Winder, Michael

University of Wisconsin – Stout

ICT 732 – Technology Futures

December 17, 2023

AI in Healthcare cybersecurity

Framework Forecasting Project

Michael Winder

Contents

[Framing 2](#_Toc153903052)

[1.1 Framing the Domain 2](#_Toc153903053)

[1.2 Domain Map 4](#_Toc153903054)

[2.1 Current Assessment 5](#_Toc153903055)

[2.2 Era Analysis 6](#_Toc153903056)

[2.3 Scanning Hits 7](#_Toc153903057)

[Futuring 13](#_Toc153903058)

[3.1 Baseline Future Inputs 13](#_Toc153903059)

[3.4 Alternative Future Inputs 14](#_Toc153903060)

[Visioning 15](#_Toc153903061)

[4.1 Baseline Future 15](#_Toc153903062)

[4.2 Key Assumptions 15](#_Toc153903063)

[4.3 2x2 Matrix Alternate Futures 16](#_Toc153903064)

[Project Summary 18](#_Toc153903065)

[Citations 20](#_Toc153903066)

## Framing

### 1.1 Framing the Domain

|  |  |
| --- | --- |
| **Key issue(s) or question(s)?** (Exploratory **or** strategic) | I consider how the world of cybersecurity is changing, especially in the field of healthcare, when trying to maintain compliance with federal regulations.  Exploratory: What type of realistic implications does cybersecurity have when dealing with healthcare? |
| **Domain definition**  *(subject of the forecast)* | I am forecasting the futures of AI in cybersecurity in the healthcare field in the United States by the year 2028.  The scope of the domain will be limited to the healthcare field, between small to medium-sized companies, where it is assumed, they have an internal security team. We will look at software currently in use and its uses, along with where that software might be in the future. We will also look at how different security practices can change workflow within the field. Not included in the scope will be the costs of products. |
| **Client** | Real Client: Family Health Center of Marshfield, Inc. |
| **Geographic Scope** | Information technology sector within the United States, focusing on the healthcare field. |
| **Time horizon** | The approximate period for the 3 horizons  H1 – now to 2025; H2 2025-2027; H3 2027-2028+ |
| **Domain Map**  (Boundaries, Categories, What’s in & What’s out) | Separate template: See Domain Map page |

#### Steep Analysis

|  |  |  |
| --- | --- | --- |
| Area | Major Points | Implications |
| Social | -Are patients affected by cybersecurity issues?  -What type of harm could be caused in the event of a breach? | -Patients assume information secured  -Breach can cause reputation harm  -Company responsible for breach/aftermath |
| Technological | -Is new equipment needed for updates to the system?  -Has there been an overall increase in system breaches in the field?  -New software that works in the security mindset? | -Time to setup and configure  -Exposure of secure data.  -Equipment capable of handling new software.  -Training of employees on new software |
| Economic | -Are more patients seeking care?  -New software/EMR/MHR  -New security software? | -More employees needed  -Accessibility to information  -Company budgets |
| Environmental | -Are there any environmental impacts?  -Does ‘green’ companies effect changes? | -More equipment could affect electrical usage, if more companies add could cause power plants to run more??? |
| Political | -Are Federal Regulations being updated/amended?  -New Certifications required | -Changes to company IT structure  -Changes to company IT policies  -Training/Certification costs |

### 1.2 Domain Map

### 2.1 Current Assessment

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Current conditions** (key facts about the domain today) | From a technology perspective, health care infrastructure is far more complex than other industries. As an environment of disparate technologies—with varying ages and security maturity—it offers a broad attack surface that is challenging to protect ( Kijewski, 2022).  Since the start of the year, 327 data breaches had been reported to the U.S. Department of Health and Human Services’ Office for Civil Rights. That figure is up more than 104% from 160 breaches as of mid-2022. (Payerchin, 2023) |
| **Stakeholders** (individuals or organizations that can influence the future of the domain) | Healthcare: Have needs to maintain records on patients to provide medical care, and provide better diagnosis to patients, quality of care,  Government: minimal political influence, provides overall regulations that must be followed, provides grants to healthcare institutions  Patients: have a want to keep their information secure, and medical history private  Education Institutions: universities, high schools, and certification entities need to be able to train upcoming students |
| **History** past event(s) that began the current era | See below |
| **Era analysis** fromseparate template | See template on next page. |

