Physical Security Plan – Alvin Sarkadi

Exterior

- Why did you propose the lighting where you did?

  The main facility will be facing the sun, with complete 360-degree visibility. During the night, the lighting will be covered with the use of floodlighting. Especially in a hospital facility, it is important for people exiting and entering the building to have a clear view of their surroundings. I propose to use 7 flood lights for specific entrances and exit points of the hospital during the night to secure the perimeter of the hospital.

- When placing the parking lots, what factors did you consider?

  The exterior of the building will include two separate parking lots, one parking lot in the back of the facility for staff, while having patient parking at the front of the building. The staff parking lots will include a gate with a built in NFC card reader installed by network engineers. This is to allow specific access to employees to the lot. This is also to prevent unwanted vehicles or person(s) entering the staff parking lot. This is significant to keep the staff safe with their property and their belongings especially if the staff possesses sensitive information within their car. (A security policy should outline the prohibition of this.)

- Why did you place cameras where you did?

  The cameras I chose are 360-degree outdoor Panoramic Network mini dome camera with night vision. I also plan to install smoke detectors attached on, or, close to the cameras. The camera features night vision with 60fps 2016 x 2016 resolution.

  The specifications make it quite effective for a facility like a hospital the details are outlined under specifications on the listing.:

  "**1.** Built-in installation aids include pixel counter, digital roll, repositioning of quad views, digital PTZ of view areas, and digital PT of panorama, corner, corridor, and quad views. **2.** Image settings include compression, color saturation, brightness, sharpness, contrast, local contrast, white balance, day/night threshold, tone

mapping, exposure control (including automatic gain control), exposure zones, forensic WDR up to 120 dB (depending on scene), fine tuning of low-light behavior, dynamic text and image overlay, mirroring, digital roll, and polygon privacy masks **3**. Security features include brute force delay protection, secure boot, signed firmware, and Axis Edge Vault with Axis device ID **4.** Analytics include video motion detection and active tampering alarm, with support for motion guard, fence guard, loitering guard, people counter, occupancy estimator, queue monitor, and third-party applications." (Axis Communications, 2016.)

I will use two cameras in the patient parking lot, one facing the north side of the hospital, while the other faces in the interior. The camera that will be facing the interior will be close to the outside of the hospital, identifying and making sure that the sides and front entrance are secure from intrusions, or malicious attacks against the hospital. The camera facing north will identify and capture vehicle entrances, and exits, and can capture other concerning materials since both camera's operate on 360 degrees.

I propose that three cameras be placed in the staff parking lot. One should be used at the gate for the NFC card reader. This is to prevent unwanted personnel into the staff parking lot, and to track and monitor any individuals pursuing to gain access to the staff parking lot without permission. The two other cameras will also follow the same procedure as the patient parking lot with some adjustments.

The first of the two cameras' will be designated to cover the NFC card reader from the rear of the hospital. Specifically, the far-left corner (Where staff also enters the facility). For the final camera, it should be put near the roof, and near the roof floodlight. The camera and floodlight will be capable of spotting any intruders from the staff parking lot. The camera will relay any video files to a server or workstation if necessary, using third party applications noted in the specifications. Any intrusions that occur will be reported and communicated to local authorities immediately.

Lobby

- What kind of windows are required? What kind of access control security are you providing for the visitor, employee, and patient?

Upon entrance, there will be full covered glass for registration into the hospital. There will be a designated area behind the glass for a security guard to collect information from a visitor, or patient.

Since the entrance of the hospital for the staff is in the back, I would suggest using the same plated glass, and hiring a security guard, guarding the door from the inside. An NFC reader will be stationed at this checkpoint for ID badges. This is to make sure that any ID badges are not being used by individuals that have stolen credentials. Regarding the security access controls of the security guards, the guards will only be able to read information from their machine/workstation using an application built by a third-party application developer. This application will only allow the user to scan ID's and read general information about appointments, registrations, patients, and staff. The security guards will be given no access to modify any data through the application. If the security guard cannot assist the patient, or visitor; A floor manager, and the specific doctor, should be advised whether the patient, or visitor can enter the hospital and visit the patient/floor. However, if the security guard can assist the individual via the third-party application, the security guard will grant the individual access to the hospital.

- What kind of information would you collect from all nonemployees to enter the hospital for security reasons?

