

Adrian N  
12/08/21  
Risk Management - Social Engineering

#### Teach 4 Hospitals


Your company is a teaching hospital. You are with the IT security department, protecting the network and the devices on the network. The hospital/school is one large network that contains equipment (servers, workstations, mobile devices, and medical devices) for a variety of people (hospital employees, school employees / staff, students, patients, visitors). The network provides both authenticated and guest access. The network is segmented, but compromise of one system could lead to compromise of other areas. Some of the devices are hardened per your company standards (hospital and faculty equipment) while other devices are unknown (student computers and patient/visitor devices). Both the hospital and school provide VPN capabilities to employees and students for remote access. Both the hospital and school run web servers providing information to students and patients. These web servers are driven by backend servers and databases containing employee, student, and patient information. Your company provides 24/7 email, web chat, and phone support to its customers. The company also uses cloud-based Outlook / Office 365 for internal and external email communication. Both email and VPN are accessible from anywhere via an email address and a password. For your exam, you will be focusing on the all types of social engineering risks to both the hospital and school (physical, network, email, ...) that may be conducted against anyone on the campus (faculty, student, doctor, patient, visitor, ...). Other vulnerabilities may also be considered if you have difficulty documented enough social engineering vulnerabilities.


## Section 1: Information Assets

In today's electronic world, cybersecurity in healthcare and protecting information is vital for the normal functioning of organizations. Many healthcare organizations possess different assets, and for our organization we shall specify so. Information that our company possesses and the data subject for that information:


Company Itself: Teach 4 Hospitals  
Business Objectives of the organization / Research  
Annual Reports  
Mission Statement

### Employees

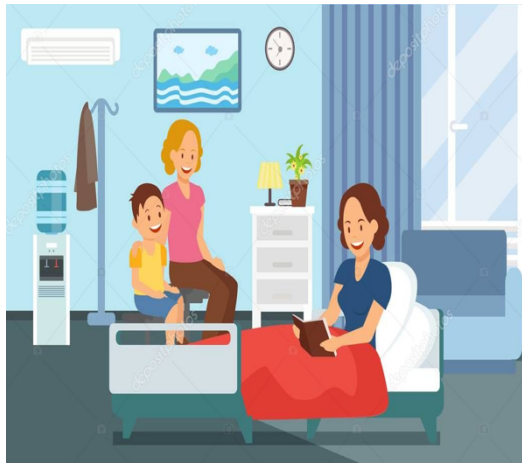
Hospital Employees	Example	
Personal information including: Name Date of Birth Address Social Security Number Phone Number Email Address Bank Information (Direct Deposit) Corporate Secrets Access to Database Access to high security checkpoints Wifi Passwords	John Adams October 30, 1995 300 John St. Rochester NY 14623 xxx-xxx-5678 585-421-2234 <a href="mailto:jadams@gmail.com">jadams@gmail.com</a> Routing Number: 012345678 Account Number: 1001001234 "New digital thermometer is being developed etc"	
School Employees	Example	

Personal information including: Name Date of Birth Address Social Security Number Phone Number Email Address Bank Information (Direct Deposit) School Identification Number Resume Information / Contact Information	Steven Bradley January 5, 2000 100 Ave Flushing NY xxx-xxx-1234 585-123-454 <a href="mailto:stevenbrad@rit.edu">stevenbrad@rit.edu</a> Routing Number: 876543210 Account Number: 1201201234 UID: 123-110-4950 Alternate Address, Old Boss Information	
---	--	--


## Patients

Patient	Example:	
Name Date of Birth Address Social Security Number Phone Number Email Address Bank Information Insurance Card Information	Johnathon Jojo July 23, 2001 E 19 Gun Hill Road NYC xxx-xxx-8555 347-969-0111 <a href="mailto:jjjojo@gmail.com">jjjojo@gmail.com</a> Routing Number: 912353111 Account Number: 1213454531 Delta Insurance Plan	

## Visitors

Family Members	Example:	
Name Date of Birth Address Social Security Number Phone Number Email Address Bank Information Insurance Card Information	Valentina Jojo November 23, 1985 E 19 Gun Hill Road NYC xxx-xxx-8421 347-999-0134 <a href="mailto:vjojo@gmail.com">vjojo@gmail.com</a> Routing Number: 872343110 Account Number: 1201204531 Delta Insurance Plan	

## Students

Students	Example:	
Name Date of Birth Address Social Security Number Phone Number Email Address Emergency Contact Info	Tom Donald February 1, 2005 383 Rochester Rd 14623 xxx-xxx-4623 585-656-6654 <a href="mailto:tomdonald@g.rit.edu">tomdonald@g.rit.edu</a> Mother Cell #: 151-232-4545	

## Data Categorization:

Personally Identifiable Information (PII), any information that can be used to determine an individual's identity

All of the subjects contain forms of PII, as things like Name, Address, SSN, Phone Number, and even University ID could lead to determining their identity.