History

* 1970s Internet/Arpanet born.
* 1972 First EMR system developed. ([www.ncbi.nlm.nih.gov](http://www.ncbi.nlm.nih.gov), 2020)
  + Created by the Regenstreif Institute in the United States
* 1990 The internet goes worldwide.
* 2000s cyberattacks become more popular (cybermagizine.com, 2021)
* 2009 Barack Obama spearheaded the American Recovery and Reinvestment Act
  + This incentivized the use of EMR for healthcare organizations. ([www.ncbi.nlm.nih.gov](http://www.ncbi.nlm.nih.gov), 2020)
* 2014 All institutions were to be using EMR’s by this year.
* 2014 First hugely significant healthcare cybersecurity event occurred (McKeon, 2022)
* 2015 Large data breaches began to occur in the healthcare field (hhs.gov, 2022)
* 2017 WannaCry cyberattack.
* 2019 Cyberattacks against healthcare continues to increase.

### 2.2 Era Analysis

Need found for doctors to maintain medical records.

**Time**

1920

2014

EMR use required.

|  |  |
| --- | --- |
| **Previous Era:**  Paper Health Charts | **Current Era** |
|  | All healthcare use EMR  **Time**  2014  2028  ??? The sky is the limit.  We are here. |
| Key features:  Paper files  EMR developed.  File under lock and key protection | Differences from previous era:  EMR’s required by all healthcare providers.  Cybersecurity is needed to protect digital records.  Digital security methods needed and used.  Attacks trends rising and need for security continues to rise. |

### 2.3 Scanning Hits

Scanning Hit 1

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Title** | Health Care Cybersecurity: Past, Present and Future | | | | | **Author** | Mike Kijewski | | | | |
| **Source** | Kijewski, M. (2022, December 21). *Council post: Health Care Cybersecurity: Past, present and future*. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2022/12/20/health-care-cybersecurity-past-present-and-future/?sh=2b95ccf11b64 | | | | | **Date** | December 20, 2022 | | | | |
| **STEEP Categories** | Technological, Social | | | | | **Keywords** | Healthcare, Cyberattacks, Medical, security | | | | |
| **Type** | **Actual event** | **New trends** | | | | **New cycle** | **New plan** | **Potential event** | **New info** | | **New issues** |
| Already happened, but few know about, and implications not fully developed | Consistent increase or decrease, more or less of something over time | | | | Recurring increase and decrease, more and then less of something over time | Publicly announced intentions | A potential happening or occurrence | Information that has just been released | | Debate, conflict, decision, “Should we/they…” |
| **Brief description of the item** | This is a short look at some events from the past related to healthcare security, but it is also taking a small look into what the future might hold. There is also a bit of discussion related to the current state of cybersecurity in relation to healthcare, and medical information. | | | | | | | | | | |
| **How could the future be different as a result?** | The article speaks of a continued growth in breaches between 2009 and 2021, if the trend continues things will only get worse, and more PHI could end up exposed, without a change in how security works in healthcare. If this trend were to continue, not only would PHI be exposed, but the cost to organizations will rise, which could then be passed onto the patients. | | | | | | | | | | |
| **What are the potential implications for ...?** | **...Stakeholder name:** | | | | Healthcare organizations across the United States | | | | | | |
| If future considerations are not taken in relation to cybersecurity in healthcare, the amount of breaches in security could begin to rise again and cause an even larger expense within the healthcare industry. | | | | | | | | | | |
| **Horizon** | H1 Confirming | | H3 Resolving | H5 Creating | | | **Impact (0-5)**  4, most people that would read this will consider or look at their current setup and evaluate it for future issues. | | | **Plausibility (0-5)**  3 | |
| (baseline scenario) confirms the baseline future | | (between scenarios) indicates one scenario becoming more probable | (new scenario) indicates a potential new scenario | | |
| **Scanner** | The person submitting the hit.  Michael Winder | | | **Date Submitted**  **10/25/23** | | | **Novelty (0-5)**  5, released last year | | | **Timeliness (0-5)**  3, current trend in healthcare | |

