Defenses

DEFENSE STRATEGY (PLAN)

Theory is good, it gives us a basis to work from, but what would an actual security plan look like? What strategy would be implemented to protect a corporation or an individual from harm? Four key elements should be used in creating this strategy and they include the following:

1. Block attacks
2. Update defenses
3. Minimize losses
4. Send secure information

BLOCK ATTACKS

A castle is an excellent analogy to information security. The moat and the walls of a castle are essentially layers of security. On the inside of the castle individuals may have personal shields to protect themselves from arrows flung over the castle walls.

To protect information from penetration from outside attackers, networks should be made secure with passwords, intrusion detection and inaccessibility. Inside the network, individual anti-virus shields and personal firewalls should be used for protection.

UPDATE DEFENSES

Personal shields to protect from attacks made over the wall may soon get out of date and not be able to withstand more modern arrows (i.e. armor piercing). Personal shields would need to be updated with Kevlar vests.

Likewise, servers and users with their own personal PCs will always have to keep their anti-virus software and operating systems up to date to eliminate vulnerabilities as much as possible.

MINIMIZE LOSSES

Defenses that are in place may not prevent harm in all cases. There will likely be damage from foiled attacks and certainly from successful attacks that have to be dealt with immediately for the fortress to remain strong.

If data in a secure network were to get compromised, there should be regular data backups and a business recovery plan in place to restore the data in an intelligent manner. There should also be a business continuity plan in place just in case the entire facility of the business became unsafe and unusable.

SEND SECURE INFORMATION

Defenses may actually break down in the castle. Reinforcements will have to be sent for by someone on a swift horse and body armor.

In a computer network, users will inevitably need to venture outside to get information (through the unsafe Internet or through an email, for example). To keep this traffic safe and secure it should be encrypted (scrambled) and secure (i.e. through a Virtual Private Network connection) so that attackers or potential attackers will not get information that could harm the sender and compromise the corporation.