John Guerrerio
COSC 19.02
10/7/2023

Security of Electronic Medical Records

Abstract

As the Digital Revolution has progressed, healthcare has become dependent on Electronic Medical Records, or EMRs. While EMRs reduce hospital costs and streamline patient care, they also present a target for attackers looking to sabotage the hospital's operations or exploit the confidential nature of EMRs to make a profit. In this paper, we examine the security of EMR systems, model potential adversary attacks against an EMR system, and use these attacks to infer mitigations system administrators can take to secure their EMR systems. We find that the two primary vulnerabilities of EMR systems are insecure endpoints (e.g., unsecured patient computers, MIoT devices coded without considering security, etc.) and social engineering attacks. We propose several mechanisms to secure these endpoints, as well as reducing a user's ability to arbitrarily execute code to reduce the probability of success of phishing attacks.

Section 1: Introduction

As the world has become increasingly digitalized so too has medical care. From the Internet of Medical Things (medical devices connected to the internet such as a glucose monitor) to telemedicine and AI-powered diagnostic tools, healthcare has become inextricably linked with computing. One of the most significant changes in this direction is the widespread adoption of Electronic Medical Records, or EMRs. EMRs are digital versions of a patient's medical records, such as a patient's chart or a doctor's notes after a visit. These records typically contain diagnoses, medical histories, medications, allergies, radiology images, lab and test results, progress notes, vital signs, patient personally identifiable information (PII), and billing information.[1] They are used by doctors to determine a patient's medical history, manage their medications and treatment, record their diagnoses, and determine the patient's recovery progress. As such, EMRs are highly critical and interface with nearly all hospital systems, such as Medical Internet of Things devices, doctor workstations, patient devices (to view their information), pharmaceutical systems, insurance providers, and so on. EMRs have many benefits. At 90% adoptions, EMRs could save $77 billion dollars each year, reduce errors in medication administration, and automatically encourage at-risk individuals to seek preventative care.[2] Doctors no longer need to find a patient's paper chart, reducing time spent searching for records and facilitating greater information sharing between multiple healthcare providers.

However, EMRs offer a highly attractive surface for cyberattacks. Unlike credit card numbers, which are monitored and can be easily changed in the event of fraud, EMRs contain difficult-to-change PII, such as social security numbers and Medicare numbers.[3] This information can be used to commit medical identity fraud, file fraudulent taxes or insurance claims, take out a fraudulent loan, or commit identity theft.[4] As such, EMRs are sold on the black market for roughly $50 a record – about ten times the worth of a credit card number.[5] If someone were to alter the content of an EMR, the resulting errors in treatment could be life-threatening. This threat is especially relevant to high-profile individuals like celebrities or politicians, who are already targets.[6] Finally, if the availability of EMRs were compromised, all treatment would grind to a halt, again with life-threatening consequences.

Despite the extreme need for cybersecurity of EMRs, healthcare is a uniquely vulnerable domain. Healthcare organizations have traditionally focused their resources on patient care, leaving few resources left for cybersecurity (sometimes as little as 1-2% of their annual IT budget, compared to 4-10% in other sectors).[7] Healthcare systems contain many non-traditional endpoints, such as integrated medical devices with built-in middleware that allows the integrated sensor to automatically access and update a patient's EMR.[8] Many healthcare organizations are still reliant on legacy systems leaving them vulnerable to publicly disseminated exploits.[9] Many medical devices run proprietary software, leaving hospital IT reliant on the manufacturer to patch vulnerabilities.[10] Complicating things further are regulations such as HIPPA, which limit how hospitals can use EMRs and penalize data breaches.[11] As such, there is an urgent need for hospitals to secure their EMRs.

Section 2: Approach

This paper follows a three-phase approach. The first phase is a set-up for the following analysis.[12] To gain a better understanding of the domain and analyze how an adversary may attack an EMR system, we develop a model of the healthcare organization's mission, the system itself (modeled as a network diagram, a data flow diagram, and a functional block diagram), and the adversaries who are most likely to attack an EMR system. We use this analysis to choose a set of probable goals an adversary targeting an EMR system might have. We calculate the monetary harm of attacks along these goals if they were to succeed (including both direct costs like HIPPA violation fees and indirect costs like loss of patient trust in an organization) and the probability of such attacks succeeding. This gives us the risk of these strategic attack goals.

The second phase is a deep analysis of the most likely attacks against an EMR system.[13] We first condense similar strategic attack goals into a single goal, creating a subset of representative attack goals. We then generate an attack tree for each representative attack goal, which models all possible methods of attack that would accomplish the strategic attack goal. We compute the probabilities of each leaf (the steps an attacker could take to accomplish the strategic attack goal) and use them to estimate the probability of an attacker accomplishing their strategic attack goal.

The third and final phase applies what was learned from our previous models.[14] Using our attack trees, we refine our expected harm estimates for each strategic attack goal. We then extract all cut sets from each attack tree; these are minimal sets of leaf nodes that would allow an attacker to accomplish their strategic attack objective. We use these cut sets to develop possible mitigation packages that would allow a healthcare organization to reduce their cybersecurity risk.

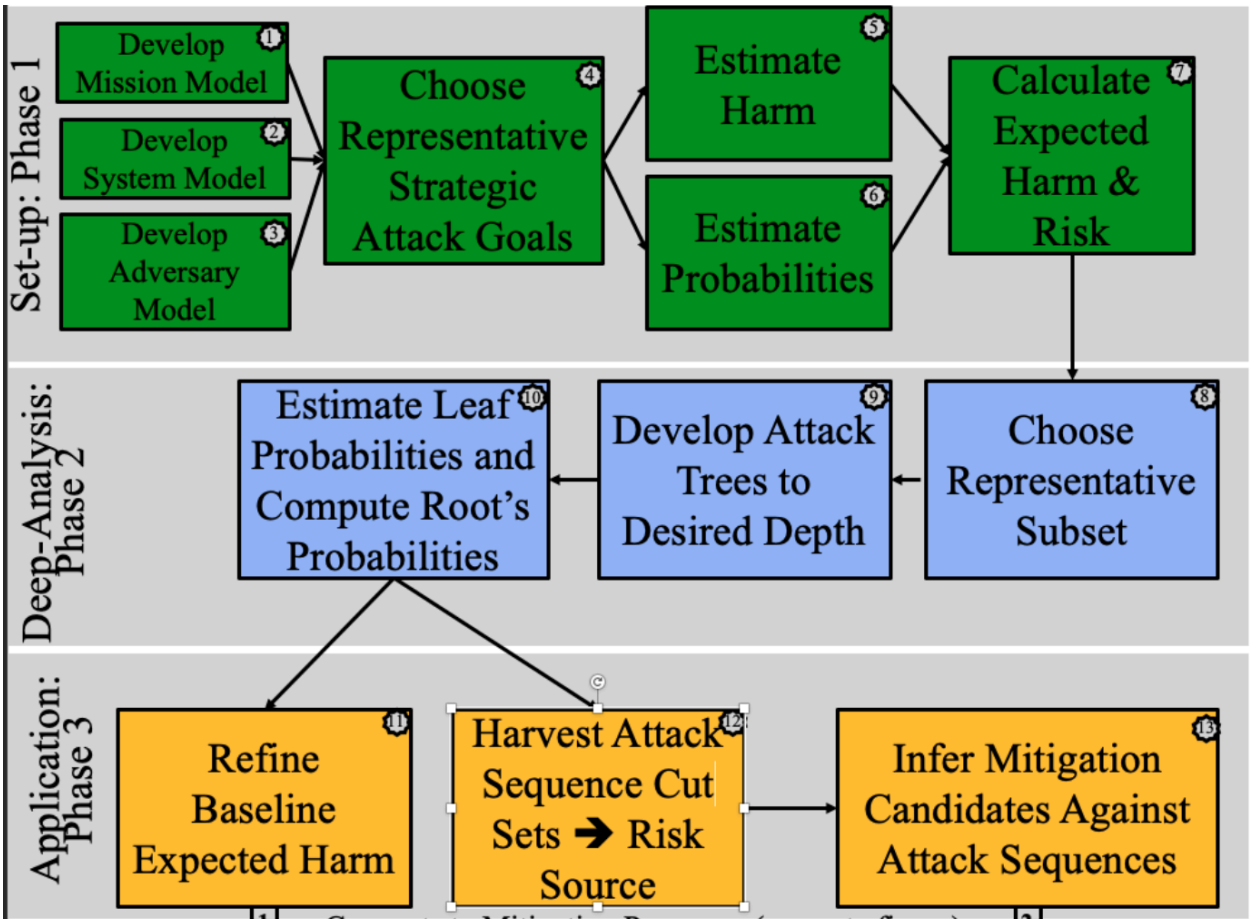

Figure 1: High-Level Risk Analysis Approach

Section 3: Mission Model

The mission of a healthcare organization is simple: to provide care to patients. One of the best hospitals in the world, Johns Hopkins Hospital, has as its mission statement: "To improve the health of our community and the world by setting the standard of excellence in patient care."[15] This care includes many specialized areas, such as cancer treatment, emergency surgery, pediatric care, and many more. However, each area of care is completely dependent on the information contained in EMRs. EMRs contain diagnoses and care histories that inform a doctor's decisions, scheduled treatments, send medication orders to pharmacies, and bill insurance companies. Without this information, a doctor cannot provide a patient with care. Thus, the mission of the EMR system is threefold: to collect accurate patient medical information, store that information securely, and allow the proper parties to access that information. We assess each sub-mission in turn:

- Collect Information: An EMR system is worthless if it contains no information. Thus, the system must have some way of collecting information about patients. This information is primarily entered by the doctor in the form of visit notes and patient charts (from either an internal hospital workstation or a secure, hospital owned portable device like a laptop). The patient is responsible for providing information such as his/her demographics, billing information, and/or any unhealthy habits (e.g., if they smoke). Most EMRs have a patient-facing portal to enter this information (for Epic, the patient portal is called MyChart). Additionally, third parties need to be able to add information to a patient's

EMR. The results of diagnostic tests done by a third party (e.g., LabCorp) need to be incorporated into a patient's EMR. OpTime, a software that helps schedule a patient's surgery and provides support during the operation, needs to be able to add information about the operation. Radiology companies need to be able to update patient X-rays. If a patient receives treatment across multiple hospitals or healthcare providers, his/her EMR needs to reflect the treatment from each organization. Medical Internet of Things Devices like pacemakers need to be able to add information about their wearer to his/her EMR.

- Store Information: Once collected, EMRs must be stored securely. EMRs must be carefully cataloged and organized so that they can be retrieved when needed. This sub-mission is highly dependent on integrity. If the validity of an EMR cannot be guaranteed, the system is worthless. Moreover, if consumers do not know the integrity of records in an EMR has been violated in a certain way, it could lead doctors to make decisions that harm a patient. For example, if an EMR has been maliciously modified to state a healthy patient has cancer, it could lead doctors to begin chemotherapy. Additionally, EMRs must be stored in such a way that their confidentiality is protected. If unauthorized parties can view a person's EMR, this constitutes a data breach, and the system fails this sub-mission.
- Retrieve Information: Authorized parties must be able to retrieve information from an EMR system. These parties are varied and include organizations outside of the hospital. In addition to doctors, who need to see a patient's medical history and diagnoses (once again, via internal hospital workstations and hospital-owned portable devices), and patients, who need to review their medical information, test companies need to receive test orders. Pharmacies need to retrieve a patient's prescription. Insurance companies need to access a patient's billing information. Third party healthcare providers need to access a patient's prior medical history. Radiology companies need to know which X-rays of a patient to take. OpTime (a software running on top of the Epic EMR management software that manages surgeries) needs to extract a patient's diagnoses and planned surgeries to schedule the surgery and aid in the operation. The EMR system must allow all of these parties to access records when appropriate while also keeping bad actors from violating a patient's confidentiality. This is difficult, as the sheer number of types of users (and the high volume of users) create a multitude of attack surfaces for adversaries to exploit.

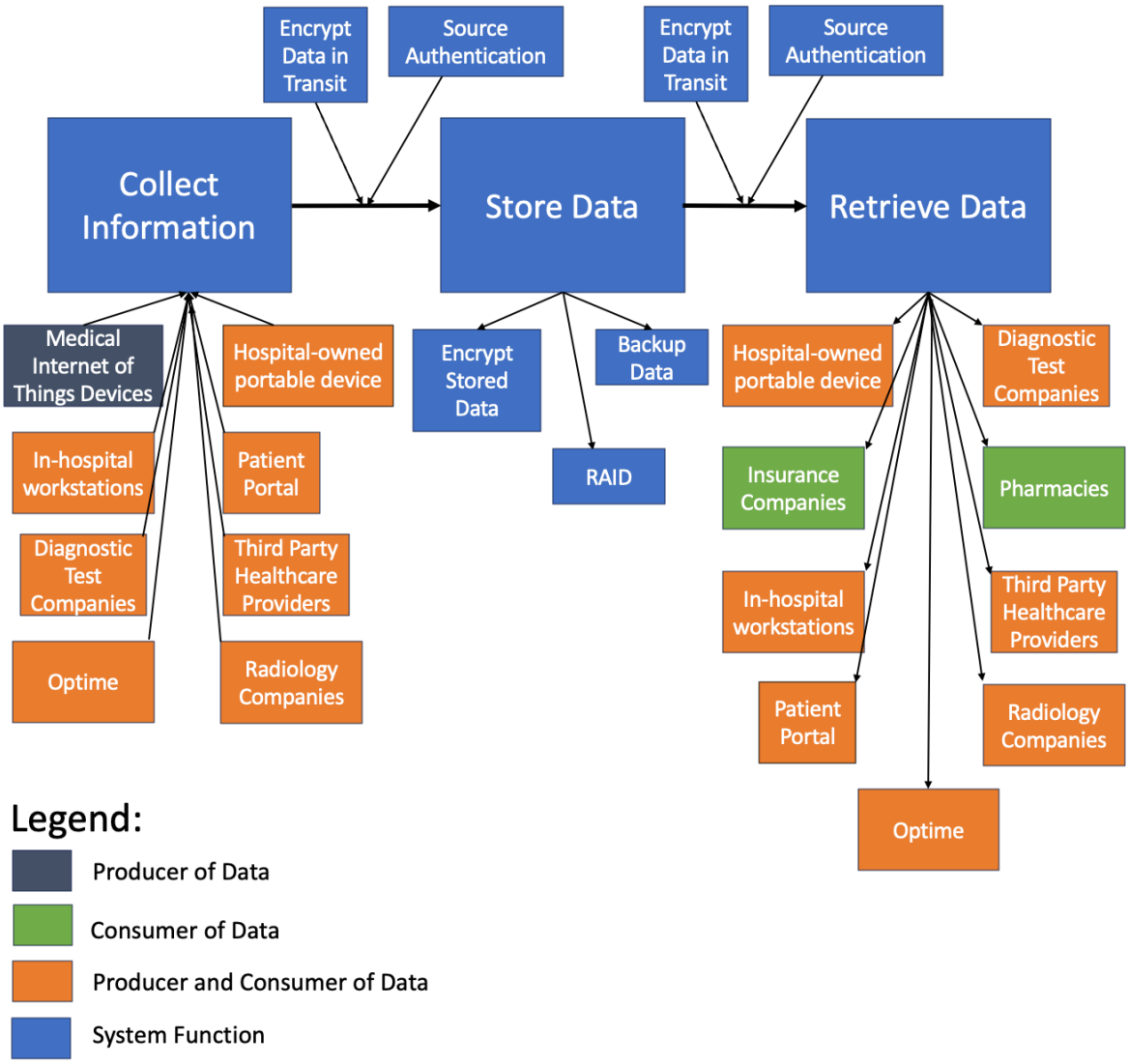

Figure 2: Functional block diagram for an EMR system. It visualizes the sub-missions of the system and their components.

Section 4: System Model

Below is a network diagram for a sample EMR system. Please note that due to the confidential nature of these systems, there is little publicly available information on their network architecture. However, with knowledge of their components and widely used cybersecurity components, one can extrapolate a likely network diagram for such a system.