Electronic Health Information (e-PHI), term given to health data created, received, stored, or transmitted by HIPAA-covered entities.

## 18 HIPAA Identifiers

**The Department of Health and Human Services (HHS) lists the 18 HIPAA identifiers as follows:**

1. Patient names
2. Geographical elements (such as a street address, city, county, or zip code)
3. Dates related to the health or identity of individuals (including birthdates, date of admission, date of discharge, date of death, or exact age of a patient older than 89)
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers
13. Device attributes or serial numbers
14. Digital identifiers, such as website URLs
15. IP addresses
16. Biometric elements, including finger, retinal, and voiceprints
17. Full face photographic images
18. Other identifying numbers or codes



Payment Card Industry (PCI) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The patients, employees, and visitors all will most likely have credit card information on file, that could be at risk.

## **Regulations that may be applicable:**

### **NIST Cybersecurity Framework**

The NIST CSF provides a common structure for managing cybersecurity risk that is flexible and more importantly adaptable, and should be used by healthcare organizations as a baseline.

## **Data Classification**

### **Company Website:**

Public Website, may be openly shared with the public

### **Employee Data:**

Internal, only available company wide to company employees (Varies employee to employee)

### **Student Information:**

Restricted, not necessary to share with public, and would cause undesirable effects if publicly available

### **Patient Records:**

Restricted / For Official Use Only, would cause serious damage if publicly available, government business and commercial activity.

### **Confidential Business Data:**

Confidential: Business specific / Team wide within the organization

Includes things like:

- Pricing
- Marketing Materials
- Contact Information

Disclosure may negatively impact business (LaLena 35).

### **Visitor Information:**

Restricted / Internal, not necessary to share with public, and should be accessible by employees

### **Secret Company Information:**

Top Secret, would cause exponential damage to national security if made publicly available.

## Section 2: Other Non-Information Assets

### Physical Building (Infrastructure)

- Construction Plans
- Physical Protections
- Heating
- Air-Conditioning
- Refrigeration
- Ventilation
- Plumbing
- Electrical Pumps
- Condensers
- Generators
- Compressors
- Mobile Beds & Wheelchairs

### Control Systems

### Data Acquisition Systems

### Networking Equipment

### Hardware Platforms for Virtual Machines (VM) or Storage

### Printers / PhotoCopiers

### Scanners

- X-Rays
- MRI
- CT
- Ultrasound

### Laboratory Equipment

- Analytic Balance
- Centrifuge
- Incubator
- PH Meter
- Kerosene Stove
- Water bath
- Vaccine Transport Box

### Theatre

- Defibrillator
- Anaesthetic machine
- Oxygen Regulator
- Vital Signs Monitor

### ICU

- ICU Bed

### Pharmacy

- Distiller
- Tablet Counter
- Drug Cabinet
- Counting Trays
- Weighing Scale (Electronic)

#### FIPS 199 - Physical Infrastructure: (8)

(i) Our organization Teach 4 Kids is a large 3500 square foot property that contains many access points. There is a blueprint containing all the ins and outs of the building, which provides the heating, air-conditioning, ventilation, plumbing, generators, server room, and compressors layout. On top of this are things like Mobile Beds & Wheelchairs which contain some tech that could be vulnerable to attacks.

SC *construction plans* = {(confidentiality, HIGH), (integrity, LOW), (availability, LOW)}

Construction plans could give up a blueprint to a physical attack, as there could be a vulnerability in the building security. (8)

SC *heating* = {(confidentiality, LOW), (integrity, MODERATE), (availability, HIGH)}

Heating is necessary during certain periods of time, and it must always be readily available (7)

SC *air-conditioning* = {(confidentiality, LOW), (integrity, MODERATE), (availability, HIGH)}

Air-Conditioning like heating, is necessary during certain periods of time and must be readily available, especially to keep the server room cool (10)

SC *ventilation* = {(confidentiality, LOW), (integrity, MODERATE), (availability, HIGH)}

Ventilation is effective at reducing hospital infections and needs to be active at all times (8.5)

SC *plumbing* = {(confidentiality, LOW), (integrity, MODERATE), (availability, MODERATE)}

Plumbing prevents leaks which could cause damage to infrastructure (7)

SC *generators* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}

A backup generator is a must in case there is a shortage, as it could mean life or death for patients that need care (10)

SC *compressors* = {(confidentiality, LOW), (integrity, MODERATE), (availability, Moderate)}

Compressors keep the patients comfortable and breathing (6)

SC *mobile beds & wheelchairs* = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, HIGH)}

A mobile bed or wheelchair can be used to transport patients in a timely manner (7)

SC *server\_room* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

The most important room to keep protected and cooled(10)

SC **physical infrastructure** = {(confidentiality, MODERATE-HIGH), (integrity, HIGH), (availability, HIGH)}

#### FIPS 199 - Control Systems: (5)

(i) Our organization uses control systems. This consists of a number of components connected together to perform a specific function like a refrigerator. The output quantity is controlled by varying the input quantity.