Scanning Hit 2

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Title** | Computer attacks in health care are booming so far in 2023 | | | | | **Author** | Richard Payerchin | | | | |
| **Source** | Payerchin, R. (2023, August 9). *Computer attacks in health care are booming so far in 2023*. MedicalEconomics. Retrieved from https://www.medicaleconomics.com/view/computer-attacks-in-health-care-are-booming-so-far-in-2023 | | | | | **Date** | August 9, 2023 | | | | |
| **STEEP Categories** | Technological, Political, | | | | | **Keywords** | Security, PATCH Act, National Cybersecurity Strategy | | | | |
| **Type** | **Actual event** | **New trends** | | | | **New cycle** | **New plan** | **Potential event** | **New info** | | **New issues** |
| Already happened, but few know about, and implications not fully developed | Consistent increase or decrease, more or less of something over time | | | | Recurring increase and decrease, more and then less of something over time | Publicly announced intentions | A potential happening or occurrence | Information that has just been released | | Debate, conflict, decision, “Should we/they…” |
| **Brief description of the item** | This article discusses current trends in the current year with cybersecurity events in relations to the healthcare field. It shows the trends of the current year of the previous year and talks about how the government is beginning to get involved with the issue since it affects so many citizens. There is also a mention about new regulations that have come into play regarding new medical devices. | | | | | | | | | | |
| **How could the future be different as a result?** | Currently there was a lack of oversight when the U.S. Food and Drug Administration was approving new medical devices especially about the cybersecurity of the device. Just recently, a new PATCH act went into effect that requires all device manufacturers to meet at least four requirements before their device can be approved. This will lead to a better overall security. | | | | | | | | | | |
| **What are the potential implications for ...?** | **...Stakeholder name:** | | | | Healthcare, Political, Manufacturing | | | | | | |
| Should the manufacturers not abide by these new regulations, they could lose funding from investors. There could also be a lengthy period where new medical devices are not sent to market since, they might need to be modified to meet the new requirements. | | | | | | | | | | |
| **Horizon** | H1 Confirming | | H3 Resolving | H5 Creating | | | **Impact (0-5)**  5, new regulations typically lead to major changes | | | **Plausibility (0-5)**  5, there is always a need for change | |
| (baseline scenario) confirms the baseline future | | (between scenarios) indicates one scenario becoming more probable | (new scenario) indicates a potential new scenario | | |
| **Scanner** | The person submitting the hit.  Michael Winder | | | **Date Submitted**  **10/25/23** | | | **Novelty (0-5)**  5, article is from August of 2023, and speaks of regulations that went into effect in October of 2023 | | | **Timeliness (0-5)**  4 | |

Scanning Hit 3

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Title** | HC3 Outlines History of Healthcare Cybersecurity From 1980s to Now | | | | | **Author** | Jill McKeon | | | | |
| **Source** | McKeon, J. (2022, March 7). *HC3 outlines history of healthcare cybersecurity from 1980s to now*. HealthITSecurity. https://healthitsecurity.com/news/hc3-outlines-history-of-healthcare-cybersecurity-from-1980s-to-now | | | | | **Date** | March 7, 2022 | | | | |
| **STEEP Categories** | Technology, Economic | | | | | **Keywords** | Healthcare, cyberattacks, SolarWinds, WannaCry, | | | | |
| **Type** | **Actual event** | **New trends** | | | | **New cycle** | **New plan** | **Potential event** | **New info** | | **New issues** |
| Already happened, but few know about, and implications not fully developed | Consistent increase or decrease, more or less of something over time | | | | Recurring increase and decrease, more and then less of something over time | Publicly announced intentions | A potential happening or occurrence | Information that has just been released | | Debate, conflict, decision, “Should we/they…” |
| **Brief description of the item** | This article takes a good look at the history of some of the major cyberattacks, most of which have affected the healthcare industry in one way or another. While not all the attacks that are mentioned were specifically targeting healthcare systems, all the attacks mentioned are ones that could potential be used to attack a healthcare company or system. | | | | | | | | | | |
| **How could the future be different as a result?** | While the article does look at the history of events, it does make some recommendations for the future to assist healthcare companies with securing their system more. If you consider the past attacks and the vectors used, it only makes sense that those are typically the weak points and the ones that should be worked on when implementing or adjusting a cybersecurity policy. | | | | | | | | | | |
| **What are the potential implications for ...?** | **...Stakeholder name:** | | | | CISO, Healthcare organization, | | | | | | |
| Future consequences of this event for a specific person, group or domain. State the person, group or domain that would be affected. | | | | | | | | | | |
| **Horizon** | H1 Confirming | | H3 Resolving | H5 Creating | | | **Impact (0-5)**  3, while most of the information is historical, there is little that is unknown mentioned in the article | | | **Plausibility (0-5)**  3, this is more of a middle ground as most companies already have some of the policies mentioned in effect. | |
| (baseline scenario) confirms the baseline future | | (between scenarios) indicates one scenario becoming more probable | (new scenario) indicates a potential new scenario | | |
| **Scanner** | The person submitting the hit.  Michael Winder | | | **Date Submitted** | | | **Novelty (0-5)**  3, posted one year ago | | | **Timeliness (0-5)**  4 | |

