RMIT UNIVERSITY

ISYS3444

INTRODUCTION TO ENTERPRISE ARTIFICIAL INTELLIGENCE

SGS - Group 2

Assignment 3

PROJECT PITCH

SingHealth

Defining Tomorrow's Medicine

Instructor: Dr. An Nguyen

Le Dieu Ha (s3979364)

Ngo Phuc Thinh (s3990389)

Nguyen Tri Thuc (s2939515)

Bui Thi Kim Thuy (s3903720)

Nguyen Thuy Truc (s3972621)

ISYS3444 – ASM 3

Course Code	ISYS3444
Course Name	Introduction to Enterprise Artificial Intelligence
Location	SGS Campus
Assignment Title	Assignment 3: Project Pitch
Lecturer	Dr. An Nguyen
Student Names	Le Dieu Ha (s3979364) Ngo Phuc Thinh (s3990389) Nguyen Tri Thuc (s2939515) Bui Thi Kim Thuy (s3903720) Nguyen Thuy Truc (s3972621)
Group Number	Group 2
Number of Pages	29
Word Count	3746
Due Date	26 January 2024
Date of Submission	26 January 2024

We declare that in submitting all work for this assessment, we have read, understood and agreed to the content and expectations of the Assessment Declaration.

ABBREVIATIONS:

The SCM System	The Sunrise Clinical Management System
SELENA +	Singapore Eye Lesion Analyser
JARVIS-DHL	Transforming Chronic Care for Diabetes, Hypertension and HyperLipidemia
CAPE	COVID-19 Artificial Intelligence Predictive Engine
ML	Machine Learning
AI	Artificial Intelligence
NLP	Natural Language Processing
PHI	Patient Health Information
APT	Advanced Persistent Threats
EHR	Electronic Health Records
HIPAA	Health Insurance Portability and Accountability Act
PDPA	Personal Data Protection Act
HMDP	Healthcare Manpower Development Program
SIEM	Security Information and Event Management
EDR	Endpoint Detection and Response
IDS/ IPS	Intrusion Detection System/ Intrusion Prevention System

TABLE OF CONTENT

I. INTRODUCTION

In the quickly changing healthcare industry, AI has become essential for enterprises trying to enhance patient outcomes, increase operational efficiency, and safeguard sensitive data. This paper explores the cybersecurity issues Singapore's leading healthcare organization, SingHealth, faced after a significant data breach in 2018. SingHealth's dedication to modernity and public health is balanced against the requirement to fortify its digital footprint protection as the custodian of patient information in many venues. The thorough study describes the organization's activities, projects its future course, evaluates its current strengths and weaknesses, and suggests strategic AI solutions to close security holes and guarantee patient data integrity.

II. AI SOLUTION SUMMARY AND JUSTIFICATION

1. SingHealth's Background Information

1.1. SingHealth's Operation Scale

SingHealth is the largest healthcare group in Singapore, established in 1998 (SingHealth n.d.). It oversees the Eastern Region's patient records across its four public hospitals, three community hospitals, five national specialty centers, and eight polyclinics (SingHealth 2022).

1.2. Vision

The organization's future-oriented vision involves continuously modernizing its service models and enhancing overall community health (SingHealth 2023). This vision demonstrates SingHealth's ongoing efforts to digitize patient records, integrate AI into diagnosis and treatment, and other achievements.

1.3. Cyber Incident in 2018

SingHealth declared EHRs their most crucial asset and took full responsibility for protecting patient data under PDPA law (COI 2019; SingHealth n.d.). Thus, the 2018 data breach incident of 1.500.000 patients' data (including the Prime Minister's) significantly impacted the hospital's reputation (COI 2019). This event is also the primary target that this report aims to address.

2. SWOT & PESTLE analysis

2.1. SWOT analysis

STRENGTHS	WEAKNESS
• Reputation • Robust Infrastructure • Skilled workforce • Research and Innovation	• Reliance on Government Funding • Limited Capability in Assessing and Responding to Risks. • No Proper Network Security Team
OPPORTUNITIES	**THREATS**
• Technological Advancement • International Collaboration	• Regulatory Changes • Cybersecurity Risks • Competitors

Figure 1: SingHealth's SWOT analysis

Despite SingHealth's reputation for good infrastructure and skilled staff, there are still areas for improvement, such as malfunctioning working procedures and limitations in human capabilities to assess risks and respond to threats. Those weaknesses are identified as the root causes of the data breach in 2018. Besides, given the sensitive nature of data and increasing reliance on digital systems, healthcare is the most vulnerable to cyber-attacks. Therefore, organizations, including healthcare institutions like SingHealth, can ensure strong cybersecurity through new technological advancements and international cooperation.