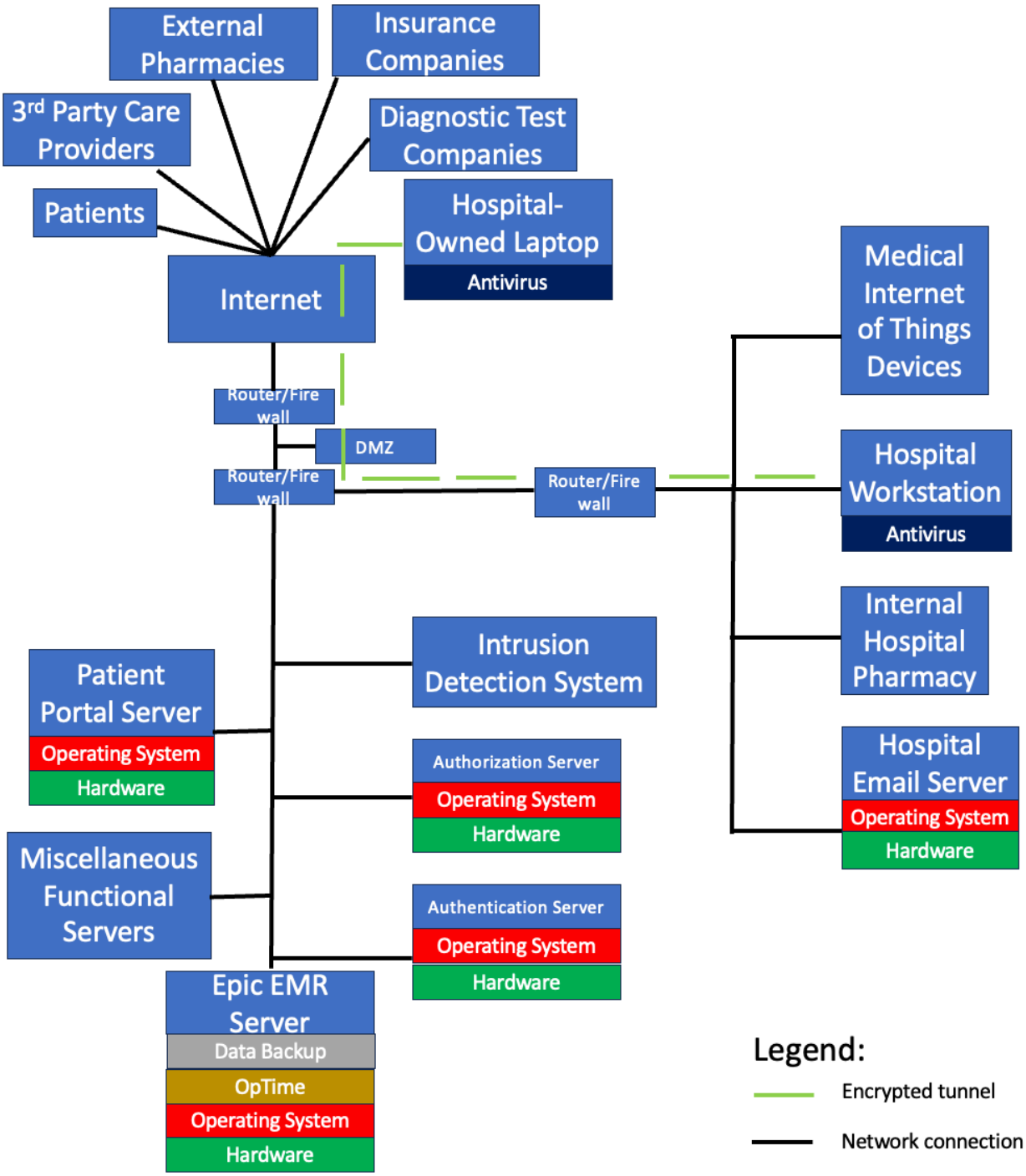

Figure 3: Representative EMR System Model

The hospital systems are divided into two separate subnetworks: an internal working hospital network and an EMR network. The working hospital network contains devices that assist in the day-to-day operations of the hospital: medical internet of things devices that administer treatment to patients and monitor their condition, workstations that allow doctors to query and enter patient information, an internal pharmacy that allows easy access to crucial medications, and an email server that handles confidential patient communication. Every system

on the internal hospital network that needs patient data can query it from the EMR network. The EMR network contains a patient portal that allows patients to access their medical information, and authentication server and an authorization server to manage access, an intrusion detection system to protect the network, and other various miscellaneous functional servers. The division between the internal hospital network and the EMR network help maintain the security of the EMR network and makes it harder for attackers to access the EMR network from the internal hospital network. Both of these networks are protected from the Internet by a Router/Firewall, a DMZ that contains the hospital's internet-facing services, and another Router/Firewall. Patients, insurance companies, and other third parties connect to the hospital's perimeter access point via the internet and are routed to the appropriate resource within the network. Doctors with a hospital-owned laptop can use a VPN to establish an encrypted tunnel that connects them directly to an internal hospital owned workstation and access internal hospital resources remotely.

The Epic EMR server contains all the hospital's EMRs. It runs on a software called Epic; a specialized database software designed specifically for medical records. The OpTime software is a module within Epic; it also runs on the Epic EMR server. EMR backups are stored on the EMR server. The EMR server contains a wide variety of data. A single patient's medical record includes billing information, diagnoses, test results, medications, and clinical notes from their visits. There are several different kinds of clinical notes, including progress notes detailing patient status, consultation notes containing the response to a request from a clinician for advice from another clinician, procedure nodes detailing medical interventions on the patient, the patient's medical history prior to their hospitalization, and a discharge note summarizing their admission and medical course in the hospital.[16] Notably, the EMR also includes information about patients in clinical trials. For example, if a patient was enrolled in a study to test the efficacy of a new drug, the details of the study and the patient's response to that drug would be stored on the EMR.

Due to the large number of users and wide variety of data types stored on the EMR system, we now provide several examples of data and control flow for the system:

- A patient on their personal device finds the patient portal server through DNS (not depicted), connects to it through two firewalls, makes a request in the form of a database query, which is returned by the patient portal via a TCP-IP link.
- A doctor on their hospital-owned laptop uses their VPN to establish an encrypted tunnel with an internal hospital workstation and connects directly to the workstation over this encrypted tunnel. They pass their EMR query to the workstation over the tunnel, which queries the EMR server and returns the results over the VPN.
- A diagnostic testing company uses a pre-provided private key to establish an encrypted connection with the EMR server, they send a patient test result to the EMR server digitally signed for integrity and confidentiality, the EMR server verifies this digital signature, and adds the test result to a patient's medical record.
- An insurance company uses a pre-provided private key to establish an encrypted connection with the EMR server and sends a digitally signed query for patient billing information. The EMR server verifies this digital signature and sends patient billing information over this encrypted connection.

Section 5: Adversary Model

We now discuss three classes of adversaries that would be likely to attack an EMR system: organized criminals, transnational terrorists, and nation states at peace. We discuss each adversary class in turn.

- Organized Criminals: These are groups of well-resourced, highly skilled cybercriminals such as the Russian mafia.[17] Their goals are primarily financial over a medium-term time-horizon, and they are relatively risk-averse (to avoid detection). In this department, an EMR system is a perfect target. Organized criminals have two methods of gaining money by breaching an EMR system; they can either encrypt the EMR data and demand a ransom in exchange for the decryption key, or they can steal the data and sell it on the black market for roughly $50 a record.[18] The first method, called ransomware, is especially effective against hospitals because every day an EMR system is down is life-threatening for patients who need urgent care. EMR data is also high value on the black market, more so than credit card numbers. These factors, combined with relatively low security, make EMRs a tantalizing target for criminals.
- Transnational Terrorists: Transnational terrorists are well-resourced, highly skilled groups dedicated to causing chaos.[19] As they want to be identified after an attack, they are risk tolerant. Their goals are short-term, and sabotage focused. An EMR system is a high-value target to sabotage. Like cybercriminals, transnational terrorists know that if an EMR system goes down, patients will be unable to receive treatments and will likely experience adverse medical outcomes as a result. Sabotaging a hospital is a high-impact, high-publicity attack that would advance a terrorist organization's mission of sowing fear.
- Nation State at Peace: A nation state at peace is extremely well resourced and extremely skilled.[20] They have access to the most sophisticated attack methods and have nearly unlimited resources. Some nation states, such as the United States, are risk averse (as they do not want to be publicly shamed for a cyberattack), while nation states that do not respond to public shaming like Russia and China are more risk tolerant. These adversaries work over a long-term time horizon and are focused on influence operations and espionage. According to the Department of Homeland Defense, health care systems are top targets for both Russia and China in 2024.[21] These countries hope to steal US biomedical information and prepare for sabotage operations they would carry out in the event of a conflict with the US.[22] EMR systems primarily play into the second part of this strategic goal, as a denial of service on an EMR system can lead to a complete denial of service for a hospital. Additionally, patient information related to clinical trials is valuable research that a nation-state might be interested in stealing.

From examining the adversary classes most likely to attack EMR systems, one can see the need for increased cybersecurity is dire. All three classes are highly skilled, well resourced, and capable of deploying sophisticated attacks. The trend within healthcare to shirk cybersecurity in favor of providing patients with better care, while admirable, does not match the reality of the significant threats healthcare organizations face. Put simply, healthcare organizations currently do not have enough cybersecurity to carry out their mission.

Section 6: Representative Strategic Attack Goals

We now develop a set of representative strategic attack goals for a cyberattack against an EMR system. This phase of the risk assessment develops a set of strategic attack goals that are intended to span the most important threats to an EMR system's mission. We derive these

strategic attack goals from a combination of mission understanding, adversary understanding, and the areas of value for adversaries.[23] While it is impossible to enumerate over all possible strategic attack goals, the chosen set is sufficiently representative of most classes of attacks that could be performed against an EMR system. We break down the strategic attack goals into three classes: confidentiality, integrity, and availability.

