Homework 4

Name: Anusha Balasubramanian
UID: 01305952
Email: ab19533n@pace.edu

1. Why did Cisco Systems transition from standalone access control systems to an IP networked systems?

Several years back Cisco had a lot issues with physical-security-management like providing unique access cards to all employee, managing, integrating and supporting a physical-security-system in each location etc. It was stated that employees who visit other locations couldn't gain access to enter the building using their own badge unless it's details are manually entered into local badge authorization database. Also the Badge-reader access systems required to be monitored by facility administrators and they needed to be specially trained in-order to understand the system. Access control system was complicated and even the security staffs were burdened with managing service- and system-integration support.

In case of Physical security, there was a need for leasing expensive phone lines to remotely monitor electronic sensors in other sites. They have to carry the signal back to the main security operations center using these phone lines. Also video recoded by surveillance cameras can be examined later and not immediately. With these major issues and in order to secure the business facilities cisco systems transitioned to IP networked system from standalone access control system.

2. What challenges did Cisco system face in order to solve the physical security problems?

Cisco faced three major challenges. There are mentioned below

- **Defining and developing a corporate physical-security philosophy**

  Creating access restrictions on Cisco employees and other contactors was a big challenge. Restrictions like 24-hour access along with access based on organization roles and productivity was needed to be defined for the Cisco employees, contractors and vendors.

- **Defining and developing a corporate physical-security design standard**.

  Creating a work culture between employees to be responsible for Cisco assets and at the same time maintaining secure work environment with minimum costs and losses was considered as a standard to be developed.

  In late 1997 the concept of using IP WAN and centralized management was under developed. Especially querying databases at

various locations from single center site was a huge challenge to implement.

- **Building a global systems-integration support model.**
  Supporting various complex system across various locations worldwide has always been a big challenge for Cisco. Due to new technology and complex system, it required skilled personnel to support and maintain the equipment.

3. How did the new architecture system solve the access control problem? Explain?

   Cisco is currently using a single set of software tools to standardize the access control system. The cisco STS developed a centralized architecture server based on single set of standards, supported by all worldwide regional security servers. Cisco IP WAN was used to link each centralized servers and to every access control system worldwide. Employee's profile was created at the time of joining and is provided with access restrictions based on their profile details. Initially STS team had lot of work as Cisco IT required servers meet server and OS standards, but now it has turned out to be easy in managing limited set of standard servers. Also the security and safety department is now free of managing and maintaining the servers, software patches and updates.

4. How did Cisco systems solve the physical security problems?

   Cisco has regional and global security operation Center(SOC) to whom all the all fire alarms, glass-break alarms, door-opening alerts, about 60 to 80 monitor points per Cisco building, are sent. CCTV cameras are installed in all the required places. They are connected using corporate IP network, and SOC can view all event in real time. The SOC logs in, to determine if they need to contact the local police or patrol. This reduced the number of false alarms reporting too. They also have emergency call center for Cisco employees where all emergency calls are routed to nearest SOC personnel and they provide emergency support accordingly.

5. What security technologies did Cisco deployed to control building security?

   Cisco has deployed various security technologies to control building security. They are listed below.

- More than 6600 proximity badge readers, 2600 CCTV cameras that streams video to networked video recorders or across the WAN was deployed.
- Deployed thousands of access-controlled doors signal, smoke and fire alarms, glass-breakage alarms, motion detectors.

- Cisco also developed two separate support models to integrate, centrally manage and maintain all its access-control systems. One for US and other one for EMEA, Asia-Pacific regions.

6. Even though the employees in the Cisco Systems have doubled STS team remains same. Why? And how it helped to save cost?

   The STS team has performed the following major operations.
   - Automated many of its access-control systems.
   - Management is made centralized using corporate IP WAN.
   - Outsourcing the maintenance to trusted partners.

   STS team was able to add, remove employees, update permissions and update the information in all locations world wide within minutes time using the integrated system. They use corporate WAN to help save a lot of costs to be invested on dial-up or data lines and separate data lines for video. The necessary IP information is easily carried to SOC personal using WAN. Thus with the help of the above mentioned actions taken, the pain of employing 300 security officers in all the 300 locations is eliminated thereby reducing each security officer in each place of access (doors, labs, cameras, alarm system etc.). This is how Cisco was able to maintain STS team to remain the same along with saving cost.