SC *refrigerator* = {(confidentiality, LOW), (integrity, LOW), (availability, MODERATE)}

Every workplace has a refrigerator but ours is not an advanced one that can be breached (5)

SC *bathroom toilet tank* = {(confidentiality, LOW), (integrity, LOW), (availability, HIGH)}

Can not really be attacked, as there would be no motive to (3)



**SC control systems** = {(confidentiality, LOW), (integrity, LOW), (availability, HIGH)}

FIPS 199 - Data Acquisition Systems: (9)

(i) Our organization uses a collection of software and hardware that allows one to measure or control physical characteristics of something in the real world.

*SC clinical trial data* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
Our trial data must be kept secure and private as it is the definition of confidential (10)

*SC interactive\_voice\_respond\_systems* = {(confidentiality, LOW), (integrity, MODERATE), (availability, HIGH)}

Our voice systems could do a lot of work for us when it comes to social endeavors, but must be monitored. (7)

**SC data acquisition** = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

FIPS 199 - Networking Equipment: (10)

(i) We use networking equipment for communication and interaction between devices on our network. This mediates data transmission on the network and is a necessity in our organization.

*SC hub* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
A necessity as it helps connect multiple PCs to a single network (10)

*SC switch* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
A switch is needed to manage traffic (10)

*SC router* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
Facilitates the movement of data (10)

*SC gateway* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
Safeguards a private network (10)

*SC access point* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
Extends wireless coverage and increases the number of users that can connect (10)

**SC networking\_equipment** = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

FIPS 199 - Hardware Platforms: (10)

(i) Our building contains every type of computer available in the modern day. This includes all of the major hardware platforms used today. These hardware platforms are sets of compatible hardware on which software applications can be run.

*SC linux\_computer* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
*SC windows\_computer* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

*SC macOS* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

*SC OpenVMS* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

*SC mobile\_devices* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

All of these computers / devices are rated 10 as they can contain information that is vital (10)

SC **hardware** = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

FIPS 199 - Medical Scanners: (10)

(i) Due to the fact that we are a hospital, we must carry medical devices at all times, and the availability of these devices could mean life or death for some patients. These devices include but are not limited to: X-Rays, MRI, CT, Ultrasound

SC *x-rays* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}  
Imaging test that can help diagnose, monitor, and treat medical conditions (10)

SC *mri* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
Helps doctors diagnose a disease or injury (10)

SC *ct* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}  
A valuable diagnostic tool, that can detect some things x-rays cannot (10)

SC *ultrasound* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}  
Uses soundwaves to produce pictures of the inside of the body. Needed to help diagnose causes of pain or infections (10)

SC **scanners** = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

FIPS 199 - Laboratory Equipment: (7.5)

(i) Our team of scientists working in our laboratories must have various tools and equipment at their disposal for the greater good of testing. This includes but is not limited to: Analytic Balance, Centrifuge, Incubator, PH Meter, Kerosene Stove, Water bath, Vaccine Transport Box, Microscopes

SC *analytical\_balance* = {(confidentiality, LOW), (integrity, MODERATE), (availability, HIGH)}  
Accurately weighs samples and precipitates (7)

SC *centrifuge* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}  
Separates fluids, gases, or liquids based on density (9)

SC *incubator* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}  
Provides controlled environments for premature and ill babies (9.5)

SC *ph\_meter* = {(confidentiality, N/A), (integrity, LOW), (availability, HIGH)}  
Measures hydrogen ion activity in solutions (5)

SC *kerosene\_stove* = {(confidentiality, N/A), (integrity, LOW), (availability, HIGH)}  
Good source of energy (5)

SC *water\_bath* = {(confidentiality, N/A), (integrity, MODERATE), (availability, HIGH)}  
Reduces the spread of infections in hospitals (8.5)

SC *vaccine\_box* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}  
Helps the transportation of vaccines, which in the modern day is a big target (10)

SC *microscopes* = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, HIGH)}

Used to observe blood cells and checked for abnormalities (9)

**SC lab\_equipment** = {(confidentiality, LOW-MODERATE), (integrity, MODERATE), (availability, HIGH)}

FIPS 199 - Theatre Equipment: (10)

(i) An operating theatre otherwise known as an operating room is a facility within our hospital where surgical operations are carried out in an aseptic environment. These surgeons need devices like a Defibrillator, Anaesthetic machine, Oxygen Regulator, Vital Signs Monitor to perform these operations.

*SC defibrillator* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

Restores a normal heartbeat by sending an electric pulse or shock to the heart (10)

*SC anaesthetic* = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}

Allows patients to undergo an operation safely without experiencing distress and pain (10)

*SC oxygen\_regulator* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

Ensures that you are receiving the correct amount of oxygen (10)

*SC vital\_signs\_monitor* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

Helps measure to obtain basic indicators of a patient's health status (10)

**SC theatre\_equipment** = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

FIPS 199 - Pharmacy: (7)

(i) Our building contains a mini pharmacy in which houses many medicinal drugs which are used during operations, or emergency situations. We also prescribe the 'harder' drugs in severe cases where it is needed immediately.