2.2. PESTLE analysis

Political	• Huge support and control from government policies: having IHiS as the IT arm of MoH to oversee the healthcare system, facilitate training abroad (HMDP), etc (MoH n.d.). • Political stability
Economic	• Healthcare expenditure: spend $3.5 thousand per person on healthcare (less than the USA but provides more quality) (The World Bank 2023) • Economic growth
Social	• High community awareness of personal information: more than half - 56.2% and rank 2nd (after India) globally in data privacy awareness (SBR 2020)

	• High AI readiness in government, business and consumers (Salesforce 2021).
Technological	• Technology advancement: launched the Singapore National AI Strategy 2.0 (NAIS 2.0) in 2023 (Smart Nation n.d.). • Data management and privacy
Environmental	• Resource consumption (hardware, software, etc.)
Legal	• National Healthcare Regulations (HIPAA;...) • Intellectual Property Protection (Förster n.d.) • Domestics Regulations: PDPA 2012 - Key Data Protection Legislation in Singapore (Lim 2022)

Figure 2: SingHealth's PESTEL analysis

A wide range of factors shapes cybersecurity in healthcare. Strong cybersecurity protections are established by regulatory frameworks, such as those typified by healthcare acts like HIPAA and PDPA, while the efficiency of enforcement mechanisms is measured by the level of political stability in the current political climate. Socially, the public's rising knowledge of protecting personal information reveals ingrained societal issues that need corrective action following the 2018 events to rebuild SingHealth's image. In an ever-changing technological world, embracing technological advancements while maintaining sufficient privacy and data management procedures is critical. Environmental factors, including the resource usage of hardware and software, influence the sustainability of healthcare institutions.

3. Problem Statement

Aligning the aforementioned statement with the insights gained from the PESTLE analysis and considering actual incidents within the hospital and two other healthcare facilities in Singapore, it is evident that safeguarding data security *is no longer an optional feature but has evolved into a vital necessity for survival*. This is because data, including PHI and EHRs if fallen to the hands of cyber-criminals, can result in identity theft for carrying out illegal loans/ credit cards or delay in providing medical care, which is detrimental to the patient's life (Alder 2023; Wetsman et al. 2023). Essentially, it is no longer just a "patient privacy issue" but a critical "patient safety issue."

Recognizing the vulnerabilities identified within the SingHealth security team, including limited capabilities in risk assessment and delayed responses to threats, it is essential to utilize AI technology to supplement and automate human efforts in combating cyber risks.

4. Current Use of AI

Notable AI applications at the organizational level in SingHealth include Doctor Covid, a multilingual chatbot designed to facilitate communication in their native languages with migrant workers infected with COVID-19 (Chong 2021). By harnessing NLP and ML technology, this AI tool enhances healthcare teams' capability to remotely monitor clinical and mental well-being, effectively overcoming language barriers (Perdana and Mokhtar 2023).