Scanning Hit 4

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Title** | Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 to 2025 | | | | | **Author** | The primary author of the piece  Steve Morgan | | | | |
| **Source** | Morgan, S. (2020, November 11). *Healthcare industry to spend $125 billion on cybersecurity from 2020 to 2025*. Cybercrime Magazine. https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/ | | | | | **Date** | The date the piece appeared.  September 8, 2020 | | | | |
| **STEEP Categories** | Technological, economics | | | | | **Keywords** | COVID-19, healthcare spending, phishing | | | | |
| **Type** | **Actual event** | **New trends** | | | | **New cycle** | **New plan** | **Potential event** | **New info** | | **New issues** |
| Already happened, but few know about, and implications not fully developed | Consistent increase or decrease, more or less of something over time | | | | Recurring increase and decrease, more and then less of something over time | Publicly announced intentions | A potential happening or occurrence | Information that has just been released | | Debate, conflict, decision, “Should we/they…” |
| **Brief description of the item** | This article puts into perspective the rising costs of not only healthcare, but the costs of protecting patient information, or the costs of getting it back should a breach occur. It also takes a good look at the effects on healthcare of these attacks. | | | | | | | | | | |
| **How could the future be different as a result?** | When looking at the information within this article, there are several things that could cause the future to be different. The cost of healthcare could rise, or healthcare providers could close, causing patients to travel further, which may make then rethink about seeking medical attention. | | | | | | | | | | |
| **What are the potential implications for ...?** | **...Stakeholder name:** | | | | Medical practices, Healthcare, Patients | | | | | | |
| Future consequences of this event for a specific person, group or domain. State the person, group or domain that would be affected. | | | | | | | | | | |
| **Horizon** | H1 Confirming | | H3 Resolving | H5 Creating | | | **Impact (0-5)**  4, I feel that change should come from this information, but it is up to each individual organization to see the information and react. | | | **Plausibility (0-5)**  2, While I feel this should change the future, many organizations are stuck in their ways and may not react appropriately. | |
| (baseline scenario) confirms the baseline future | | (between scenarios) indicates one scenario becoming more probable | (new scenario) indicates a potential new scenario | | |
| **Scanner** | The person submitting the hit.  Michael Winder | | | **Date Submitted**  **10/25/2023** | | | **Novelty (0-5)**  3, around three years old | | | **Timeliness (0-5)**  4 | |

## Futuring

### 3.1 Baseline Future Inputs

|  |  |
| --- | --- |
| Trends (can say “more,” “less” or “continuation” of a change) | -Cybersecurity incidents will continue to target healthcare industry due to the amount of money that is to be made on the dark web in relation to other types of information being sold.  -The use of telehealth devices will continue to rise and be used more than regular visits as the technology improves. |
| Plans (announced intentions/plans of key stakeholders) | -Cybersecurity experts are expecting agencies to begin to adopt the use of AI into their cybersecurity toolkits. While nothing seems to have been officially announced for this, there are several blogs that hint towards the use of AI/ML in relation to cybersecurity in all fields.  -Increase training and awareness of end users. There is a need to make sure that healthcare end users have information on how to recognize common attacks, like phishing attacks. |
| Projections (baseline forecasts made by others, if any) | -The global Healthcare Cybersecurity Market size is projected to grow from USD 18.2 billion in 2023 to USD 35.3 billion by 2028, at a Compound Annual Growth Rate (CAGR) of 14.2% during the forecast period (MarketsandMarkets Research, 2023)  -The use of AI in healthcare specifically the cybersecurity of healthcare will begin to increase and be widely accepted throughout the industry. |
| Cycles | -At this point in the cybersecurity field, cycles have not been completely established. This area is still considered new and is on a steady growth pattern currently that has not fluctuated.  -The use of AI has been on a steady increase since its inception, and currently does not seem to be slowing down. |
| Constants | -HIPPA privacy regulations  -PATCH Act |