*SC distiller* = {(confidentiality, LOW), (integrity, LOW), (availability, HIGH)}

Dissolves the toxins from our body that accumulate over time (9)

*SC tablet\_counter* = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}

Accurately count prescription medications (5)

*SC drug\_cabinet* = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}

A good way to keep drugs in a safe place (5)

*SC counting\_trays* = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}

Accurately counts and dispenses medications (5)

*SC weighing\_scale* = {(confidentiality, LOW), (integrity, LOW), (availability, MODERATE)}

Help weigh the proper dosage of medication (5)

*SC drugs* = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

Medicines help control things like high blood pressure, high cholesterol etc. (10)

**SC pharmacy** = {(confidentiality, HIGH), (integrity, LOW), (availability, HIGH)}

## Section 3: Threats

Our organization Teach 4 Hospitals, is a big target that can attract all types of threat actors. Our establishment houses many high tech devices that are breachable and easily targeted by attackers who seek to gain anything from money, to simply causing harm and destruction. The potential threat actors our organization will face are: (LaLena, 14, Threats and Threat Actors)

- Internal Human Error
  - Simple User Errors
  - No motivation, not malicious
  - User might have elevated permissions within our organization
  - Damage could be catastrophic
  - TTPS: Data misuse, poor data security and hygiene
- Cyber Terrorists
  - Motivated by the idea of causing harm and destruction to further their cause
  - Disrupting critical services and to cause harm
  - TTPs: Defacements and claimed leaks
- Organized Cybercriminals
  - Motivated by potential financial gain
  - Steal sensitive data, money, and personal information that could be sold on black market
  - TTPS: Social Engineering attacks, Phishing emails, scams, botnets, exploit kits, ransomware, malware
- State-Sponsored Actors
  - Motivated by political, military, or government espionage
  - Target private sector networks to compromise, steal, alter, or destroy data
  - TTPS: Spear-Phishing password attacks, Social Engineering, data exfiltration, remote access trojans, destructive malware.
- Hacktivists
  - Motivated by the thought of exposing secrets and disrupting 'evil' services
  - Motivated by ideological activism as well
  - Focused on bringing awareness to a cause
  - TTPS: DDoS attacks, doxing, website defacement
- Inside Agents and Bad Actors
  - Motivated by personal goals, whether it be financial gain or defamation
  - May infiltrate workforce themselves or turn an inside towards their cause/goal
  - Very high risk due to the level of access they could have
  - Could include former employees that retain system access
  - TTPS: Data exfiltration or privilege misuse
- Script Kiddies
  - Goal is to attack computer systems and networks to inflict as much damage as possible
  - Unskilled threat actors who use other peoples developed tools
  - TTPS: Open Source attack software and tools

The assets that will most likely be targeted by these actors are:

Personally Identifiable Information (PII)

All of our subjects contain forms of PII, like their Name, Address, SSN, Phone Number, and even University ID. These threat actors that are looking for financial gain might target these PII's in hopes of selling this information on the black market.

#### Electronic Health Information (e-PHI)

These PHI's might be targeted by people looking for financial gain, or state sponsored acts who want to discover and analyze our organizations health data.

#### Payment Card Industry (PCI)

The patients, employees, and visitors all will most likely have credit card information on file, that could be at risk from these threat actors who are steadily searching for financial gain.

More specific assets are:

Health Records - Threat actors who want to know something specific about a high level target could potentially try to breach our database and search for health records.

Vaccine Data - In the present day a State Sponsored attack might be looking for our clinical data on vaccines that they hope to steal for either their own sake, or financial gain.

Construction Plans - A inside threat might want to get their hands on our buildings blueprint, to see the access they might have throughout the premises as it could help lead them to their goal

## Section 4: Vulnerabilities

Personal Health Devices like pacemakers and defibrillators are increasingly connected to the internet to provide continual monitoring and control. There is an ability to exploit vulnerabilities in these devices to deliver painful shocks to patients and/or to install ransomware or other malware on the systems.

- MITRE ATT&CK tactic Impact & Execution (TA0040 & TA0002)
  - The attackers are trying to run malicious code, and in doing so trying to manipulate our system.
- STRIDE threat type Tampering
  - The attackers are trying to tamper with our devices to exploit them

Patient Monitoring devices like the vital signs monitor are regularly using networked devices for patient heart rate and oxygen level monitoring and medicine dispensing. Attacks against these devices could block alerts to nurses and/or give patients dangerous levels of medication or the wrong medicine in general.

- MITRE ATT&CK tactic Impact (TA0040)
  - The attackers are attempting to get into our system to potentially kill a patient
- STRIDE threat type Spoofing
  - In our organization you can not get into the medicine/drug database without valid credentials, so the attackers must aim at accessing and using another user's credentials

Scanners and imaging devices like the Ultrasounds, CT, MRI, and X-Rays are commonly connected to hospital networks. An attacker with access to these systems could tamper images, resulting in misdiagnoses.