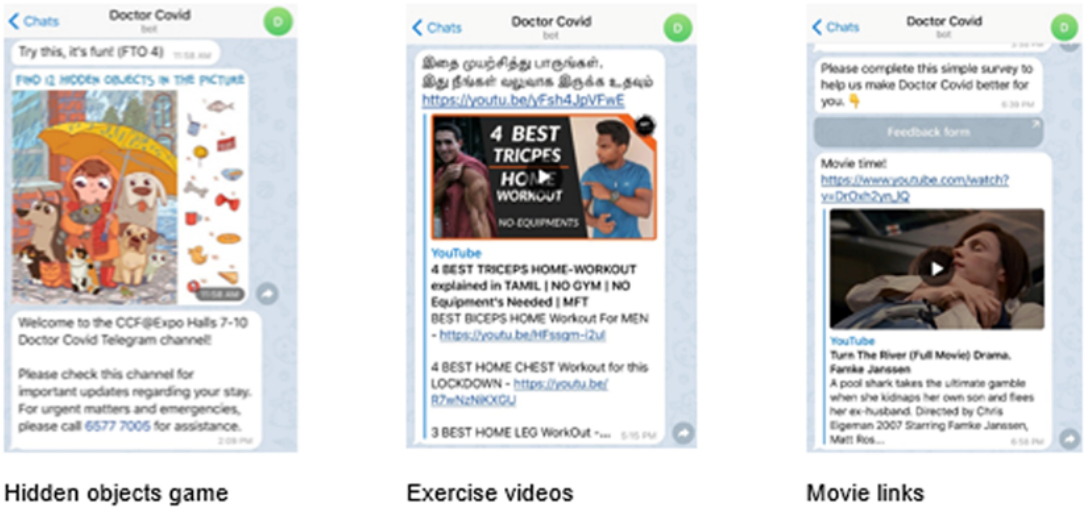

Figure 3: Doctor Covid Interface

Another significant innovation is the Singapore Eye Lesion Analyser (SELENA+), an AI-powered image reader specialized in analyzing eye scans to identify indications of diabetic eye diseases. Employing advanced computer vision algorithms, SELENA+ enables early and precise detection of eye conditions, streamlining the screening process and ensuring prompt intervention.

Despite numerous applications and the potential for harnessing AI capabilities, a specific implementation to effectively address the cybersecurity challenges at SingHealth has yet to be developed. Consequently, the hospital must adopt an AI-based solution for its vulnerability management initiatives.

5. Related AI Solution

Following the drawn conclusion, a CyberAI application that exploits the power of both ML and NLP is proposed to SingHealth. It aims to enhance the cybersecurity practices of this hospital as it will detect vulnerabilities and threats in the hospital's system, network, endpoints, etc. (IBM n.d.a). Assisting the security team in assessing risk, providing EHR protection functionality, and responding to these threats (Amos 2023), creating a 90% reduction in triage time (Darktrace n.d.a).