### 3.4 Alternative Future Inputs

|  |  |
| --- | --- |
| Trend Breaks | -Should a breach occur, clients would become skeptical of a specific company, and cause a shift in focus for that company, and the industry. |
| Events (including wildcards) | * Recession * Large breach that causes overall doubt in healthcare field * Changes in healthcare regulations |
| Issues (including conflicts, controversies, dilemmas, choices) | -Many healthcare organizations remain reluctant to openly disclose news of an incident or attack despite regulations to do so.  -Adoption of AI in healthcare has not gained traction yet. |
| Ideas (including images, perspectives) | One of the largest threats to the healthcare field regarding cybersecurity is internal threats.  A close-up of a computer  Description automatically generated (Bishara, 2023)  -Overall use of AI is adopted, and healthcare begins use of AI in cybersecurity efforts. |
| Key Uncertainties | -Internal errors in healthcare cybersecurity  -Adoption of AI in healthcare cybersecurity  -Regulations on AI use in the healthcare industry  -Overall Growth of AI |

## Visioning

### 4.1 Baseline Future

It is a Tuesday, I wake up early and have some coffee, get my kids up and get them off to school. After that I have some breakfast and start reading some morning news. Nothing that I do not do every other day. After breakfast, I head upstairs to my office, since I typically work from home, getting to the office is a breeze for me. Once in my office, I start waking up all my computers that I use throughout the day. As someone who works in security, there are always typically two or three computers in use, most have some specific uses.

As I get my computers on and running, I start loading some of the programs that I need, including my personal interface of the new AI based security monitoring software that keeps an eye on the network for me overnight, and assists during the day. The interface loads and in a ‘Jarvis-type’ voice I hear ‘good morning, there were no occurrences last night, and everything is looking ok at this time. Would you like me to open the logs for you to review.’ I answer in the affirmative. After reviewing the logs from the previous night to make sure that nothing obvious was missed, I continued with my day monitoring the network for security issues, and other normal daily tasks.

One of the tasks today is an important one to me. There are a bunch of new hires that I have a meeting with to talk about our security posture, and vet them into our security system. Although I am higher up in the management structure, this is something I still enjoy doing and do not mind taking off the plate of my team. After my meeting with the new hires, and talking to them about the company’s security posture, I scan their names into our AI security software and have it vet the user and assign security settings to them.

At this point I decided to have lunch and go downstairs. I cook myself some lunch and bring it back to my office to eat and monitor our systems. It is at this point that I notice the AI system has a couple alerts that a breach may be in progress. I also got a notification on my phone of an active breach in our system. I put my lunch aside for a second and clicked the alert button on my computer screen and let the AI system take over to actively mitigate the breach. At the same time, a meeting invites the entire security team along with CISO, and CIO to join to discuss what is going on.

Once everyone is in the meeting, we talk about the breach that is still active, but under control as the AI system is fighting back the attacker at a speed that is much quicker than the human attacker can combat. And, before we know it, the attack is over, and the authorities have been notified of the attempted breach, along with the attacker information so they can go pick him up and charge him.

At the end of the day, I once more click a button within the AI system that reviews the logs of the day and exports them to one of my many other devices for me to break them down more and review them later. This button also puts the AI into night monitor mode, which allows the AI to actively monitor and stop attacks without human intervention like earlier today.

### 4.2 Key Assumptions

There are a few key assumptions that could alter the outcome of this baseline. Any change to these could and would alter this baseline.

* Work from home is still possible.
* AI progress and Implementation is halted due to hazards or governmental oversite.
* AI is implemented and grows to a point where human interaction is no longer needed and monitoring is all automated.

Key Uncertainties

* Regulations on AI use in the healthcare industry
* Adoption rate of AI in all aspects of cybersecurity
* Growth of AI
* Increase in Internal errors in healthcare:

### 4.3 2x2 Matrix Alternate Futures

Internal Errors not checked.