- MITRE ATT&CK tactic Collection & Impact (TA0009 & TA0040)
  - The attacker could be trying to collect data for their goal, such as collecting a person of interest's x-ray images etc. They also are trying to manipulate our systems.
- STRIDE threat type Elevation of Privilege
  - The attacker is intending to gain privileged access to a machine in order to gain unauthorized access to information or to compromise the system.

Surgical Devices like our surgical robots undertake more precise operations than previously thought possible, and the use of this technology continues to increase risks. Attacks against these devices could render our hospital unable to provide life-saving care or cause harm to a patient during surgery.

- MITRE ATT&CK tactic Impact (TA0040)
  - The attacker is striving to manipulate our robotic surgical devices for their own goal which could be to cause harm to a patient.
- STRIDE threat type Elevation of Privilege
  - Again, the attacker needs to have privileged access in order to get to our robotic surgical machines so that they can have unauthorized access.

Server / Network:

Distributed Denial of Service Attack (DDoS) TTP used to overwhelm a network to the point of inoperability. Our hospital might follow a potential attack like Boston Children's Hospital in 2014.

Anonymous (a well-known hacktivist group) targeted the Boston's Children's Hospital with a DDoS attack after the hospital recommended one of their patients, a 14-year-old

girl, be admitted as a ward of the state and that custody be withdrawn from her parents. The doctors believed the child's ailment was actually a psychological disorder and that her parents were pushing for unnecessary treatments for a disorder the child did not have. The custody debate put Boston Children's Hospital in the middle of this controversial case, and some, including members of Anonymous, viewed this as an infringement on the girl's rights. Anonymous took action by conducting DDoS attacks against the hospital's network, which resulted in others on that network, including Harvard University and all its hospitals, to lose Internet access as well. The networks experienced outages for almost a week, and some medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information, according to the Boston Globe. As a result, the hospital spent more than \$300,000 responding to and mitigating the damage from this attack, according to the attacker's arrest affidavit (Cisecurity 1).

- MITRE ATT&CK tactic Impact (TA0040)
  - This is because the adversary is trying to manipulate, interrupt, and/or destroy our systems and data by potentially running a DDoS attack on our network.
- STRIDE threat type Denial of Service
  - The threat action is attempting to deny access to valid users, such as by making a web server temporarily unavailable or unusable as in the case with Boston's Children's Hospital.

#### Patient Records:

Our organization, although it keeps digital files, also contains paper copies of patient records. This could lead to many different types of attacks that are listed below:

#### Physical Stealing

- MITRE ATT&CK tactic Reconnaissance & Resource Development & Lateral Movement & Collection
  - The attacker is trying to physically steal our files by trying to gather information they can use to plan future operations. They are also trying to establish resources they can use to support operations, as well as trying to gather data of interest to their goal. They also will have to physically move throughout our environment which connects to our potential physical infrastructure assets like our blueprint.
- STRIDE threat type Information Disclosure
  - The attacker is intending to read or steal file that he/she was not granted access to

#### Insider Threat - Employee

- MITRE ATT&CK tactic Reconnaissance & Resource Development & Lateral Movement & Collection
  - The attacker is an inside threat who potentially has direct access to our physical storage room or database in which they can secretly take photos, or steal files for the greater good of their goal
- STRIDE threat type Information Disclosure

- They are still intending on reading or stealing a file that they should not have access to, as we as a company should have done better with giving certain people certain permissions and checkpoints

#### Internal Human Error - Employee

- MITRE ATT&CK tactic N/A
- STRIDE threat type N/A
- There are no tactics or threat types for an internal human error. This still could be catastrophic however, as these users with elevated permissions within our organization's physical building could accidentally misplace or destroy a patient record.

#### Social Engineering Attacks:

Our organization has many people who are working and or studying at all times. This means that there is a lot of risk in terms of social engineering attacks. These attacks could potentially compromise an entire organization like ours. According to the Verizon 2019 Data Breach Investigations Report, 33% of data breaches were social engineering attacks (Smith, 2019). These attacks exploit human weaknesses in human interactions and behavioral/cultural constructs and occur in many forms. This will always be a huge risk and like our patient records, could affect a lot of our assets shown below:

#### Employees

- MITRE ATT&CK tactic Privilege Escalation, Initial Access, Defense Evasion Credential Access, Exfiltration (TA0004, TA0001, TA0005, TA0006, TA0010)
  - The Social Engineer will persistently try to send phishing emails trying to trick an employee into giving up any information. This process can last a while and these engineers will use all types of psychological tricks to get closer to their goal.
- STRIDE threat Elevation of Privilege
  - The attacker must gain privileged access to a resource like an employee computer, in which they will compromise and use for their goal.