Number	Attack Class	Attack Scenario	Resulting Harm
1	Confidentiality	Make money by stealing patients' medical records from the EMR and selling them on the dark web.	Millions of dollars of damages (in the form of legal fees and an erosion of trust) to the hospital, the violation of patient confidentiality, and potential identify fraud against patients.
2	Confidentiality	Acquire valuable biomedical research secrets by stealing clinical trial/research related data from the EMR.	Loss of research secret(s) potentially worth millions.
3	Integrity	Harm or assassinate a high-profile individual by modifying their medical record to influence care decisions in a way that harms them (e.g., including a positive diagnosis for cancer in a healthy patient, leading to the prescription of chemotherapy drugs).	This could lead to an adverse health outcome for the patient, and millions of dollars in lawsuits and an erosion of trust in the hospital.
4	Availability	Make money by encrypting the patient records on the EMR and	This could result in millions of dollars of damages (in the form of ransom,

		demanding a payment for the decryption key.	legal fees, and an erosion of trust) for the hospital and potential loss of life during the period when the EMR is down.
5	Availability	Cause chaos and death by irreparably sabotaging the EMR, causing a complete denial of service. Alternatively, lay the groundwork to destabilize an enemy nation by inserting sleeper code into the EMR systems of their hospitals.	Depending on the scope and length of the outage, this could lead to massive loss of life and billions of dollars in re-establishing the EMR system, legal fees, and an erosion of trust.

This representative set of strategic attack goals was chosen to cover all of confidentiality, integrity, and availability, as well as take into the account the most likely set of goals of the adversaries in the adversary model. Transnational terrorists are interested in sowing chaos and harming as many people as possible, which can be accomplished by modifying a patient's medical record or causing a complete denial of service on the EMR system (goals 3 and 5). Organized criminals are interesting in making money through cybercrime; EMR records are inherently valuable, and the urgent, life-and-death nature of a hospital's mission makes them extremely susceptible to paying ransoms (goals 1 and 4). Finally, nation states are interested in laying the groundwork for future sabotage and sealing biomedical research secrets (goals 2 and 5).

These strategic attack goals are representative of the larger attack space because the only ways to attack data are violate the confidentiality of secret data, modify the data, or make the data unavailable. An EMR is a data-centric system; any attack against the system has some malicious action against the EMR's data as its end goal. Thus, as these strategic goals cover the confidentiality, integrity, and availability of the EMR's data, they are representative of the larger attack space. Other attackers may want to do slightly different things with the EMR's data, but they will always be attacking the data's confidentiality, integrity, or availability.

Section 7: Estimated Harm

We now develop an estimate of the harm that would be done is each of the strategic attack goals were to be realized. This phase of the risk assessment is essential to provide a rough

idea an organization's cyber risk.[24] If all strategic attack goals against an organization have few consequences, an organization has little cyber risk and does not need significant cybersecurity investments. On the other hand, if the consequences for one or more of the strategic attack goals is devastating, the cyber risk for an organization is high and they will need a higher investment in cybersecurity. We estimate harm as orders of magnitude in dollars. We use orders of magnitude because these are rough estimates and therefore imprecise. The dollars cost includes both direct costs (e.g., the cost of establishing a new EMR system after the old one was sabotaged) and indirect costs (e.g., erosion of trust, adverse health outcomes for patients).

Number	**Attack Class**	**Estimated Harm**
1	Confidentiality	$10^8
2	Confidentiality	$10^6
3	Integrity	$10^8
4	Availability	$10^8
5	Availability	$10^10

We now discuss the nature of the loss for each one of the strategic attack goals and how the harm estimate was calculated in turn.

- Attack Goal 1: The losses from this attack take the form of lost confidentiality of patient medical information, HIPPA violation fees, legal fees (if/when victims seek legal recourse against the hospital), and loss of reputation for the hospital. The average cost of a data breach in the healthcare industry was $6.45 million in 2020.[25] However, this figure does not include legal fees and loss if institutional reputation. In the event of a large-scale data breach against an entrenched institution, these additional costs can run into the millions or tens of millions. For example, Johns Hopkins Hospital had a major data breach in May of 2023. Not only is Johns Hopkin's brand as the best hospital in the word significantly damaged, but there are multiple class action lawsuits pending against it.[26]
- Attack Goal 2: The losses from this attack represent the value of the secrecy of a biomedical research secret. We estimate this value using the annual budget for the National Institutes of Health, the premier biomedical research facility in the United States. The NIH has an annual budget of roughly $40 billion dollars to fund both internal research and research at universities across the country.[27] As biomedical research is typically published openly, the value of secrecy for most biomedical research is low. We assume that a particularly valuable research secret has a secrecy value 1/1000 of the annual budget for the NIH, or $10^6.
- Attack Goal 3: The losses from this attack represent potential loss of life for a patient, lawsuits against a hospital, and an erosion of trust in the EMR system. FEMA places a value of $7.5 million per human life; we use this figure throughout this analysis.[28] The nature of this strategic attack goal is somewhat targeted, so we assume it affects a small number of patients (~5). Assuming all 5 patients die, we have reached $10^7 in damages from that fact alone. The medical malpractice lawsuits would likely be tens of millions more, and an erosion of faith in EMRs, which are widely used and drastically increase hospital efficiency and reduce costs, millions more.

- Attack Goal 4: The losses from this attack represent the cost to pay a ransom, potential patient deaths during EMR downtime, legal fees for patient lawsuits, and an erosion of institutional trust. For a large-scale hospital, the ransom can cost tens of millions of dollars.[29] Patient deaths or adverse health events during EMR downtime cost an additional tens or hundreds of millions of dollars. Finally, legal fees and loss of institutional reputation are measured on a similar scale. When all the costs are added up, the harm caused by this attack is roughly $10^8.
- Attack Goal 5: The losses from this attack are primarily represented in terms of loss of human life. If the EMR system is kept down for an extended period of time, patients cannot receive care and critically ill patients are likely to experience adverse health events. Johns Hopkins has a 1,000 bed Level-1 trauma center (for patients in critical condition).[30] If even half of those patients die because they cannot receive care, the cost of this attack is already in the trillions of dollars without counting non-fatal adverse health events suffered by other patients. The cost to re-establish the EMR system, legal fees, and loss of institutional trust also play a role in these losses, but they pale in comparison to the cost of the human lives lost due to this attack.

Section 8: Estimated Probabilities

We now develop an estimate of the probability that attackers would succeed in executing the strategic attack goals defined in the previous sections. Probabilities are given as order of magnitude values, exponentials of base 10, to indicate the lack of precision of the estimate. This estimate helps guide the selection of strategic goals to focus on in the remainder of the analysis and calculate the expected harm of each event.[31]

When making these estimates, I am assuming that the adversaries I assigned to each goal in the "strategic attack goals" section will be attempting to execute their strategic attack goals. I am also assuming that the hospital system is relying on legacy systems (which is common practice in healthcare). Both factors increase the probability of a successful attack.

As rough baseline statistics, there are approximately 6090 hospitals in the US and there were 24 successful reported ransomware attacks against hospitals and 707 large-scale data breaches in healthcare in 2022.[32] These numbers are likely higher as some attacks almost assuredly went unreported (especially ransomware attacks, as there are few legal statutes compelling hospitals to report ransomware attacks). From these numbers, we extrapolate the probability of a successful ransomware attack is 0.00394 and the probability of a successful confidentiality attack is 0.11609 (this assumes each hospital was attacked exactly once by attacks of equal sophistication against equal defenses but serves as a rough value to inform our estimate).

Number	Attack Class	Estimated Probability
1	Confidentiality	10^-1
2	Confidentiality	10^-1
3	Integrity	10^-3
4	Availability	10^-2
5	Availability	10^-3

Section 9: Expected Harm and Risk

Using our estimated harm values and probabilities, we now calculate the expected harm for each of the strategic attack goals. Expected harm is calculated as estimated harm * estimated probability.[33] This step provides initial values for expected harm that are refined in subsequent analyses. We then sum the expected harms to provide an overall sum for expected harm due to cybersecurity risk. From this sum, and the orders of magnitude for expected harm we calculate, we can get a sense of the overall risk level of an EMR system as well as the strategic attack goals that contribute the most to that risk.

Number	**Attack Class**	**Estimated Probability**	**Estimated Harm**	**Expected Harm**
1	Confidentiality	10^-1	$10^8	$10^7
2	Confidentiality	10^-1	$10^6	$10^5
3	Integrity	10^-3	$10^8	$10^5
4	Availability	10^-2	$10^8	$10^6
5	Availability	10^-3	$10^10	$10^7
Sum				$10^7

Strategic attack goal 1 and strategic attack goal 5 make up the majority of the expected harm. Attack goal 5 has such a high expected harm because, although it is less likely to succeed than the other strategic attack goals, its cost is measured in trillions of dollars. Strategic attack goal 1 also has a high expected harm because the probability of it succeeding is very high. A massive number of data breaches have occurred in healthcare in recent years (663 in 2020, 715 in 2021, 707 in 2022), which indicates that attackers are more likely to succeed at violating the confidentiality of EMR records than the other strategic goals.

Section 10: Choose a Representative Subset of Strategic Attack Goals

We now choose a representative subset of our strategic attack goals to drive the remainder of the analysis. We group together strategic attack goals that have similar attacks – these groupings are called equivalence classes.[34] As a general rule, two strategic attack goals are equivalent if addressing the attacks in the tree would cause a cybersecurity engineer to select and weight the possible defensive options in nearly the same way. This step streamlines our analysis and allows us to develop a representative set of attack trees.