  Full name, date of birth, COVID-19 vaccination status, and what they are doing in the organization and for how long. Any large suspicious belongings will be inspected upon registration, if the security guard believes there is probable cause to inspect the individuals or individuals' belongings. (Unusual behavior, indications of the use of narcotics, indications of an attempted network intrusion, unusual number of wireless devices, multiple phones, Raspberry Pi's, firearms, explosives etc.) The security guard may search the individual and call local authorities if needed.

- What kind of security would you have at the door? (Physical, ID badges, cameras)

  I would propose 2 security guards at the front of the entrance of the hospital. Also, 1 security guard at the back entrance of the facility. Employees such as

guards, surgeons, doctors, nutritionists, janitors, IT, and tech should have one key to the back entrance of the hospital. A security policy should be noted that no duplicates should be made.

The employees and staff will now use NFC ID badges. The badges will include their name, and name of the job applied by the employer. These badges contain a chip which can be read using an NFC ID reader. This is the safest and most reliable form of secure entrance because it is a physical key that offers discrete, brief, and isolated communications, unlike RFID.

For interior cameras for the lobby, I chose two Meraki MV32 Ultra Compact Indoor fisheye cameras. The camera's provide cloud management for further indoor security on floors, elevators, etc. This is for the security guards at the lobby of the hospital.

Maternity Unit

- From a security perspective, why is the placement of the nurses' station important?

  In a maternity unit a lot of congestion is unnecessary and could be hazardous. The maternity unit would be separate from usual patient areas due to this nature. The maternity unit would be included within the facility. However, separate from the standard security rules established for the exterior and the lobby. Individuals will be met with a stricter security policy inside the maternity unit.

- For security reasons, why do you encourage visitors to stay in designated areas or tell them where to go?

  I encourage visitors to stay in designated areas due to congestion, safety, and most importantly hygiene. Having visitors where they need to be, makes the hospital safer, it also creates efficiency, effectiveness, and separation. Allowing the staff to be caring to patients makes it easier for the patient by not being inconvenienced. By having signs and identifiable maps around the hospital, large signs by certain hospital unit doors, this will eradicate congestion among the

workplace. Furthermore, it would give an opportunity for employees and patients to feel comfortable at the workplace.

- How do you secure the newborns from potential abduction and accidental switching?

  Two network security managers will be hired to maintain indoor camera systems installed to protect the infants. This includes a temperature thermo-stat monitoring system to assure that the temperature and humidity is suitable for the infants and HIPAA regulations. This security manager will have to understand the strict security policy he/she/they are under. For instance, a company approved phone will be issued to this employee, no personal phones would be permitted in the hospital. This is to help protect and sustain the hospitals network from vulnerabilities. Furthermore, a strict legal policy should be in place for these employees regarding the severity of a potential abduction or accidental switching. To protect our security managers, we must implement a new security policy for the maternity unit. Staff and employees that will have access to the maternity unit will need a new, limited NFC ID badge separate from the rest of the employees and staff entrance/lobby entrance. Infants will not only be tagged, but geotagged. The network security managers will be instructed to set up parameters regarding the GPS information of each infant. When parents/patients have gained access to pick up their infant in the maternity unit, the geotagging device and tag will be removed, but the data from the GPS device will be extracted and put into a database by network security managers, in case of emergencies with the infant.

  Additionally, the maternity unit will be locked with an 8-digit pin to enter the Maternity unit. The security manager will advise all employees and staff to create a digital signature, Key, and profile, to create a PGP encrypted messaging system. The passcode to the maternity unit will be changed every week. This code will be sent out to trusted employees via PGP encryption that are allowed within the maternity unit, the employees would need to decrypt the message sent by the security manager to gain access to the maternity unit each week.

  The security managers can also choose different indoor camera systems that are to their convenience if it abides by the security policy established by the hospital. The Meraki MV32 Ultra Compact Indoor fisheye camera is a modern camera used

in organizations like hospitals. However, some security managers find other cameras to their convenience. In this case I would like to be contacted.

Security Training

- What kind of security training would you offer to employee staff, and how often would it take place? Why?
    - Would the training be different for each group? How?
    - Employee Numbers / ID's: Database of employers to verify credentials if needed.
    - The principle of least privileged: Allowing certain access and permissions to the network based on employee data.
    - .USB mounting, CD, DVD-ROM will be disabled on all machines
    - Reading/Writing/Modifying files on workstations will be re-evaluated for all workstations, such as Human Resources, Accounting etc.
    - Personal devices such as personal smartphones and smartwatches are prohibited from the hospitals network. This crucial to keep the network infrastructure efficient and maintainable from intrusions. Company phones will be provided that are permitted by the security cell-phone policy.