#### Patients

- MITRE ATT&CK tactic Privilege Escalation, Initial Access, Defense Evasion Credential Access, Exfiltration (TA0004, TA0001, TA0005, TA0006, TA0010)
  - The attacker might try to gain access to a network by targeting a patient. They might pretend to be someone the patient knows, a healthcare provider, or even a doctor in order to get the information they are after.
- STRIDE threat Elevation of Privilege
  - The engineer will want to gain access to a network in order to compromise more and more systems.

#### Visitors

- MITRE ATT&CK tactic Privilege Escalation, Initial Access, Defense Evasion Credential Access, Exfiltration (TA0004, TA0001, TA0005, TA0006, TA0010)
  - The threat actor will use the situation at hand to manipulate the hospital visitors and ask for information that can later help them achieve their goal.
- STRIDE threat Elevation of Privilege
  - The social engineer can use the sad situation at hand, and manipulate the hospital visitors to give up information when they are in a vulnerable situation.

#### Students



- MITRE ATT&CK tactic Privilege Escalation, Initial Access, Defense Evasion Credential Access, Exfiltration (TA0004, TA0001, TA0005, TA0006, TA0010)
  - The attacker will understand that a student is more vulnerable than a potentially trained employee, and will use this to their advantage when implementing their phishing emails
- STRIDE threat Elevation of Privilege
  - The social engineer will again manipulate the young student into giving up information they did not even know was important

#### Computer Vulnerabilities:

As discussed prior, our organization has hundreds of computers at our disposal, while good for completing tasks, it means there are hundreds of risks associated with them as well. We have all types of operating platforms which all have their own vulnerabilities that we must constantly keep updated. Our potential vulnerabilities are as follows:

#### Linux - CVE Reference: CVE-2021-3177

A stack-based buffer overflow was discovered in the ctypes module provided within Python. Applications that use ctypes without carefully validating the input passed to it may be vulnerable to this flaw, which would allow an attacker to overflow a buffer on the stack and crash the application. The highest threat from this vulnerability is to system availability.

MITRE ATT&CK tactic Impact (TA0040)

STRIDE threat Denial of Service

#### Windows - CVE Reference: CVE-2021-43221

The vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed, up to and including the entire Internet. Such a vulnerability is often termed 'remotely exploitable' and can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers).

MITRE ATT&CK tactic Lateral Movement (TA0008)

STRIDE threat Elevation of Privilege

#### MacOS - CVE Reference: CVE-2021-30919

An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 15.1 and iPadOS 15.1, macOS Monterey 12.0.1, iOS 14.8.1 and iPadOS 14.8.1, tvOS 15.1, watchOS 8.1, Security Update 2021-007 Catalina, macOS Big Sur 11.6.1. Processing a maliciously crafted PDF may lead to arbitrary code execution.

MITRE ATT&CK tactic Defense Evasion & Execution (TA0005 & TA0002)

STRIDE threat Tampering

#### OpenVMs - CVE Reference: CVE-2017-17482

An issue was discovered in OpenVMS through V8.4-2L2 on Alpha and through V8.4-2L1 on IA64, and VAX/VMS 4.0 and later. A malformed DCL command table may result in a buffer overflow allowing a local privilege escalation when a non-privileged account enters a crafted command line. This bug is exploitable on VAX and Alpha and may cause a process crash on IA64. Software was affected regardless of whether it was directly shipped by VMS Software, Inc. (VSI), HPE, HP, Compaq, or Digital Equipment Corporation.

MITRE ATT&CK tactic Privilege Escalation (TA0004)  
STRIDE threat Elevation of Privilege

## Section 5: Risks

### Personal Health Devices Vulnerability

There is an ability to exploit vulnerabilities in these devices to deliver painful shocks to patients and/or to install ransomware or other malware on the systems.

Confidentiality - MODERATE

Integrity - MODERATE

Availability - MODERATE

Impact - Serious

Likelihood - Unlikely

Resulting Risk - Moderate

### Patient Monitoring Devices

Attacks against these devices could block alerts to nurses and/or give patients dangerous levels of medication or the wrong medicine in general.

Confidentiality - MODERATE

Integrity - MODERATE

Availability - HIGH

Impact - Significant

Likelihood - Rare

Resulting Risk - Moderate

### Scanners

An attacker with access to these systems could tamper images, resulting in misdiagnoses.

Confidentiality - LOW

Integrity - MODERATE

Availability - HIGH

Impact - Serious

Likelihood - Unlikely

Resulting Risk - Moderate

### Surgical Devices

Attacks against these devices could render our hospital unable to provide life-saving care or cause harm to a patient during surgery.

