Chapter 11 Review Questions

1. **What would be the most threatening security threats for the next five years?**

Data theft, in which information is illegally copied or taken from business or an individual, like passwords, SSN, credit cards and bank info; all these could be really harmful and have major economic and legal implications

1. **Why are wireless applications becoming a new target for hackers?**

Because hackers do not need to be physically connected to the attacked pc, therefore they can offer more opportunities for attacks

1. **Describe the five pillars of information security**
2. Authentication: Verifying the authenticity of users. There are three ways people can authenticate themselves to, say, a system, says RSA: by something they know, something they have, and something they are.
3. Identification: Identifying users to grant them appropriate access. In the Internet world, identification is moving toward application-level security, says RSA, that is, authentication for each application.
4. Privacy: Protecting information from being seen. This is especially important when information travels through the Internet because it is a public space where interception is more possible
5. Integrity: Keeping information in its original form. The most common method of protecting data is encryption.
6. Non-repudiation: Preventing parties from denying actions they have taken. Non-repudiation services can prove that someone was the actual sender and the other the receiver; no imposter was involved on either side.
7. **How does the Internet services company “check its locks”?**

* By keeping track of the latest bugs found in systems.
* By subscribing to security organizations and constantly visiting their Websites for the latest security attacks that have taken place around the world.
* By subscribing to hacker e-mail lists and bulletin boards to “think like the enemy.”
* By setting up a test system and trying various attacks on it—attacks they have read about on the e-mail lists and bulletin boards.
* By logging and monitoring all incoming and outgoing traffic, with a dedicated team managing the firewalls.
* By having a senior security person scan the company’s Websites monthly from a remote site, comparing the services being run on the servers with the official inventory of services that should be running on the servers. He also checks to ensure that no servers are running known compromised software.

1. **How did the University of Texas at Austin deal with a computer attack? Expand the notion of disaster recovery**

The disaster recovery steps taken by the University of Texas were the following

* Security audit: The University of Texas Information Security Office conducted a full security audit. Independent consultant and major IT firms were hired to perform a comprehensive evaluation of the campus computer systems and application software
* Countermeasures to reduce vulnerabilities: Many security steps were taken to secure the information stored on the computer servers
* Cooperation with law enforcement authorities: The University involved the Cyber Crimes Unit of the Texas Attorney General Office, the Federal Bureau of Investigation, and the University Police Department

1. **Discuss the human side of computer security**

Security is much a human problem as a technical problem, that’s why companies are as safe as their weakest link, which could be a supplier or a contractor with securing access to a company’s system. Also some of the most expensive and most damaging to the organization’s reputation is are made from criminals from the inside of the organization, they could do many things such illegally access employee’s email and steal information, an angry employee could bring down the entire computer system by deleting sensitive data records, a system admin could create bad data by change the code of legacy systems, a marketing salesperson can steal sensitive data and sell it to a competitor