      Janitorial Services: Cleaning service employees are prohibited from entering the hospital with their personal wireless devices such as smartphones. An NFC ID badge will be given to this/these employee(s). A company issued cell phone will be provided to bring into work.

      General Employees: (Accountants, Chefs, Management, Human Resources). Will also be issued company cell phones to mitigate the risk of an attack. Employees with significant tasks within the network, such as accounting, human resources, IT and tech, and all other departments working with the hospitals network via workstation will only be allowed to read and write privileges within their designated network.

      Security Guards, Secretaries: Security guards will be granted reading permissions but no writing permissions. Instead, secretaries will have the

privileges to read and write within their designated department on their workstations. (Modify files)

IT / Security Management: IT / Security management will have admin / root access to the organization's security. This means monitoring traffic on each network of the hospital, making sure that there are no inside or outside attackers. Again, these employees will also have to follow the company cell phone policy, instructing all employees that their personal wireless electronics are prohibited from connecting to the network unless advised by a network administrator.

Doctors, Nurses, Pediatricians etc.: Advise all the listed employees to keep personal confidential records only at the organization. Not in a car, cellphone, or at home. Copies of keys from all employees are forbidden unless told otherwise by the policy administrator.

Personal cellphones for employees are permitted but disconnected from the hospital's wireless internet services and cellular services. All employees will follow this condition to protect the hospital's network and data. The hospital facility will offer a guest Wi-Fi service with limited access, and completely disconnected from the hospitals main network infrastructure.

Third party services: (Inspections, plumbers, repairs,): Security guards must define third party services as visitors. Security guards must check and record ID's and instruct them to keep all personal cellphones and wireless technology outside of the hospital unless permitted.

Phishing emails: Employees must be able to identify suspicious emails. An information guide will be handed out to employees, so they are aware of phishing emails.

Social engineering: Staff, guards, receptionists, customer service representatives must be aware of social engineering attacks. Whether the attacker is communicating via telephone or in person. Employees must carefully verify credentials such as full name, and Employee ID, or through the NFC reader's UI. Especially with third party services, and visitors. An information guide will be handed out to employees, so they are aware of social engineering attempts.

Jailbroken phones, phones with root access, Android, and iOS: Jailbroken phones, unauthorized operating systems (anything outside of Android / IOS) are prohibited from being within the workplace.

Conclusion:

Due to the recent rise in cyber-attacks against U.S hospitals nationwide, it is necessary that we take these precautions to secure the hospital and its data. Without an effective and strict policy, hospitals are vulnerable to many cyber-attacks, and current vulnerabilities and exposures. Thank you for taking the time to read my security plan. Hospitals secure confidential information about patients, visitors, and employees. It is important that we take further precautions to mitigate network vulnerabilities and trespassing.

Best Regards,

Alvin Sarkadi

Works Cited:

Axis Communications M3057-PLVE 6MP 360° Outdoor Panoramic Network Mini Dome Camera with Night Vision. (2016). Bhphotovideo.com. Retrieved from: https://www.bhphotovideo.com/c/product/1636682-REG/axis_communications_02109_001_m3057_plve_mk_ii_6mp.html/overview?ap=y&ap=y&smp=y&smp=y&lsft=BI%3A6879&gclid=CjwKCAiA9aKQBhBREiwAyGP5lcXjs2W2OvgDis-iivqoudOHockl1QnHpZeOOwIfbLG7ceygOTXQPxoCXAEQAvD_BwE

uCertify. (2016). *Lesson 10 : Securing specialized systems -uCertify*. UCertify. https://www.ucertify.com/?func=ebook&chapter_no=11#top

uCertify (2016.) Learning Topic: Security Considerations for a Hospital. Retrieved from

https://leocontent.umgc.edu/content/umuc/tus/cmit/cmit320/2222/learning-topic-list/security-considerations-for-hospitals.html?ou=628413

uCertify. (2016). *Lesson 9 : Securing hosts and data -uCertify*. UCertify. Retrieved From https://www.ucertify.com/?func=ebook&chapter_no=10

Meraki MV32 Ultra Compact Indoor Fisheye Camera. (2022). Retrieved from: https://4tekgear.com/meraki-mv32-ultra-compact-indoor-fisheye-camera-1635768293-1636151211-1643496465.html?gclid=CjwKCAiA9aKQBhBREiwAyGP5lVLnWIn_Fh6iS0kkXHW8q1T_PJdlUzawk8nsB8sPVrmiauW_-6wWZBoClPgQAvD_BwE