6. Stakeholder analysis

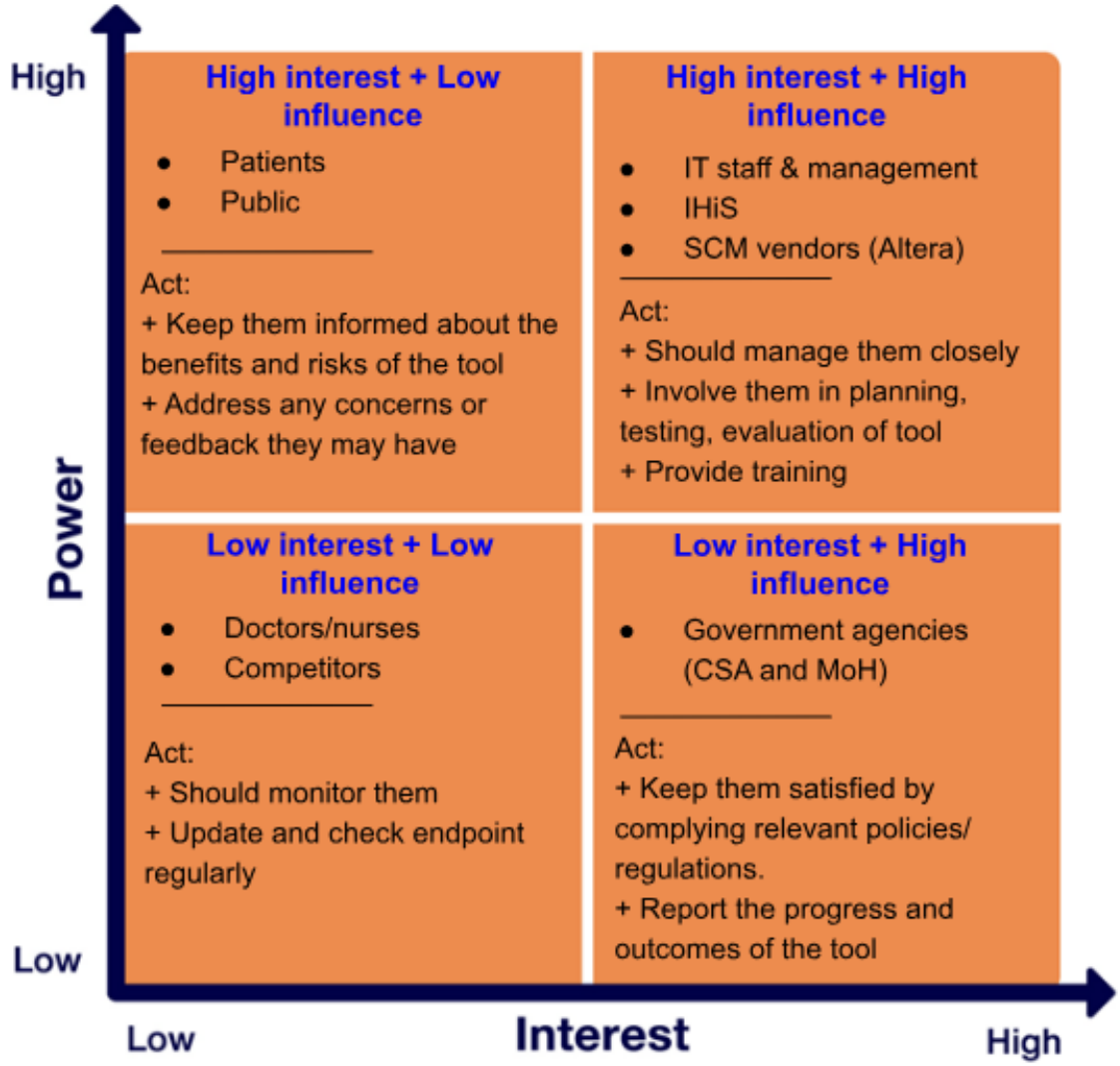

Figure 4: Stakeholders Map of CyberAI Project

Figure 4 depicts the key stakeholder groups for SingHealth's proposed AI cybersecurity tool and their level of interest in its application.

Overall, the IT staff, IHiS, and SCM vendors, such as Altera, require the most attention as they will interact directly with the tool. Specifically, the IT staff will be responsible for using the tool, IHiS/BoD will manage the hospital's infrastructure, and vendors will provide products like SCM systems that enable AI integration.

The figure also classifies other stakeholders and communication strategies. Some prominent communication strategies include training, compliance with the law, and prioritizing information provision to one party. Hence, these strategies need to be allocated accurately and effectively.

III. AI STRATEGY

1. Goal

In addressing the throbbing issue of cybersecurity, a powerful AI is required to protect EHRs and effectively enhance the efficiency of detecting, preventing, and mitigating cyber threats by 25%, with a minimum accuracy of 90% and within an affordable budget range. With this objective in mind, an AI solution is proposed below.

2. CyberAI Use Case

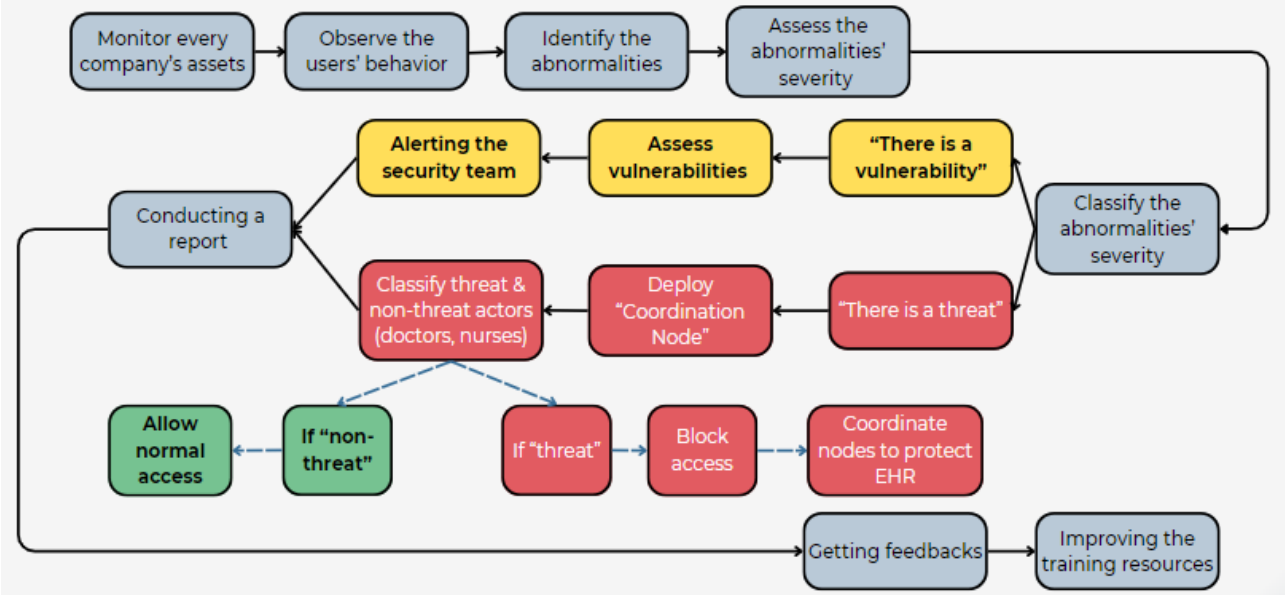

Figure 5: CyberAI Step-by-Step Process

3. Data Strategy

Data Strategy				
Data Category	**Data Collected**	**How to collect?**	**How to process?**	**How is it being used?**
System Behavior (Current and Past Data)	+ System Process + Resource Usage + Normal Network Flow + Endpoints (Xiarch Solutions 2023)	+ SIEM system + EDR, IDS/ IPS (Vectra n.d.)	+ Unsupervised ML	Learn Organization's Activities: Pattern Changes → Detected Deviations (Krishnappa 2023).