For this step, we group together strategic attack goals 1 and 2. Both goals involve stealing information from the EMR; goal 1 relates to stealing patient personally-identifiable information for profit, and the other involves stealing research-based data. However, both of these attacks involve violating the confidentiality of the EMR system, and as such would follow nearly identical steps until the very end of the attack. Thus, their attack trees are similar, and we group them together into an equivalence class.

We also group together strategic attack goals 3 and 4. Strategic attack goal 3 is maliciously modifying patient data to induce poor healthcare decision-making and an adverse health outcome, and strategic attack goal 4 is encrypting the EMR data and forcing a hospital to pay for the decryption key. While attack goal 4 is focused on availability, it first requires the attacker to violate the integrity of the EMR system by encrypting it. Thus, the two strategic attack goals have similar attack trees, where an attacker must breach the EMR system and maliciously modify its contents. Strategic attack goal 4 requires the attacker to encrypt the data

as opposed to changing patient information and demand a ransom, but these differences are marginal.

Section 11: Attack Trees

We now present attack trees for the representative strategic attack goals. This breaks down a representative strategic attack goal into sub-goals that are necessary to accomplish the top-level goal.[35] We continue refining the sub-goals into their composite steps until we reach steps that are easy to calculate the probability of attacker success (e.g., one could calculate the probability of a healthcare professional clicking on a malicious link in a phishing email, but it much harder to calculate the probability of the higher level "attacker gains control of hospital workstation" goal). The nodes on each level should be mutually exclusive (accomplishing one node provides no progress toward any other node) and exhaustive (they capture all possible means of achieving the root node). These attack trees allow us to update our estimates of expected harm and inform our mitigation packages. By calculating the probability of each node, we can build back up and calculate the probability of the top-level node. We then focus our mitigation packages on reducing the probability of success for the highest-probability leaf nodes.

Attack Tree for Strategic Attack Goals 1 and 2

Please see the file Strategic Attack Goals 1 and 2.rit included with my submission.

Attack Tree for Strategic Attack Goals 3 and 4

Please see the file Strategic Attack Goals 3 and 4.rit included with my submission.

Attack Tree for Strategic Attack Goal 5

Please see the file Strategic Attack Goal 5.rit included with my submission.

Section 12: Estimated Leaf Probabilities and Calculated Root Probabilities

We now estimate the probability of success of each leaf node and use these probabilities to "build up" to the revised probability of the strategic attack goal at the root of the attack tree. For two leaf nodes in an "AND" relationship, we multiply their probabilities to generate the probability of success of the root node. For two leaf nodes in an "OR" relationship, we take 1 – Pr(A and B not occurring).[36] The new estimate for the probability of the strategic attack goal being accomplished can be compared to the original estimate for a sanity check. However, as defenders tend to underestimate the probability of successful attacker events when developing strategic attack goals, we use the calculated value as the better estimate going forward. Additionally, the high-probability leaf nodes in the attack tree provide insight into the nodes we should target with our mitigation actions.

Several key facts related to my probability estimates:

- The healthcare domain overwhelmingly relies on legacy systems.[37] These legacy systems may not have the proper hardware to run the latest patched version of an application or operating system. This forces the system to run versions of applications and operating

systems that have known vulnerabilities with publicly available exploitation code, increasing the probability of finding a vulnerability.

- Researchers have found that healthcare workers click on phishing links roughly 17% of the time (similar to the average click rate of roughly 18%).[38] While system administrators may be savvier when it comes to fishing, an attacker can be reasonably confident a normal system user will fall victim to their social engineering attack, especially if it is individually crafted. In the population at large, more targeted spear phishing campaigns work roughly 53% of the time.[39]
- Zero days have grown more common in recent years; 69 zero days were detected in 2021 and 41 in 2022 (the two years with the greatest number of zero days found).[40]
- As hospitals lack significant resources to invest in cybersecurity, they are more likely to have configuration errors in their security controls e.g., allowing *.* on their firewalls.[41]
- Medical Internet of Things devices are typically not designed with security in mind. They lack security controls, and software patches can be rare. Thus, they offer a vulnerable device for attackers to exploit, and the probability of successfully finding an exploit is higher than a normal device.[42]
- Hospital physical access control varies from hospital to hospital; however, almost all hospitals have security guards, badge-based access control, and keep the physical location of their systems secret. This makes physically breaching the hospital difficult.
- Hospital-owned laptops are more secure than normal patient laptops. They have mandatory patches, antivirus, security controls, and may not allow users to access certain vulnerable websites or services. Patient computers on the other hand, have no such protections, making them more vulnerable. There is likely at least one vulnerable service running on a patient's computer, and its os/applications may be unpatched.
- Insider attacks are made easier due to the weak access controls within many healthcare organizations. On average, every employee has access to 20% of all files in the organization, and more than 1 in 10 sensitive files are open to every employee.[43]
- Many healthcare organizations have poor password management, making it easier to crack user credentials. 77% of healthcare organizations have 500 or more accounts with passwords that do not expire.[44]
- In general, lifecycle attacks are more difficult than a direct attack on a healthcare organization. However, adversaries such as nation states have the resources and expertise to carry out these attacks.
- As most servers run some form of Linux, I assume the hospital servers run Linux as well. Most versions of Linux (e.g., Ubuntu) are open source, which makes lifecycle attacks harder.[45]

Probability for Strategic Attack Goal 5

Node Number	Node Name	Probability	Probability Roll-Up
0	Sabotage EMR System Availability	10^-1	1-(1-10^-1)* (1-10^-1)* (1-10^-2)* (1-10^-1)* (1-

			10^-3)*(1-10^-2)
5	Lifecycle Attack	10^-3	10^-3*1.0*1.0*1.0
5.1	Gain Access to Source Code Used by EMR System	10^-3	1-(1-10^-3)*(1-10^-3)*(1-10^-3)
5.1.1	Hack EMR Server OS Provider	10^-3	Leaf
5.1.2	Hack Epic	10^-3	Leaf
5.1.3	Hack EMR Server middleware/underware provider	10^-3	Leaf
5.2	Insert A Trojan Horse Code into Source Code	1.0	Leaf
5.3	Access System Through Backdoor	1.0	Leaf
5.4	Shut Down EMR Server	1.0	Leaf
3	Physical Attack	10^-2	1-(1-10^-2)*(1-10^-4)*(1-10^-6)
3.1	Cut Server Coolant	10^-2	1-(1-10^-2)*(1-10^-3)
3.1.1	Infrastructure Attack	10^-3	1-(1-10^-3)*(1-10^-3)
3.1.1.1	Destroy Coolant Pipes	10^-3	Leaf
3.1.1.2	Destroy Coolant Station	10^-3	Leaf
3.1.2	Cyberattack on Control System	10^-2	1-(1-10^-2)*(1-10^-2)*(1-10^-3)
3.1.2.1	Application Vulnerability	10^-2	Leaf
3.1.2.2	OS Vulnerability	10^-2	Leaf
3.1.2.3	Lifecycle Attack	10^-3	Leaf
3.2	Destroy Server	10^-4	10^-2*10^-2*1.0
3.2.1	Infiltrate Hospital	10^-2	Leaf
3.2.2	Locate Server Room	10^-2	Leaf
3.2.3	Physically Destroy Server	1.0	Leaf
3.3	Cut Server Power	10^-6	10^-4*10^-2
3.3.1	Attack Power Infrastructure	10^-2	1-(1-10^-2)*(1-10^-2)
3.3.1.2	Attack Power Supplier	10^-2	Leaf
3.3.1.1	Attack Power Lines	10^-2	10^-2*1.0*1.0
3.3.1.1.1	Find where power lines converge	10^-2	Leaf
3.3.1.1.2	Rent heavy machinery	1.0	Leaf
3.3.1.1.3	Destroy power lines	1.0	Leaf
3.3.2	Attack Backup Generators	10^-4	10^-2*10^-2*1.0
3.3.2.1	Infiltrate hospital	10^-2	Leaf

