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.

   Business impact analysis (BIA)- is the first major component of the contingency planning process, it provides the contingency planning management team with information about systems and threats that they face. It provides an assessment of the system operations that the organization absolutely needs to keep going during and after an event.

   Incident response plan is the actions an organization should take while an incident is in progress. The incident response plan deals with the identification, classification, response, and recovery from an incident and provides answers to questions that victims might pose in the middle of an incident. The incident response plan also enables the organization to take coordinated action that is either predefined and specific or ad hoc and reactive.

   Disaster recovery plan covers the preparation for and recovery from a disaster, whether natural or human made. A disaster has occurred when either of two criteria are met the organization is unable to contain or control the impact of an incident or the level of damage or destruction from an incident is so severe that the organization cannot quickly recover from it. The key role of a disaster recovery plan is defining how to reestablish operations at the location where the organization usually operates.

   Business continuity plan ensures that critical business functions can continue if a disaster occurs. While the disaster recovery plan is managed by the IT community of interest. The business continuity plan is managed by the CEO or an organization. It is activated and executed concurrently with the disaster recovery plan when the disaster is major or long term and requires fuller and complex restoration of information and IT resources. If a disaster has rendered the current business location unusable, there must be a plan to allow the business to continue to function. The business recovery plan reestablishes critical business functions at an alternate site.

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

   The primary goal of digital forensics is to identify, collect, preserver, and analyze electronic items of potential evidentiary value so that they may be admitted as evidence in a court of law, used to support administrative action, or simply used to further analyze suspicious data.

3. [2 points] What are the major steps in a business impact analysis? Briefly describe what happens in each step.

   The three major steps in a business impact analysis are:

1. Determine mission/business processes and recovery criticality. Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.

2. Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

3. Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

4. [2 points] Name and describe the four steps in collecting digital evidence.

    1. Identify sources of evidentiary material- this is the same as gathering bloodstains and fingerprints with digital forensics you are looking for things like disks in a desktop or laptop computer, disks in external storage encloses, memory sticks or cards, PDA's, Cell phones, Storage devices like mp3 players, Optical storage like CD's and DVD's, Network storage, Disks attached to servers, Storage attached to a storage network, files on network-attached storage devices, logs on severs, routers, firewalls, or centralized logging servers. Volatile information is information on a computers memory that can be lost if it is shut down.

    2. Authenticate the evidentiary material this is making sure that the evidence is authentic, and it is done by means of cryptographic hashing. They do this by collecting a file or data into evidence and then feeding that data through the hash function. When the evidence is collected its hash, value is calculated and recorded later the hash value can be recalculated to show that the item has not been modified since its collection.

    3. Collect the evidentiary material the first step when collecting evidence is deciding whether to collect the evidence live or dead. Live is where the system is running, and dead is when the system is powered down and the files are then collected. There must be no changes made to the evidence. To prevent doubts regarding the handling labels and seals are used as well as specialized packaging. Evidence envelopes are preprinted with a form that collects relevant information about the evidence like whom and where the information is collected. Great care must be taken so that evidence is not contaminated in order to prevent contamination sterile media is used. If volatile information is found live acquisition must be used by using tools like Windows Forensic Toolchest. A dead acquisition is when the

computer is powered down and drives are removed and imaged. In order to not corrupt evidence write blockers are used when imaging the disks so that data is not written to the disks when they are imaged.

4. Maintain a documented chain of custody demonstrates that the evidence has been protected from accidental or purposeful modification at every point from its collection through analysis to presentation in court. Chain of custody is a legal record of where the evidence was at each point in its lifetime as well as documentation of each and every access there was to it. The evidence must also be properly stored where it is protected, controlled access environment with sound processes governing access to its contents. The environment the evidence is stored must be temperature and humidity controlled, free from strong electrical and magnetic fields that might damage the items, and protection from fire and other physical hazards. The storage facility can be a specialized evidence room or a locked filing cabinet in an office.

5. [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. The type of events that are considered possible indicators of actual incidents are the presence of unfamiliar files, presence or execution of unknown programs or processes, unusual consumption of computing resources and unusual system crashes. Probable indicators would include activities at unexpected times, presence of new accounts, reported attacks and notification from your intrusion detection system. Definite indicators include the use of dormant accounts, modified or missing logs, presence of hacking tools, notifications by a partner or peer, and notification by the attacker or hacker. Loss of availability, loss of integrity, loss of confidentiality, violation of policy and violation of law are also incident indicators.

6. [3 points] Describe the components of an incident response plan.

