been missing or modified, there is also the presence of hacker tools, and notifications from a peer or the hacker.

1. [3 points] Describe the components of an incident response plan.

The first component is to identification of what the attack is, the action plan, the second is the response which is how are they going to respond to the attack, third is containment and eradication where they corner the threat and have it removed, finally there is recovery where they determine what has been lost, what can be brought back, and how to move forward.

1. [2 points] Describe the effects of cryptography on the practice of digital forensics.

Cryptography is used to encrypt data so when it is collected to be used as evidence, if they do not know the key then it will be hard or even impossible to crack in some cases making the evidence unusable.

1. [2 points] What is an after-action review? What are the primary reasons for undertaking one?

The after-action review is a means of debriefing and determining what happened and why during steps of the process. The main reason for undertaking one is to get everyone on the same page of why something happened and to determine if the next steps need to be changed as outside variables can cause some steps to become obsolete and the original plan will need to change accordingly.

1. [7 points] Examine this journal article on cloud computing and digital forensics: “[Cloud Computing: Pros and Cons for Computer Forensic Investigations](http://infonomics-society.org/wp-content/uploads/ijmip/published-papers/volume-1-2011/Cloud-Computing-Pros-Cons-for-Computer-Forensic-Investigations.pdf).” Briefly summarize the article. What are the problems associated with digital forensics on cloud computing platforms?

New link: <http://infonomics-society.ie/wp-content/uploads/ijmip/published-papers/volume-1-2011/Cloud-Computing-Pros-Cons-for-Computer-Forensic-Investigations.pdf>

The advancement of technology has led to the need for computer forensics to be able to gather digital evidence and help protect people online. The introduction of cloud computing has led to more challenges for computer forensics and how it needs to go about handling it. Some problems that cloud computing platforms have for digital forensics is that they are not prepared for computer forensics meaning that the level of security they have causes trouble when needing to collect evidence. There is also the idea of how it is harder to pin the gathered evidence as with the cloud computing, the data is touched by several different people each time. There is also difficulty in maintaining a chain of command as the information is stored in the cloud storage which has more data from others and is not owned by the offender meaning that there can be trouble getting access to it.

1. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about.  In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This week we looked at the contingency planning, incidence response, and digital forensics. I always find it interesting to learn more on the security side so learning about the digital forensics was quite fun. I know that there are several different levels of difficulty when it comes to this based on where the evidence is stored and who needs to be talked with to acquire it. If they plan on using a folder saved on a person’s computer for evidence then it is easier to access as they can get a warrant to search the computer. This is easier when it is just affecting the charged, the cloud computing is harder as the evidence is saved onto the cloud system run by the company and has to take a longer approach to get the evidence as some may not want their system to be gone through. I remember when Apple was in the news because they would not give a back door into their systems so the authorities could access a phone to use in a case. This became the ethical dilemma of is the evidence worth pursuing or is it better that Apple protects its users from possible threats these backdoors could cause. This is one of my favorite ethical dilemmas as both sides have very valid points and different priorities in the scenario.