3.3.2.2	Locate backup generators	10^-2	Leaf
3.3.2.3	Destroy backup generators	1.0	Leaf
4	Sabotage Authentication/Authorization	10^-1	10^-1*1.0
4.1	Gain control of authorization server	10^-1	1-(1-10^-3)*(1-10^-4)*(1-10^-1)*(1-10^-4)
4.1.1	Lifecycle attack	10^-3	1-(1-10^-3)*(1-10^-3)*(1-10^-3)
4.1.1.1	Hack server microcode provider	10^-3	Leaf
4.1.1.2	Hack authorization software provider	10^-3	Leaf
4.1.1.3	Hack server of software provider	10^-3	Leaf
4.1.4	Network Attack	10^-4	10^-1*10^-3
4.1.4.1	Establish a Toehold	10^-1	1-(1-10^-1)*(1-10^-1)*(1-10^-1)
4.1.4.1.1	External Hospital Laptop	10^-1	See 6.1.1.1
4.1.4.1.2	Medical IOT Device	10^-1	See 6.1.1.2
4.1.4.1.3	Hospital Workstation	10^-1	See 6.1.1.3
4.1.4.2	Move to Authorization Server	10^-3	10^-1*10^-2
4.1.4.2.1	Escalate Privileges	10^-1	Leaf
4.1.4.2.2	Interface with Authorization Server	10^-2	1.0*10^-2
4.1.4.2.2.1	Establish Communications Channel to Authorization Server	1.0	Leaf
4.1.4.2.2.2	Use Toehold Device to Gain Account on Authorization Server	10^-2	1-(1-10^-2)*(1-10^-2)*(1-10^-3)*(1-10^-2)
4.1.4.2.2.2.1	Steal Administrator Credentials	10^-2	Leaf
4.1.4.2.2.2.2	Zero Day	10^-3	Leaf
4.1.4.2.2.2.3	Take Advantage of OS Vulnerability	10^-2	Leaf
4.1.4.2.2.2.4	Take Advantage of Application-Level Vulnerability	10^-2	Leaf
4.1.2	Social Engineering	10^-1	1-(1-10^-1)*(1-10^-1)
4.1.2.1	Spear Phish Internal User	10^-1	Leaf
4.1.2.2	Steal Credentials	10^-1	1.0*10^-1
4.1.2.2.1	Trick User into Revealing their Credentials	10^-1	1-(1-10^-1)*(1-10^-1)
4.1.2.2.1.1	Spoofed Call	10^-1	Leaf
4.1.2.2.1.2	Spoofed Email	10^-1	Leaf
4.1.2.2.1	Access EMR Server Using Credentials	1.0	Leaf
4.1.3	Willing Insider	10^-4	10^-3*10^-1

4.1.3.1	Recruit Insider	10^-3	Leaf
4.1.3.2	Provide Means of Damaging System	10^-1	1-(1-10^-1)*(1-10^-1)
4.1.3.2.1	USB	10^-1	1.0*1.0*10^-1
4.1.3.2.1.1	Create USB With Malicious Code	1.0	Leaf
4.1.3.2.1.2	Give USB to Insider	1.0	Leaf
4.1.3.2.1.3	Insider Plugs USB into Server	10^-1	Leaf
4.1.3.2.2	Malicious Code	10^-1	10^-1*1.0
4.1.3.2.2.1	Provide User with Malicious Code	1.0	Leaf
4.1.3.2.2.2	Insider Executes Malicious Code	10^-1	Leaf
4.2	Shut Down Authorization Server	1.0	Leaf
1	Insider Attack	10^-1	1-(1-10^-3)*(1-10^-1)
1.1	Willing Insider	10^-3	10^-2*10^-1
1.1.1	Recruit Insider	10^-2	Leaf
1.1.2	Provide Means of Damaging System	10^-1	1-(1-10^-1)*(1-10^-1)
1.1.2.1	USB	10^-1	10^-1*1*1
1.1.2.1.1	Create USB With Malicious Code	1.0	Leaf
1.1.2.1.2	Give USB to User	1.0	Leaf
1.1.2.1.3	Insider Plugs USB Into Server	10^-1	Leaf
1.1.2.2	Malicious Code	10^-1	1*10^-1
1.1.2.2.1	Provide Insider with Malicious Code	1.0	Leaf
1.1.2.2.2	Insider Executes Malicious Code on Internal Device	10^-1	Leaf
1.2	Social Engineering	10^-1	1-(1-10^-1)*(1-10^-2)
1.2.1	Spear Phish Internal User to Execute Malicious Code	10^-1	Leaf
1.2.2	Steal Credentials Method	10^-2	10^-1*1*10^-1
1.2.2.1	Trick System Administrator into Giving Up Credentials	10^-1	1-(1-10^-1)*(1-10^-1)
1.2.2.1.1	Spoofed Call	10^-1	Leaf
1.2.2.1.2	Spoofed Email	10^-1	Leaf
1.2.2.2	Access EMR Server Using Credentials	1.0	Leaf
1.2.2.3	Shut Down Server	10^-1	Leaf
2	DDos Attack	10^-1	1-(1-10^-1)*(1-1)
2.2	Use Packet Spam to Overwhelm EMR System	1.0	1-(1-1)*(1-1)
2.2.1	Packet Flood EMR Internal Network	1.0	Leaf
2.2.2	Packet Flood EMR Server	1.0	Leaf
2.1	Bypass Security Controls	10^-1	1-(1-10^-2)*(1-10^-1)*(1-10^-1)
2.1.1	Use Patient Traffic to Bypass Firewalls	10^-2	10^-2*1

2.1.1.1	Develop Patient Botnet	10^-2	10^-1*10^-1
2.1.1.1.1	Locate Patient Computers	10^-1	Leaf
2.1.1.1.2	Take Control of Patient Computers	10^-1	1-(1-10^-1)*(1-10^-1)*(1-10^-2)*(1-10^-1)*(1-10^-3)
2.1.1.1.2.2	Application Layer Attack	10^-1	Leaf
2.1.1.1.2.1	Take Advantage of Vulnerabilities in OS	10^-1	Leaf
2.1.1.1.2.3	Lifecycle Attack	10^-3	Leaf
2.1.1.1.2.4	Phishing Email that Executes Malicious Code	10^-1	Leaf
2.1.1.1.2.5	Zero Day	10^-3	Leaf
2.1.1.2	Use Patient Computers to Interface with EMR System	1.0	Leaf
2.1.2	Use Internal Device Traffic to Bypass Firewall	10^-1	10^-1*1.0
2.1.2.1	Gain Control of Internal Device	10^-1	1-(1-10^-1)*(1-10^-1)*(1-10^-1
2.1.2.1.1	External Hospital Laptop	10^-1	See 6.1.1.1
2.1.2.1.2	Medical IOT Device	10^-1	See 6.1.1.2
2.1.2.1.3	Hospital Workstation	10^-1	See 6.1.1.3
2.1.2.2	Use Internal Device to Interface with EMR System	1.0	Leaf
2.1.3	Take Advantage of Poorly Configured Firewall	10^-1	1.0*10^-1
2.1.3.1	Probe Firewall	1.0	Leaf
2.1.3.2	Find a Misconfiguration that Allows Packets Past	10^-1	Leaf
6	Network Attack	10^-2	10^-2*1
6.1	Access EMR System via the Network	10^-2	10^-1*10^-1
6.1.1	Establish a Toehold	10^-1	1-(1-10^-1)*(1-10^-1)*(1-10^-1)
6.1.1.1	External Hospital Laptop	10^-1	1-(1-10^-1)*(1-10^-2)*(1-10^-1)*(1-10^-3)*(1-10^-2)
6.1.1.1.1	Phish Owner	10^-1	Leaf
6.1.1.1.2	Steal User Credentials	10^-2	Leaf
6.1.1.1.3	Hack Local (non-hospital) Network	10^-1	Leaf
6.1.1.1.4	Zero Day	10^-3	Leaf
6.1.1.1.5	Application-Layer Vulnerability	10^-2	Leaf
6.1.1.2	MIot Device	10^-1	1-(1-10^-1)*(1-10^-2)*(1-10^-2)
6.1.1.2.1	Take advantage of OS vulnerability	10^-1	Leaf
6.1.1.2.2	Lifecycle Attack	10^-2	Leaf

6.1.1.2.3	Steal/Crack Password	10^-2	Leaf
6.1.1.3	Hospital Workstation	10^-1	1-(1-10^-2)*(1-10^-1)*(1-10^-2)*(1-10^-3)*(1-10^-2)
6.1.1.3.1	Application-Layer Vulnerability	10^-2	Leaf
6.1.1.3.2	Phish Owner	10^-1	Leaf
6.1.1.3.3	Steal User Credentials	10^-2	Leaf
6.1.1.3.4	Zero Day	10^-3	Leaf
6.1.1.3.5	“USB Scatter” Attack	10^-2	Leaf
6.1.2	Move to EMR System	10^-1	
6.1.2.1	Escalate Privileges on Toehold	10^-1	Leaf
6.1.2.2	Interface with EMR System	1.0	1-(1-1)*(1-10^-2)
6.1.2.2.1	Establish Communications Channel to EMR System	1.0	Leaf
6.1.2.2.2	Use Toehold Device to Gain Account on EMR System	10^-2	1-(1-10^-2)*(1-10^-2)*(1-10^-3)*(1-10^-2)
6.1.2.2.2.3	Take Advantage of EMR server os Vulnerability	10^-2	Leaf
6.1.2.2.2.4	Take Advantage of EMR server Epic Vulnerability	10^-2	Leaf
6.1.2.2.2.2	Zero Day	10^-3	Leaf
6.1.2.2.2.1	Steal user credentials and log in from internal device	10^-2	Leaf
6.2	Compromise EMR System	1.0	1.0*1.0
6.2.1	Compromise EMR Server	1.0	1-(1-1)*(1-1)*(1-10^-2)*(1-10^-3)
6.2.1.1	Encrypt Data	1.0	Leaf
6.2.1.2	Purge Data	1.0	Leaf
6.2.1.3	Shut Down Via Fatal Error	10^-2	1-(1-10^-2)*(1-10^-2)
6.2.1.3.1	Epic Vulnerability	10^-2	Leaf
6.2.1.3.2	OS Vulnerability	10^-2	Leaf
6.2.1.4	Corrupt Crucial Software	10^-3	1-(1-10^-3)*(1-10^-3)
6.2.1.4.1	Corrupt the OS	10^-3	
6.2.1.4.2	Corrupt the Middleware	10^-3	
6.2.2	Compromise Backups	1.0	1-(1-1) *(1-1)
6.2.2.1	Encrypt Backups	1.0	Leaf

