**CS 5601 Exam 4**

**Adam Hoffmeister**

1. **What does RPO and RTO stand for and why are they so important? (10 pts)**

RTO - Recovery Time Objective: The length of time that a process/data needs to be recovered in which is acceptable by the organization.

RPO - Recovery Point Objective: The length of time and amount of service needed for a business to be able to continue functioning to avoid undesirable consequences due to the failure.

These are important because they define the importance of recovering a disaster as quickly as possible. It is very imperative for a company to maintain as much uptime as possible so they can operate their normal day-to-day activities. Without a plan, it would be difficult to consistently meet these objectives.

1. **You have been promoted to Security Officer after a major data breach has occurred and the previous Security Officer resigned. You discover that there is not on official process for defining a forensic response plan. You are required to create a detailed process for the business to follow on all future investigations. Use Slides from Lesson 19, SP 800-86 and/or A Ten Step Process for Forensic Readiness.pdf on Canvas. (40 points)**

1. Examine the central, system, and network logs before accessing the machine  
2. Investigate the potential system issue  
- Do not use the utilities on the system  
- Do not open files or start any applications  
- Document current memory, swap files, processes, and open files   
3. Immediately report the situation even if it doesn’t seem important  
  
If action is needed:  
1. Unplug the system from the network  
2. Escalate the situation to CIRT  
3. Secure more logs (mail, DNS, network service) with another individual, or record yourself   
- Ensure they are labeled and stored correctly  
- Keep a log book with the correct labels  
- Log identifying marks and damage  
- Protect and store it properly in the evidence room  
  
In the case of unauthorized access:  
1. Engage the forensics team (they will investigate, provide analysis, and legal)  
2. Report to law enforcement immediately  
3. Collect evidence (documents, verbal statements, logs, etc)

For the future, a response team should be established with budget for proper training. Also, a chain of custody needs to be established to handle the evidence properly.

1. **DRP Scenario (50 Points)**

I classified the risks into the following:

* Operational – Affects, or will affect, the day-to-day operations
* Availability – Affects system uptime during a disaster and recovery time
* Security – Affects the safety of a system or network
* Reputation – Affects the wellbeing of the business or employees

Needed changes:

* **Generator:** Not large enough generator to keep both the IT components and the HVAC running at the same time.
  + Availability risk.
  + The generator should be big enough to run the IT components and HVAC. It needs to be regularly tested. If possible, another incoming power line needs to be ran from an additional utility company for additional backup.
* **UPS:** They do have a UPS capable of keeping all servers and HVAC running for 15 minutes.
  + No risk, this is well.
  + The UPS should be able to last long enough for systems to be shut off or for the generator to start up.
* **BCP/DRP:** Nothing currently documented.
  + Operational risk.
  + In the case of a disaster, this would be an issue. The staff needs to have a clear policy and guidelines to follow. Especially in the case of an emergency when tension is high.
* **Backups:** Onsite disc-to-disc backups using incremental type of a backup plan. There are no offsite copies. Backups run nightly and have a very hard time completing overnight. This is becoming an increasing problem
  + Operational and availability risk.
  + Daily delta backups should be made, and weekly full backups should be made. Both need to be replicated and kept off site for a minimum of 7 days. In the case of disaster, a full backup can be used with the deltas applied.
  + As there are medical records, follow all laws and regulatory guides for frequency and retention of those backups.
* **Data Segregation:** Each client has a segregated storage area.
  + No risk, this is well.
  + This keeps information consolidated to individuals.
* **Data Protection:** Data not encrypted at rest. Servers are running Antivirus. No host firewalls
  + Security risk.
  + Any financial and medical data needs to be encrypted. All machines and servers need an antivirus and a firewall. The firewall should be equipped with packet filters, ACLs, application layers proxies, and network interface weighting.
* **Networking:** Router ACL’s only, no stateful firewall, no IDS/HIDS
  + Security risk.
  + Wireless access points need to have 802.1x encryption. A stateful firewall can be deployed before the router. The IDS can be deployed before the financial and medical database server.
* **Internet:** Single ISP providing 1000Mbit connection is nearly saturated currently
  + Availability risk.
  + An additional line from another Internet provider should be ran; this can also help with redundancy. Also, a mobile data service provider would be useful as a third backup.
* **Servers:** all are real hardware running raid storage system, one or more server per client depending on their needs. Must install new hardware as capacity grows for client. This can require replicating data over to the new installation resulting in data being offline for the client during the process.
  + Operational and availability risk.
  + The servers should be backing up regularly as they are on RAID. If possible, processes should be abstracted to Amazon AWS. This would prevent them from having to introduce downtime when upgrading their machines. Otherwise, they need to be implementing hardware redundancy to keep the client online. They could load balance all users to the redundant server while porting the data.
* **Operations Personnel:** One network engineer who knows all the router configs/passwords who doesn’t share with his assistants. Two system admins who insist on writing all the mission critical code themselves but do not allowed to be code reviewed. Data center does have at least one person monitoring the system 24/7. However when issues arise, the person is over tasked in processing the events. There is no CIRT. The rest of the staff live anywhere from 30 minutes to 2 hours away.
  + Many risks: operational, security, availability.
  + Configuration files should be copied to network storage. Passwords need to be inputted into a password manager, or properly traded through a public key infrastructure.
  + Any application working with financial, employee, or customer data needs to have a formal code review and inspection. Other work requires a team review, regardless of the application. For quick patches or bug fixes, the code can be passed around to get it deployed quickly.
  + The data center should have someone on staff 24/7 with an additional assistant available on call. This individual should be located close to the facility.
  + There needs to be a CIRT made up of the IT department, a member of legal, and public relations.
* **System Administrators:** All share the root/admin password
  + Security risk.
  + Each administrator should have their own account (with least privilege). This is more secure and allows for logs to be properly made. Otherwise, the user of root is unknown.
* **Budget:** Limited currently, but executives are concerned and willing to allocate whatever you need.
  + No risk, this is well.
* **Change Management:** No formal change management exists. Configurations are not backed up on network devices. Systems at least have their configurations backed up.
  + Availability risk.
  + A procedure needs to be made for change of management. It should involve description, priority, date, etc. If nothing is established, employees could become annoyed. All configurations need to be backed up on network storage.
* **Risk management:** Nothing formal, but most of the staff are extremely worried about the business be able to continue in case of an emergency. Not to mention the businesses would not have access to financial records.
  + Reputation and availability risk.
  + With the proposed changes, public relations can announce the updates. Employees should be satisfied with the upgrades.
* **Data Center Wiring:** has little to no cable management. Mistakes happen with wiring.
  + Operational risk.
  + Floors should be elevated to prevent flooding and to allow cable runs. The ceiling should have cable conduits implemented to future proof. Budget needs to be allocated for cable management and some new cabling.