   The components of an incident response plan are Identification which begins with a trigger or circumstance that caused the IR team to be initiated. Examples of triggers include a phone call from a user to the help desk about unusual computer or network behavior, notification from a systems administrator about unusual server or network behavior, notification from an intrusion detection device, review of system log files indicating unusual pattern of entries, loss of system connectivity, or device malfunctions. The IR teams lead person then decides if the IR team must be activated. Identification involves data collection where data is routinely collected to properly detect and declare incidents. Events must be classified as they occur incident candidates can be actual incidents or false positives. The IR team must classify incidents such as actual, probable, and definite indicators. Response is what must be done to react to a particular situation. Response involves notification by phone call or message. Documenting an incident is the next step the documentation should include who, what, when, where, why and how and interviews are conducted in this step. Containment/Eradication is where the incident is stopped and

containing the incidents impact. Some containment strategies include disabling comprised user accounts and reconfiguring a firewall to block questionable traffic. Recovery is the last step where the IR team must identify and resolve the vulnerabilities, restore the data from backups, restore services and processes, restore confidence across the organization which may involve a memo or email assuring that the incident was handled and the damage was controlled, and an after action review is conducted to review and learn as much as possible about the incident.

7. [2 points] Describe the effects of cryptography on the practice of digital forensics.

   Data collected by a forensic investigator that is encrypted is not readable without the key. Some forensic products offer brute force attacks against the encrypted information by using dictionaries. The same rules apply as with other cryptography and passwords strongly encrypted evidence may be very difficult to decrypt.

8. [2 points] What is an after-action review? What are the primary reasons for undertaking one?

   An after-action review is a detailed examination of the events that occurred from first detection to final recovery. The primary reasons for undertaking an after-action review are to allow the team to update the IR plan, the AAR is recorded so that it can be used as training for future staff. The AAR is used as a review tool allowing the team to examine how it responded to the incident. The AAR is also a historical record of events.

9. [7 points] Examine this journal article on cloud computing and digital forensics: "Cloud Computing: Pros and Cons for Computer Forensic Investigations." Briefly summarize the article. What are the problems associated with digital forensics on cloud computing platforms?

   The article talks about the growing popularity of cloud computing and how it presents several challenges to digital forensics. The first note of issue the author brings up is that data in cloud computing is stored in many different locations. Because the data is mobile because it is moved amongst servers it may be difficult to seize the original data with multiple copies in existence, in contrast this makes it nice for administrators who have multiple backups they can use and don't need to worry about the original data for court purposes. He describes two different cloud computing models Google and Amazon to give us an idea of how cloud computing works. He then goes over the different types of computer forensics in this paper he states digital, intrusion and network forensics. In explain computer forensics he goes over the same steps we covered in our book except he makes a point to talk about timelining and how it is important to collect evidence that can be pinpointed to a specific time. Computer forensics makes the case that cloud computing was not set up from the start for computer forensics however the cloud computing side has used a loophole in that computer forensics isn't and inherent part of data security. Computer forensics can however be used in cloud computing with logging but needs to be more robust as physical devices cannot be collected. The author then describes virtualization and how virtualization is becoming more and more popular with servers. While virtualization has the benefit of being able to take snapshots it also presents the problem of if the VM is booted in a different environment that you could run into the problem of contaminating the

data as it has been changed by the new VM system. The author notes there are advantages of using cloud computing like the ability to run a virtualized server, the ability to utilize vast data and inbuilt hash authentication for authenticating disk images. The ability for several users to be able to use the same resources is also considered to be an advantage as well as a disadvantage because even though it is much quicker to gather evidence it has not been proven to be forensically sound. He states the main drawback of cloud computing is the acquisition of data. The search and seizure procedures used in the conventional computer forensic process are impractical because of the way the data is stored in the datacenters. Chain of custody is also an issue relating the acquisition of the evidence. With cloud computing investigators are unable to conform to the ACPO guild because the principles of the guide cannot be met. He leaves us in his conclusion saying that neither cloud computing nor forensic investigators have taken up the challenge, but the ball is in the forensic investigators court.

10. [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.

    I work in manufacturing at an essential business, we have had a lot of people gone and I have been forced to work a 19-hour day and a 16-hour day this week aside from my normal schedule. I didn't get as much time as I would have liked with this material. I think the questions can be a bit tricky as some of the answers really are several pages of text. I read the material and got a lot out of it. Disaster recovery had been an area I didn't have as much interest in but the incident response part of the chapter was very interesting to me and I even took notes on the organization that certifies for it because I was very drawn in by incident response. I thought computer forensics would go deeper in the means of how they obtain the data, but I understand the significance of getting evidence right as it is used in court.

    I also wanted to thank you for the course very much. I really enjoyed it. I really appreciate that you take the time to go over the book in detail and give us your own experience and times where you do disagree with what the book is laying out. I don't know if you teach any of the other cyber security classes, if you do I will look out for you and hope to see you in the future even if it is at a Franklin event. Stay safe and I hope the virus end soon they are killing me at work. It is very difficult to do your best when your being pulled in so many directions. Thank you again.