High Adoption Rate

|  |  |
| --- | --- |
| Lack of service  -AI use is High outside of healthcare  -Regulations make implementation in healthcare difficult | Adoption rate  -AI is everywhere  -Data being used full of errors  -Breachers still occurring |
| Adherence  High Regulations  -Growth of AI is slowed  -Governmental oversight | Large Breaches  -Internal errors lead to large breaches  -AI not able to determine where breaches start |

Slow Growth in AI

#### Alternate Future 1: Lack of Service

It has been a busy year for me. While things have been improved in everyone’s personal life, including mine, by using AI in our everyday lives, it has made my job more difficult. Using AI daily allows me to get some tasks completed without ever having to leave my house. For instance, my groceries are kept track of by my appliances now, and if something is low it automatically creates an order and has it delivered; in fact, the AI is even able to determine when I begin to change eating habits and adjusts things accordingly. However, with work, the cybersecurity field in healthcare has not been so lucky with implementing AI into its workflow.

While AI is commonplace in the world today, to use it in healthcare there are so many regulations that are required to be followed, that it makes it almost impossible to implement AI in cybersecurity for any healthcare company. So, this makes long days at work, combing through log files, and monitoring traffic to make sure there are no data breaches.

#### Alternate Future 2: Adoption rate

What an exciting time to be alive. With the rapid growth of AI in technology, it has made most jobs easier to oversee, and increased efficiency for all workers as it is able to help make choices easier in everyday situations. However, today several members of my team found out that they are being replaced and will not have a job in a few months once the company completed the conversion to AI based security practices. And, while I, as the manager of the department, have voiced my opinion about this, and requested not to have anyone released, the senior managers have decided to go ahead with this anyway. As they believe that the use of AI can eliminate some jobs and increase profits. So, I have been tasked with giving this unwelcome news to my team.

I decided to have this meeting towards the end of the week, and most of my employees take it as good as they can, however most of them are highly upset about this, as they rightfully should be. I explain my stance on the subject to them and they understand it is outside of my control. After a few weeks the company completed the rollout of the new AI security software, and are assessing it, and so far, they believe it is doing a fantastic job, however, I am still reviewing the logs daily as a backup. As I review these logs, I notice a pattern, while the AI system can identify when a security breach is occurring, it is only identifying two distinct types of breaches, and flags others as no issue. I have one of my employees who is about to lose their job review these findings with me and he agrees. I bring the findings to the attention of my supervisor, and it appears that while the software was a solid AI implementation, the datasets that the senior management used to ‘train’ the software were flawed on its data. And there was never a proper review of this data. But they did not care, because they were told that the AI can still learn, but I inform them that the AI is only as good as the data it is fed, and now that it has learned wrong data, that breaches will still occur for months, if not years due to an improper dataset.

#### Alternate Future 3: Adherence

The technology of today is great, computers are everywhere, they are fast, dependable and state-of-the-art. However, using them to their full potential has been rough. Years ago, we started looking at a technology called AI, which was supposed to help speed up technology and assist us in making decisions at high rates of speed based on this technology. However, the growth expectations of AI were overestimated. While there are some AI systems out there, they are based on older technologies, and really do not work well in today’s world. Why you ask, well the government got involved in the AI industry, which slowed this growth rate down to a crawl. While previously developers of AI software were free to use every programming language, they were comfortable with. However, the government stopped that practice and adopted regulations that require AI to be developed using specific programming languages. The issue with this is that many of the languages that the government requires to be used are archaic and not a common type of language nowadays.

What does this mean for my current position at work, it means, if I want to use AI to assist in cybersecurity efforts, I need someone that can understand this archaic programming language, along with figuring out a way to integrate this into a modern computer system and network. For these reasons, currently, my company is not using AI to assist us, and has resorted to using live monitoring round the clock for all security incidents we are able to catch.

#### Alternate Future 4: Large Breaches

After many years of attempting to implement AI into my company’s cybersecurity program, I have decided to stop. The overall growth of AI in recent years has slowed to a crawl, due to many issues. For instance, datasets that are needed to train the AI are corrupt due to the continued increase in internal employee errors. These errors are attributed to lack of proper training, and lack of general care by most employees throughout the world. In fact, AI has become so difficult to train properly, that most developers that were working in this field have started to look for a better way, or a different path to follow.