6.2.2.2	Purge Backups	1.0	Leaf

Section 13: Baseline Expected Harm

Using the probability of success for the overall strategic attack goal calculated using our attack tree, we update our estimate of expected harm for each strategic attack goal. This allows us to use our more reliable probability estimate that, due to the tendency of humans to under-estimate cyber risk at a large scale, is likely more accurate than our initial estimate.[46] These updated expected harm values will be used in the analysis going forward.

Strategic Attack Goal 5:
Updated Probability of Attack Success: 10^-1
Estimate of Harm Caused by the Attack: $10^10

Updated Expected Harm: $10^9

The updated expected harm for this attack is two orders of magnitude greater than our initial estimate. As the attack tree demonstrates, the susceptibility of healthcare workers to phishing attacks and the vulnerability of many hospital endpoints dramatically increases the probability of a successful attack. A well-researched spear phishing email can fool a system admin and execute malicious code that gives an attacker control of the EMR server. Similarly, devices like the control systems for coolant for the EMR system and MIoT devices were not designed with security in mind. This leaves their operating systems and applications riddled with vulnerabilities attackers can exploit.

Section 14: Attack Sequence Cut Sets

We now enumerate over the cut sets of the attack trees. These are sets of attack tree leaf nodes that contain sufficient steps for accomplishing a strategic attack goal with no extraneous nodes. These cut sets give us an indication of where system risk is concentrated and system weaknesses to address via mitigation packages.[47] High probability nodes, especially in an "OR" relationship, are prime targets to address. Often, the same leaf nodes appear repeatedly in multiple goal nodes and across multiple trees, typically as prerequisites for further steps. These leaf nodes should also become the focus of mitigation packages, as addressing them will reduce system risk on multiple fronts.

Due to the size of the attack trees, we enumerate over five representative cut sets per attack tree. I list attack steps in chronological order within the cut sets; the attack steps that must be executed first come first, and the attack steps that follow a previous step come after that step in the set. I reference nodes using their node number within their respective attack tree.

Cut Sets for Strategic Attack Goals 1 and 2

- {2.1.1.1.3, 2.1.1.2, 2.1.1.3}
- {1.1.4.1, 1.1.4.2, 1.2, 1.3.1.1, 1.3.1.2, 1.3.1.3}
- {1.1.3.2.1.1, 1.1.3.2.2, 1.2, 1.3.2.3}
- {1.1.1.1.2.1, 1.1.1.2.1, 1.1.1.2.2.1, 1.2, 1.3.2.2}
- {2.1.3.1.2, 2.1.3.2, 2.1.3.3}

Cut Sets for Strategic Attack Goals 3 and 4

- {1.1.1.3.3, 1.1.2.1, 1.1.2.2.2.2, 2.1}
- {1.1.1.2.1, 1.1.2.1, 1.1.2.2.3, 2.1}
- {1.2.1.1, 1.2.1.2, 1.2.1.3, 1.2.1.4, 2.2}
- {1.3.1, 1.3.2.2, 1.3.3, 2.2}
- {1.4.1.1, 1.4.2, 2.1}

Cut Sets for Strategic Attack Goal 5

- {1.2.2.1.1, 1.2.2.2, 1.2.2.3}
- {2.1.1.1.1, 2.1.1.1.2.2, 2.1.1.2, 2.2.1}
- {6.1.1.1.1, 6.1.2.1, 6.1.2.2.2.4, 6.2.1.2, 6.2.2.2}
- {5.1.1, 5.2, 5.3, 5.4}
- {3.3.1.2, 3.3.2.1, 3.3.2.2, 3.3.2.3}

From these cuts sets, we can see three consistent sources of risk are insider attacks, insecure endpoints, and phishing attacks. These is little a hospital can do to prevent lifecycle attacks other than reduce their reliance on external software providers as much as possible, and as lifecycle attacks have a far lower probability of success than other attack vectors, we do not consider them in our proposed mitigations. Vulnerable endpoints, on the other hand, are a worrisome attack vector. An EMR system has many different types of users, each of which has their own endpoint to access the system. Endpoints such as patient computers or MIoT devices are not optimized for security and have latent vulnerabilities attackers can use to gain a toehold on the EMR network. Additionally, the wide variety of users, many of whom are not security conscious, make phishing attacks an attack vector with a high probability of success. These are the two most pressing areas mitigation packages must address.

Section 15: Inferred Mitigation Packages Against Attack Sequences

We now develop potential mitigation packages from the attack trees and cut sets. These mitigation packages are related technologies/programs that target specific leaf nodes. Mitigation packages should be directed at the highest probability of success leaf nodes, or leaf nodes that are repeated throughout the attack tree.[48] Targeting these nodes with mitigation packages yields the greatest benefit in risk reduction, as the easy path for the attacker will be made more difficult.

Mitigation Aspect	**Description**
Designation	Package A
Attack Category Addresses	Confidentiality, Integrity, and Availability
Technology	Software
Description	Install software across all hospital laptops and workstations that prevents users from running executable files not on a list of pre-approved applications. Tech support will grant exceptions to this policy on a case-by-case basis.

Risk Impact	Targets nodes such as 1.2.1 and 4.1.2.1 (on attack tree for strategic attack goal 5) throughout many branches of all three attack trees.
Mission Impact	Significantly reduce user friendliness, makes it harder to try new tools and share resources. Places an increased burden on tech support.
Variation (80/20)	Instead of blocking users from accessing executable files not on a pre-approved list, prompt users with an "are you sure" prompt that warns them the executable file could be malicious. Costs the same to install but decreases the burden on tech support and still allows for user friendliness/collaboration.

Mitigation Aspect	**Description**
Designation	Package B
Attack Category Addresses	Availability
Technology	Server Load Balancing
Description	Purchase additional servers to use for load balancing in the event of heavy patient traffic on the EMR network. This makes the EMR system more resistant to a DDoS attack by a botnet of patient computers.
Risk Impact	Targets node 2.2 on the attack tree for strategic attack goal 5
Mission Impact	Improves performance, but costly in terms of time and money to implement
Variation (80/20)	Configure firewalls to shut off all patient traffic in the event of heavy load. This means that the internal hospital network would still be able to access the EMR system in the event of a DDoS attack, although patients would not be able to access or update their data

Mitigation Aspect	**Description**
Designation	Package C
Attack Category Addresses	Confidentiality, Integrity, and Availability
Technology	Subnetwork
Description	Place all MIoT devices on their own subnetwork within the internal hospital network. This subnetwork should have its own router/firewall that carefully monitors outgoing traffic. While the hospital cannot

	patch MIoT device software itself, it can make it harder for attackers to take advantage of MIoT devices as toehold
Risk Impact	Targets node 6.1.1.2 on the attack tree for strategic attack goal 5
Mission Impact	Little impact on mission, but costly and difficult to implement. May also require MIoT downtime.
Variation (80/20)	Ensure MIoT devices install software patches immediately and automatically. This costs little to implement but may cause an MIoT device to go down at a crucial time.

Section 16: Conclusion

EMR systems are critical for healthcare organizations to care for patients. The valuable information they contain, combined with a hospital's complete reliance on its EMR system to support its mission, makes them enticing targets for terrorists, nation states, and cybercriminals. However, the security of most EMR systems is woefully inadequate, especially against such sophisticated adversaries. The mission of a hospital requires many users to be able to access the EMR system, creating many potential toeholds for adversaries. Some of these users, such as patients or MIoT devices, are not security conscious. Patient computers likely have vulnerable applications running, unpatched operating systems, and improperly configured security settings. MIoT device software often does not consider security, and patches are released infrequently. These easy entry points allow attackers to bypass the first ring of hospital defenses, making it easier to infiltrate the EMR system.

Social engineering is also a significant concern. For the most part, healthcare workers are not security conscious, and spear phishing attacks are more likely than not to succeed. Depending on who an attacker can successfully phish, the consequences could range from gaining a toehold to gaining control of the EMR server. Hospitals and healthcare providers need to have better training and protections that make it harder for social engineering attacks to succeed.

