Outline for the Speech Presentation

- The healthcare sector is one of the most important aspects of our modern day society. Not only do they provide us with the care and treatment that we need when ill or injured, but they house some of our most private, intimate and valuable information about ourselves. Such information thus needs to be guarded with the utmost care to protect patient confidentiality.
- So today, we will be going over
    - The major threats the healthcare industry faces in terms of cyber security
    - The preventative measures healthcare companies need to take

Slide 1:

- Good Evening everyone. Today we will be presenting a cybersecurity threat analysis and recommendations for enhancing security measures within the healthcare system.

Slide 2: Current State of Cyber Threats

- The cybersecurity landscape is constantly evolving, with healthcare organizations facing a wide range of sophisticated threats. Some major threats include phishing attacks, ransomware, insider threats, distributed denial-of-service or DDoS attacks, and advanced persistent threats designed to remain undetected for extended periods while stealing sensitive data.

Slide 3: Cyber Attacks in Healthcare

- The healthcare industry has become an attractive target for cybercriminals due to the valuable nature of patient data and the potential for financial gain through fraud or extortion. Alarmingly, around 45% of healthcare organizations have experienced a data breach in recent years. One high-profile example is the 2015 Anthem Data Breach, which exposed the personal information of nearly 79 million individuals and cost the company up to $260 million to address.

Slide 4: Impacts of Cyber Attacks

- The impacts of cyber attacks on healthcare organizations can be devastating, ranging from significant financial losses to reputational damage and loss of customer trust. On a personal level, compromised data can lead to identity theft, financial losses, and mental health implications for affected individuals.

Slide 5: Modes of Attack

- Attackers employ a variety of modes to infiltrate healthcare systems, such as malware and software exploits, web application attacks targeting patient portals and electronic health records, vulnerabilities in cloud and remote access solutions, as well as attacks on Internet of Things devices and medical equipment with limited security controls.

Slide 6: Recommended Security Measures

- To effectively mitigate these threats, we recommend a multi-layered security approach. This includes implementing firewalls, data encryption, intrusion detection and prevention systems, as well as robust employee training programs. Organizations should also have

thorough third-party risk management methods, continuous monitoring and threat intelligence, secure configuration and patch management procedures, incident response and disaster recovery plans, and more.

Slide 7-

Firewalls are usually the first line of defense when it comes to security. They are placed between the Local Area Network, the internal private network, and the Wide Area Network, the internet. They block incoming and outgoing traffic based on predefined rules, such as ip addresses, transport layer protocols, and port numbers, so known malicious packets wouldn't be able to enter as traffic has to pass through the firewall.However, firewalls shouldn't be used as the only form of security as it has it's vulnerabilities, including IP spoofing, where IP address is intently changed from the original, packet redirecting, where a packet's path is redirected past the firewall, and DDoS, distributed denial of service attacks.

Slide 8-

The OSI Open System interconnection layer has seven layers and each layer tells about how packets, information, are transferred to and from different end systems. A good firewall depends on several environmental conditions and constraints, such as it's placement in the OSI layer and the kind of data protected. There are two categories of firewalls categorized as cloud firewalls and traditional firewalls. Studying cloud firewalls are essential because of the ongoing move towards cloud based servers for healthcare systems. For cloud based firewalls we have the next-generation firewalls which offer advanced attack detection and removal features for cloud environments, but are often costly and very complex to implement. Packet filtering firewall at the traditional level, which operates at the network layer, managing IP addresses. However, it's too vulnerable and cannot prevent a lot of attacks. Therefore, to implement a firewall, you need to consider the placement, adaptability, user friendliness, flow of network, financial cost and secureness. Upon careful research the firewalls that are best suited for the healthcare system are the WAF, less complex than Next Gen, protects against the application layer, HTTP traffic and log monitoring. They also establish a secure socket layer, which encrypts the data in a connection, making it more confidential and secure. For traditional firewalls, we have the stateful inspection firewall, like a dynamic packet filtering firewall but keeps track of all packet information previously processed, preventing spoofing risks. They are more ideal than the application firewall because of less overhead which can increase traffic.

Slide 9-

What if data happened to be intercepted, hacked? The attacker could read the data and potentially leak it, but they would have a harder if not impossible time doing so, with proper encryption of the data. Encryption uses an algorithm and a key to scrambled the readable data to an unreadable form. The only way to read the data is if you have a key that can decipher it, usually shared between trusted individuals. Different types of

encryptions includes symmetric encryption, where the same key is used to encrypt and decrypt, which causes security risks as a way to distribute the key is needed. However, they are fast which makes them ideal to use. AES was introduced recently as of 2000, faster and more powerful than DES, involving key lengths of 128/192/256 bit which most healthcare systems use, and so far there is no known optimal methods to break AES. Asymmetric encryption uses a public key for encrypting and a private key for decrypting, so users only have to know the receiver's public key to encrypt data, and the receiver can decrypt with their own private key. Because of the slow amount of time for asymmetric encryption, they are typically used along with symmetric encryption to first secure a private connection, then transfer data using a symmetric key. They are also used in digital certificates, non-repudiation, that the information came from the actual sender, and not some unknown entity, as asymmetric encryption goes both ways the public key can be used to decrypt the private key. Hashing is the last encryption algorithm and they ensure integrity, that the message has not been tampered with. How hashing works is that information once hashed, cannot be unhashed, so it's typically used to compare passwords, as passwords stored on the system are hash values, and compared data sent. These three encryption methods are necessary and work together to ensure confidentiality, integrity, and non-repudiation providing a good user experience.