Confidentiality - MODERATE

Integrity - HIGH

Availability - HIGH

Impact - Severe

Likelihood - Rare

Resulting Risk - Moderate

### Server

Confidentiality - HIGH

Integrity - HIGH

Availability - HIGH

Impact - Severe

Likelihood - Possible

Resulting Risk - High

### Patient Records / Stealing

Confidentiality - HIGH  
Integrity - HIGH  
Availability - MODERATE  
Impact - Severe  
Likelihood - Possible  
Resulting Risk - High

Insider Threat  
Confidentiality - MODERATE  
Integrity - HIGH  
Availability - HIGH  
Impact - Severe  
Likelihood - Possible  
Resulting Risk - High

Internal Human Error  
Confidentiality - HIGH  
Integrity - MODERATE  
Availability - HIGH  
Impact - Severe  
Likelihood - Possible  
Resulting Risk - High

#### Social Engineering Attacks

Employees  
Confidentiality - HIGH  
Integrity - MODERATE  
Availability - HIGH  
Impact - Severe  
Likelihood - Possible  
Resulting Risk - High

Patients  
Confidentiality - HIGH  
Integrity - HIGH  
Availability - HIGH  
Impact - Severe  
Likelihood - Possible  
Resulting Risk - High

Visitors  
Confidentiality - HIGH  
Integrity - HIGH  
Availability - HIGH  
Impact - Severe  
Likelihood - Possible  
Resulting Risk - High

Students

Confidentiality - HIGH  
Integrity - HIGH  
Availability - HIGH  
Impact - Severe  
Likelihood - Likely  
Resulting Risk - Critical

Computer Vulnerabilities  
Confidentiality - HIGH  
Integrity - HIGH  
Availability - HIGH  
Impact - Severe  
Likelihood - Likely  
Resulting Risk - Critical

## Section 6: Mitigations

### Personal Health Devices Vulnerability

This is an ability to exploit vulnerabilities in these devices to deliver painful shocks to patients and/or to install ransomware or other malware on the systems.

This could be mitigated by continuing to program, test, and evaluate different patients. We should also maintain control of our programmers within our facility at all times according to our IT policies. We should also only use home monitors, programmers, and implantable devices obtained directly from the manufacturer to ensure integrity of the system. We should also remind patients to keep their home monitors plugged in.

- The benefits of remote wireless monitoring of an implantable device outweigh the practical risk of an unauthorized user exploiting these devices' vulnerabilities.
- The monitor must remain powered on to ensure timely transmission of any wireless CareAlerts programmed by the physician and to ensure automatically-scheduled remote transmissions occur at the specified time. (FDA 2).

### Recovery Security Control Function

We can make disaster recovery plans in which we plan for the worst in case a health device like a defibrillator malfunctions.

### Physical Controls Repair Capability

We can make sure that we can repair any malfunctioning device

### Patient Monitoring Devices

Attacks against these devices could block alerts to nurses and/or give patients dangerous levels of medication or the wrong medicine in general.

According to the report, investigators from McAfee purchased from eBay a bedside monitor and central monitoring station just like the ones used by several hospitals. They then simulated the setup typical in hospitals, where vital signs from multiple patients' bedside monitors can be viewed by doctors and nurses in a centralized hub or monitoring station. Then the investigators found that they could alter the information transmitted to the monitoring station in such a way that they could make it appear that one patient's heart rate was too high or too low. Depending on the numbers, providers would have to decide to treat that patient with medication (Journal Of Ahima, 2).  
<https://journal.ahima.org/vital-sign-monitors-pose-vulnerability-to-hacking/>

### Deterrent Security Control Function

### Technical Controls Repair Capability

We can have intrusion detection and audit log reviews that our monitoring devices give us, along with securing our internet and server better.

### Scanners

An attacker with access to these systems could tamper images, resulting in misdiagnoses.

To mitigate this risk I would implement a third party, by teaming up with JFrog, a company who "provides an end-to-end, hybrid, secure and universal DevOps Platform for continuous delivery of software updates. With easy integration into your DevOps ecosystem and Openshift certification." (JFrog 1).

### Preventative Security Control Function

### Administrative Controls

We can go with this third party, and have a separation of duties, and classify data better.

## Surgical Devices

Attacks against these devices could render our hospital unable to provide life-saving care or cause harm to a patient during surgery.

We can mitigate this by making a checklist we must adhere to avoid such as the following:

- Network vulnerability with the lack or the adoption of basic security measures, robotic systems are vulnerable to various wired/wireless communication and connections attacks including replay, man-in-the-middle, eavesdropping, sniffing, spoofing, etc.
- Platform vulnerability includes the lack of constant updates of software and firmware patches, as well as security patches to maintain a secure up-to-date robotic system. This results into also having configuration and database vulnerabilities.
- Application vulnerability applications that are not tested and evaluated for coding or compatibility bugs, can also affect the robotic system's performance. Hence, further testing is essentially required.
- Security vulnerability the adoption of new security measures without thorough testing can sometimes affect the performance of both robotic systems and devices. Hence, testing is essential before deployment.
- Bad practice vulnerability includes the bad choice of security measures and means, as well as lack of coding skills, which can be easily re-modified to cause errors or to perform the wrong tasks.
- Update vulnerability robots are also prone to update vulnerabilities that can cause their systems and operating systems to act differently due to the new update, including the loss of unsaved data, interruption of the ongoing process, etc.
- Heterogeneity and homogeneity vulnerability the heterogeneous nature of robotic systems makes their integration prone to many security issues. Moreover, their homogeneous nature also leaves them prone to similar attacks with possibly cascading effects. Management vulnerability includes the lack of advised planning, security guidelines, procedures and policies. (SpringerLink 2021)