The reliance of nearly all EMR systems on Epic also make a lifecycle attack highly effective. If a sophisticated adversary were able to insert malicious code into the Epic source code, they would be able to affect thousands of EMR systems with one attack. Although Epic's systems are generally secure, this "black swan" event where an adversary could influence the ability of hospitals to provide care nationwide would be cataclysmic.

To make EMR systems more secure, hospitals should immediately move to secure their endpoints. Every device connected to the internal network needs to be patched regularly and automatically, especially MIoT devices. Hospitals should also assume the adversary has a toehold in their network and prepare appropriately. For example, mitigation package B prepares for the contingency an adversary has a toehold via a patient computer, and mitigation package C prepares for the contingency an attacker has a toehold via a MIoT device.

Proper system configuration is also necessary. Permissions on the EMR network should follow least privilege, and system administrators should eliminate unnecessary services on the internal EMR network to reduce the attack surface. Special care should also be taken to ensure accounts are configured correctly. Many attacks require the attacker to escalate their privileges,

so locking down account settings on all devices would be a worthwhile step. Similarly, hospitals need better password management. Users should be expected to reset their password on at least a semi-regular basis, and common passwords should be disallowed to make password cracking harder. Ideally hospitals would implement multi-factor authentication via biometrics and physical tokens. This would eliminate the inherent vulnerability of passwords while simultaneously increasing system ease of use.

---

[1] "Electronic Health Records: the Basics," HealthIT.gov, The White House, Accessed Oct. 5, 2023, https://www.healthit.gov/faq/what-information-does-electronic-health-record-ehr-contain.
[2] R Hillestad, J Bigelow, A Bower, F Girosi, et. al, "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs," *Health Affairs* 24, no. 5 (2005): 1103-1117.
[3] AJ Cartwright, "The Elephant in the Room: Cybersecurity in Healthcare," *J Clin Monit Comput* 37, (2023):1123-1132.
[4] AJ Cartwright, "The Elephant in the Room: Cybersecurity in Healthcare," *J Clin Monit Comput* 37, (2023):1123-1132.
[5] AJ Cartwright, "The Elephant in the Room: Cybersecurity in Healthcare," *J Clin Monit Comput* 37, (2023):1123-1132.
[6] AJ Cartwright, "The Elephant in the Room: Cybersecurity in Healthcare," *J Clin Monit Comput* 37, (2023):1123-1132.
[7] G Martin, P Martin, C Hankin, A Darzi, J Kinross, "Security and Healthcare: How Safe are We?," *British Medical Journal*, 358, (2017): 1.
[8] Lynne Coventry, Dawn Brawnley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, 113, (2018): 48-52.
[9] Lynne Coventry, Dawn Brawnley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, 113, (2018): 48-52.
[10] Lynne Coventry, Dawn Brawnley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, 113, (2018): 48-52.
[11] Lynne Coventry, Dawn Brawnley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, 113, (2018): 48-52.
[12] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 295.
[13] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 295.
[14] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 295.
[15] "The Johns Hopkins Hospital," Johns Hopkins Medicine, Johns Hopkins, Accessed Oct. 5, 2023, https://www.hopkinsmedicine.org/the-johns-hopkins-hospital/about#:~:text=Vision%20and%20Values-,Our%20Mission,of%20excellence%20in%20patient%20care.
[16] "Clinical Notes," HealthIT.gov, Office of the National Coordinator for Health Information Technology, Accessed Nov. 12 2023, https://www.healthit.gov/isa/uscdi-data-class/clinical-notes#:~:text=Contains%20the%20response%20to%20request,or%20advice%20from%20another%20clinician.&text=A%20synopsis%20of%20a%20patient%27s,or%20post%2Dacute%20care%20setting.&text=Documents%20the%20current%20and%20past%20conditions%20and%20observations%20of%20the%20patient.
[17] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 95.
[18] AJ Cartwright, "The Elephant in the Room: Cybersecurity in Healthcare," *J Clin Monit Comput* 37, (2023):1123-1132.
[19] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 95.
[20] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 95.

[21] Tim Starks, "DHS Warns About 2024's Cyberthreats," *The Washington Post* (Washington DC, MD), Sep. 15, 2023.
[22] Andrew Hollister, interviewed by Bill Siwicki, *Healthcare IT News*, Healthcare IT News, Oct. 28, 2022.
[23] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 297.
[24] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 298.
[25] Narendra Sharma, Ebere Oriaku, Ngozi Oriaku, "Cost and Effects of Data Breaches, Precautions, and Disclosure Laws," International Journal of Emerging Trends in Social Sciences, 8 (2020): pp. 31-41.
[26] CBS Baltimore Staff, "Johns Hopkins hit with class action lawsuit connected to data breach," CBS News Baltimore, CBS News, Accessed Nov. 12 2023, https://www.cbsnews.com/baltimore/news/johns-hopkins-university-health-system-hospital-hit-with-class-action-lawsuit-connected-to-data-breach-information-security-baltimore/.
[27] "Budget," National Institutes of Health, US Department of Health and Human Services, Accessed Nov. 12 2023, https://www.nih.gov/about-nih/what-we-do/budget#:~:text=Based%20on%20historical%20distribution%20of,comprise%20the%20annual%20NIH%20budget.&text=Reflects%20the%20sum%20of%20enacted,Consolidated%20Appropriations%20Act%2C%202023%20(P.L..
[28] "FEMA Benefit-Cost Analysis (BCA) Toolkit 6.0 Release Notes," FEMA, US Department of Homeland Security, Accessed Nov. 12 2023, https://www.fema.gov/sites/default/files/2020-08/fema_bca_toolkit_release-notes-july-2020.pdf.
[29] Paul Bischoff, "Since 2016, ransomware attacks on healthcare organizations have cost the US economy $77.5bn in downtime alone," CompariTech, CompariTech, Accessed Nov. 12, 2023, https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/.
[30] "Hospital Profiles," Johns Hopkins Hospital, Johns Hopkins, Accessed Nov. 12 2023, https://www.hopkinsmedicine.org/emergency-medicine/em-residency/hospitals#:~:text=The%20Johns%20Hopkins%20Hospital%20is,of%20our%20health%20care%20system.
[31] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 299-300.
[32] Mark Elias, "85 Hospital Statistics & Facts: How Many Hospitals Are There?," DiscoveryABA, DiscoveryABA, Accessed Nov. 12, 2023, https://www.discoveryaba.com/statistics/hospital-statistics-facts#:~:text=How%20Many%20Hospitals%20Are%20There%20in%20the%20U.S%3F,local%20government%20entities%20(26.6%25).
Naomi Diaz, "289 healthcare organizations were impacted by ransomware attacks in 2022," Becker's Health IT, Becker's Health IT, Accessed Nov. 12, 2023, https://www.beckershospitalreview.com/cybersecurity/289-healthcare-organizations-were-impacted-by-ransomware-attacks-in-2022.html#:~:text=2.,the%20data%20of%20623%2C000%20patients.
[33] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 300.
[34] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 301.
[35] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 301-302.
[36] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 305.
[37] Lynne Coventry, Dawn Brawnley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, 113, (2018): 48-52.
[38] Mohammad Jalali, Maike Bruckes, Daniel Westmattelmann, Gerhard Schewe, "Why Employees (Still) Click on Phishing Links: Investigation in Hospitals," *J Med Internet Res,* 22, (2020).
[39] Mohammad Jalali, Maike Bruckes, Daniel Westmattelmann, Gerhard Schewe, "Why Employees (Still) Click on Phishing Links: Investigation in Hospitals," *J Med Internet Res,* 22, (2020).
[40] Maddie Stone, "The ups and downs of 0-days," Google Threat Analysis Group, Google, Accessed Nov. 12, 2023, https://blog.google/threat-analysis-group/0-days-exploited-wild-2022/.
[41] AJ Cartwright, "The Elephant in the Room: Cybersecurity in Healthcare," *J Clin Monit Comput* 37, (2023):1123-1132.
[42] Wencheng Sun, Zhiping Cai, YangYang Li, Fang Liu, Shengqun Fang, Guoyan Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks* 2018 (2017).
[43] "Insider Threats in Healthcare," Department of Health and Human Services, Department of Health and Human Services, Accessed Nov. 12, 2023, https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf.
[44] "Insider Threats in Healthcare," Department of Health and Human Services, Department of Health and Human Services, Accessed Nov. 12, 2023, https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf.

[45] "Linux vs Windows: What is the Best Server OS for Web Servers?" RedSwitches, RedSwitches, Accessed Nov. 12, 2023, https://www.redswitches.com/blog/linux-vs-windows/.
[46] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 305.
[47] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 306-307.
[48] Sami Saydjari, *Engineering Trustworthy Systems*, (New York: McGraw-Hill Education, 2018), 308.