Slide 10-
IDS [Intrusion Detection System] maintains network traffic, looks for unusual activity and sends alerts when it occurs to the administrator. It looks for patterns in the traffic indicating unusual behavior.
Two types of IDS are Network-Based IDS and Host-Based IDS. Network-Based IDS monitors network traffic, effective against attacks that target multiple hosts and works together with the firewalls to aid in preventing malicious attacks.
Host based IDS monitors activities on individual hosts servers, by examining system logs, file integrity, user activities and network connection, therefore providing a more secure detection but only on a small scale as it cannot detect network traffic.
NIDS can be deployed on a large scale in the infrastructure, monitoring the machines, and HIDS can be deployed on the server and data centers to help secure information.

Slide 11-
IPS [Intrusion Prevention System] is just IDS but with the added authority to block malicious traffic. It uses Signature, patterns that have been defined as malicious to detect attacks, and anomaly behavior patterns that indicate malware. Like IDS, IPS has network based IPS which works in the whole network, and host based IPS which works in individual hosts. IPS can use a sandbox approach, where it quarantines code in an isolated area, runs the code, and monitors it's behaviors.
IPS is more of a problem to false positives, because then it can block good traffic from entering the network.

Jeremy Convocar section:
Cybersecurity tech, antivirus softwares, firewalls, etc. are all well and good, but they can only do so much in preventing malicious attacks in your organization, especially if your employees are not as tech savvy or cybersecurity literate.

This is why it is extremely important to do regular cyber-security trainings for all relevant employees, even for hospitals and healthcare sectors. Anyone who deals with the organization's

Spotting a Phishing Scam:
Ask Yourself any of the following when sent any sort of email, text message or online message, be it within your job or life:

1. Is this message asking me to input or give sensitive information or credentials?
2. Is this the first message you have received from this specific sender?
3. Does their number, email address, or username match with an official organization? (or have a mismatched email domain)
4. Does the sender use unfamiliar language or greetings than they would normally use?

Is there generally bad grammar or spelling within the message?

If you answer yes to any of these, hesitate and think twice before giving the sender any confidential information or access. Confirm with the sender in person, or via another platform, and especially confirm with higher up security management and report the suspicious message.

Good Password/Passkey
Myth: You should change your passwords every year or two.
Fact: The frequency in which you change your password is dependent on how strong it is, how often your account is used, etc.

- Nowadays, numbers such as every 30, 60 or 90 days are being thrown around by experts.
- Best practices are to change your password after any of the following:
    - After a Security Breach that affects one or more services you use/work for.

Other general tips (personally):

- If a password is easy to remember for you - it also is likely easy to guess! Strike a balance between rememberability and complexity.
- Avoid using personal life details such as birthdays in your password, or at least combine them with unexpected phrases, characters, etc.
- Keep a physical password book incase you are bad at remembering passwords and keep it safe, well-hidden and secure

NIST Password Recommendations

- The National Institute of Standards and Technology (NIST) actually has a guideline released every few years on good password habits. It is important to have employees keep up to date with these standards.

- The NIST recommends always having Single Sign-On (SSO) and Multi-Factor Authentication (MFA) enabled
- Authentication always consists of three different things: something you KNOW (passwords, PIN numbers), something you HAVE (Authentication App, Keycard), something you ARE (fingerprint scanner, retinal scanner, biometrics)
    - It is recommended that you have 2 out of 3 of these authentication methods atleast
    - Multi Factor Authentication Options typically include:
        - SMS verification
        - Authentication applications like the one we as NJIT students use

The Health Sector Cybersecurity Framework Implementation Process

- This is a 7 step process, outlined and recommended by the ASPR (Administration for Strategic Preparedness and Response) under the U.S. Department of Health and Human Services.
- Informative References - standardized information and references that help an organization grow and achieve core outcomes for cyber security. This is
- Each step of the process is meant to provide input/resources for the step that follows it in the process,

1. Prioritizing and Scoping -
    - Within this step, the organization should decide how it wants to allocate and prioritize its resources and risk management. Strategize on how risks and threats should be responded to and have your systems categorized.
    - Focus on high value targets and critical systems, then work your way and focus down to less critical ones (as resources will permit)
2. Orientation -
    - In this step, the organization and employees familiarize themselves with the systems, assets, compliance/best practice requirements and approaches that are at their disposal.
3. Creating the Target Profile -
    - The target profile acts as the desired goal/state for the organization in terms of its cybersecurity. This profile is tailored to the Informative References the organization has.
4. Conduct a Risk Assessment -
    - Identify and evaluate potential threats, weak points and fault tolerances within the organization.
    - Some organizations already have risk assessment as part of typical business practices, but it is important to make sure the cybersecurity of the organization is also assessed via internal audits, as well as outside analysis from dedicated cybersecurity groups and firms.
5. Creating a Current Profile -
    - The current profile is created by assessing the organization as it currently stands.
        - What is the current situation for cybersecurity within the organization?
        - What practices are being practiced? What safeguards are currently in place?

6. Gap Analysis
    - Analyze the gaps between the two profiles created.
    - Determine which gaps need to be addressed based on each one's potential consequences
    - Identify the actions that will be taken to resolve these gaps
    - Perform cost benefit analysis (CBA) on your possible actions
    - Prioritize and implement actions.
7. Action Plan

Act upon the actions discussed in step 6 and get the informative references and resources required.

Repeat the cycle onto step 1. This process is meant to be a cycle in order to keep up to date with one's cybersecurity assessment.