So, what does this mean for my current company? Well, this mean that we will continue to enforce our cybersecurity the old-fashioned way, we will continue to send memos to employees, and manually review logs, and monitor the network for abnormalities in real time the best we can. However, due to the time it takes to review logs, this leads to increased time to find breaches, and stop them, or even to notice them at all. This leads to an increase in personal information that gets leaked each time there is a breach within the network.

## Project Summary

While AI is a common phrase in today’s world as it seems, everyone is talking about it, there is still room for this technology to grow. Yes, AI is being used in some areas of the world in technology currently, but there are still many uses of AI that are not being used currently. AI is an amazing technology that not only can assist with daily tasks but should also be able to take some workloads off humanity. The future of AI is the world is still as a whole unknown, however, the possibilities are endless. In fact, the use of AI in the Cybersecurity field for healthcare is a certainty by the year 2028.

Currently, there are some technologies now in cybersecurity that use things like machine learning, however, the full integration of AI has not yet occurred. Yes, there are some companies that are using “AI” in their software, but this software still needs human intervention to work properly. What I am talking about is a full AI that will be able to replace the human for certain tasks. For instance, overnight monitoring of the network for security breaches, and if one was to occur, then it notifies all appropriate personnel immediately, and assists with mitigating the incident. This is something that is not currently happening with the use of AI in cybersecurity. Currently, the AI being used will alert a human who then needs to alert response teams to mitigate the incidents. This is why we as an industry need to keep improving the structure of AI and growing it to a proficient level. And we need to continue to implement AI into company cybersecurity efforts to assist in “reducing the likelihood of misconfigurations, accidental data leaks, and other inadvertent mistakes that could compromise security” (Bonnie, 2023).

## Citations

Bishara, Y. (2023, October 30). *4 healthcare cybersecurity challenges*. Maryville University Online. https://online.maryville.edu/blog/healthcare-cybersecurity/

Bonnie, E. (2023, December 6). *How artificial intelligence will affect cybersecurity in 2024 & beyond*. Secureframe. https://secureframe.com/blog/how-will-ai-affect-cybersecurity

Davies, V. (2021, October 4). *The history of Cybersecurity*. Cyber Magazine. https://cybermagazine.com/cyber-security/history-cybersecurity

Department of Health and Human Services. (2022, February 17). *Electronic Medical Records in healthcare - hhs.gov*. Electronic Medical Records in Healthcare. https://www.hhs.gov/sites/default/files/2022-02-17-1300-emr-in-healthcare-tlpwhite.pdf

Filipkowski, B. (2023, July 31). *The top five healthcare cybersecurity issues to watch this year*. Field Effect. https://fieldeffect.com/blog/top-five-healthcare-cyber-security-issues-to-watch

Honavar SG. Electronic medical records - The good, the bad and the ugly. Indian J Ophthalmol. 2020 Mar;68(3):417-418. doi: 10.4103/ijo.IJO\_278\_20. PMID: 32056991; PMCID: PMC7043175.

Kijewski, M. (2022, December 21). *Council post: Health Care Cybersecurity: Past, present and future*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/12/20/health-care-cybersecurity-past-present-and-future/?sh=2b95ccf11b64

McKeon, J. (2022, March 7). *HC3 outlines history of healthcare cybersecurity from 1980s to now*. HealthITSecurity. <https://healthitsecurity.com/news/hc3-outlines-history-of-healthcare-cybersecurity-from-1980s-to-now>

MarketsandMarkets Research Pvt. Ltd. (2023, May 5). *Healthcare cybersecurity market worth $35.3 billion by 2028, growing at a CAGR of 14.2% : Report by MarketsandMarketsTM*. GlobeNewswire News Room. https://www.globenewswire.com/en/news-release/2023/05/05/2662628/0/en/Healthcare-Cybersecurity-Market-worth-35-3-billion-by-2028-growing-at-a-CAGR-of-14-2-Report-by-MarketsandMarkets.html

Miller, E. (2023, April 26). *The state of healthcare cybersecurity: Top insights and trends*. BitLyft. https://www.bitlyft.com/resources/state-healthcare-cybersecurity

Morgan, S. (2020, November 11). *Healthcare industry to spend $125 billion on cybersecurity from 2020 to 2025*. Cybercrime Magazine. https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/

Payerchin, R. (2023, August 9). *Computer attacks in health care are booming so far in 2023*. MedicalEconomics. <https://www.medicaleconomics.com/view/computer-attacks-in-health-care-are-booming-so-far-in-2023>