## Server / Network

Mitigations for our servers and network, we must follow these steps

1. Conduct a risk assessment to determine vulnerabilities
2. Establish network access controls  
Once we have assessed your assets and identified high-priority problem areas, the next step is to establish network access controls to help mitigate the risk of insider threats. Many organizations are turning to security systems such as zero trust, which assesses trust and user access privileges on an as-needed basis depending on each user's specific job function. This helps minimize both the likelihood and impact of threats or attacks that occur due to employee negligence or a simple lack of awareness of cybersecurity best practices. Additionally, as the number of connected devices on a network increases, endpoint security will also become a growing concern.
3. Implement firewalls and antivirus software  
Another important cybersecurity risk mitigation strategy involves the installation of security solutions such as firewalls and antivirus software. These technological defenses offer an additional barrier to your computer or network. Firewalls act as a buffer between the outside world and your network and gives your organization greater control over incoming and outgoing traffic. Similarly, antivirus software searches your device and/or network to identify any potentially malicious threats.

4. Create a patch management schedule  
Many software providers release patches consistently, and today's cybercriminals are aware of that. As such, they can quickly determine how to exploit a patch almost as soon as it is released. Organizations should be aware of the typical patch release schedule among their service or software providers to create an effective patch management schedule that can help your organization's IT security team stay ahead of attackers.
5. Continuously monitor network traffic
6. Build an incident response plan

#### Patient Records

Mitigations for our records require some physical infrastructure broadening along with more employee training.

- Create a multidisciplinary team with executive leadership to identify privacy and security issues, set priorities, and standardize access and disclosure practices.
- Conduct periodic assessments of risks and controls to identify gaps in privacy and security. Update policies, procedures, and technology accordingly—specify who may access what PHI and what to do if a breach has occurred.
- Encrypt all electronic information using the National Institute of Standards and Technology standard for data at rest and data in motion. If an unencrypted device, drive, or piece of data is stolen or misplaced, the Office for Civil Rights automatically presumes a HIPAA breach. Breach notification is not required because the information can't be accessed without a key.
- Use technology to detect and prevent unauthorized use and transmission of electronic data. Applications are available to continually monitor software and system hardware for outside threats and security risks. Ensure effective management of privacy and security controls.
- Establish authorization processes to continually monitor PHI disclosures. Develop a comprehensive ROI manual providing step-by-step instructions for handling each aspect of the disclosure process aligned with HIPAA requirements.
- Invest in cyber insurance to help mitigate the financial risks of breach. Be sure to determine both the extent of coverage and the cost.
- Provide ongoing enterprise wide education and training to promote understanding of organizational policies and procedures as well as relevant laws and regulations governing disclosure of PHI. Follow each training program with an assessment to measure effectiveness (For The Record, 1).

#### Social Engineering Attacks

The social engineer will use persuasion to request information from their victim, such as account logins, payment methods, contact information, etc., that they can use to commit their cyberattack. A person's natural tendency to avoid doing something wrong or to get in trouble will be exploited. If an attacker can make an employee feel that he or she caused a problem or performed a task incorrectly, then the employee may become open to suggestion and thereby agree to compromise a policy or standard in order to correct the perceived error, which then leads to a breakdown in information security protocols.

To mitigate this we can follow 5 steps:

1. Build a positive security culture
2. Learn the psychological triggers
3. Train our staff



4. Test the effectiveness of the training
5. Implement appropriate technical instruments

If we want more on how to understand these triggers we can reference my groups final paper or my youtube video!

## References

- Adopting the NIST Cybersecurity Framework in Healthcare.*  
<https://docs.broadcom.com/doc/adopting-the-nist-cybersecurity-framework-in-healthcare-en>
- “DDoS Attacks: In the Healthcare Sector.” C/S, 10 Oct. 2016, [www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/](http://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/).
- Health, Center for Devices and Radiological. “Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication.” FDA, 30 Jan. 2020, [www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home](http://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home).
- MEDICAL EQUIPMENT LIST for TYPICAL DISTRICT HOSPITAL.*
- “Red Hat Ecosystem Catalog.” *Catalog.redhat.com*, [catalog.redhat.com/software/vulnerability-scanner/detail/jfrog\\_xray](http://catalog.redhat.com/software/vulnerability-scanner/detail/jfrog_xray). Accessed 12 Dec. 2021.
- “Seven Strategies to Mitigate Privacy and Security Risks during the ROI Process - for the Record E-News Exclusive.” *Www.fortherecordmag.com*, [www.fortherecordmag.com/news/enews\\_1015\\_01.shtml](http://www.fortherecordmag.com/news/enews_1015_01.shtml).
- Yaacoub, Jean-Paul A., et al. “Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations.” *International Journal of Information Security*, 19 Mar. 2021, 10.1007/s10207-021-00545-8.