	+ Past Behavior of the system/ network/endpoints experienced cyber-attacks	+ SIEM system + EDR, IDS/ IPS	+ Unsupervised ML	
Upcoming Threats	+ Unstructured data (cyber reports, news, forums…) (Darktrace n.d.; Kuppuswamy 2023)	+ Cyber reports + Hackers' forum	+ NLP + Predictive analysis	Gain insights → Develop incident response plan → Communicate with the security team
Users Behavior	+ Normal activities	+ Cookies (Marr 2017)	+ Behavioral analysis + Predictive analysis	Detect abnormalities → Deploy proactive prevention plans.
Common threat characteristics	+ Characteristics (from malware, phishing attacks, etc.) + Common response	+ IDS/ IPS	+ Predictive analysis + Supervised ML	Assess Threat Severity level (hospital assets) → Find ways to respond.
Authorize accounts access list	Users, actions which are authorized access (Frontegg 2022)	+ SIEM system	+ Supervised ML	Assess and grant accessibility.

Figure 6: Summary of Data Strategy of CyberAI

4. Architecture

After determining CyberAI's data strategy, the next step is to examine SingHealth's current infrastructure, what is needed, and its compatibility with the proposed solution in this report.

The important thing is not simply owning a large amount of data, but rather how to transform this data into useful insights that can benefit protecting EHR and improving the data security of hospitals. Therefore, based on the guidance of Marr (2017), the infrastructure is divided into 4 factors: "Data collection", "Data storage", "Data analysis and processing", and "Providing access to data" (as shown in Figure 1). This part aims to provide a clearer view for developers to build an actual application.

The Architecture of the Proposed CyberAI	
Layers of big data	**Infrastructures (Tools/Services/Technology)**
Data Collection	• SIEM system (ManageEngine Log360) • EDR agent (Cisco AMP) • IDS/IPS (Cisco Secure IPS) • Cookies
Data Storage	The Sunrise Clinical Management (SCM)
Data Analysis and Processing	TensorFlow
Providing Access to Data	Citrix Virtual Application

Figure 7: Summary of Architecture of CyberAI

4.1. Data Collection

Concerning the SIEM system, the utilized tool will be ManageEngine Log360 as it will collect logs on SingHealth's site and cloud system (Keary 2024). Also, this SIEM system tracks access control, helping to monitor every action taken by authorized users (Utilities One 2023).

Since Cisco AMP offers the collection capability of the entire endpoint environment (Malllick 2022), it will be the appropriate EDR tool to be employed in the development of this Cyber AI. Combining with the IDS/ IPS from the same provider - Cisco, Cisco Secure IPS, helps monitor the network behavior, and system protocol to detect intruders (Mallick 2022).

4.2. Data Storage

The question here is where will the data required to be collected by CyberAI as per the data strategy be stored.

SingHealth's current infrastructure uses SCM - a third-party platform from Altera - to manage all of the hospital's data and secure EHRs since 1998. The contract between the two companies has been extended till 2029 (Ang 2022).

In addition, SCM also supports storing and categorizing large data sets through a BI solution (called Sunrise Clinical Performance Manager) - which is very suitable for storing the diverse datasets

collected from CyberAI's data strategy (Altera n.d.). Furthermore, Altera provides technical consulting teams to SingHealth throughout the contract period to ensure SCM operations (Ang 2022). Therefore, the safety of CyberAI's collected data can be guaranteed.

4.3. Data Analysis and Processing

Regarding data analysis and processing, TensorFlow will be an appropriate open-source machine learning framework since it offers the developers a semi-supervised machine learning model, making it appropriate for the development of this Cyber AI technology. This platform also provides analytic tools such as natural language processing to support extracting insight from text (Vega 2023), and logistic regression can be used to help detect threats and calculate the possibility of threat levels in binary.

4.4. Providing Access to Data

Coming to the final layer, the problem to be solved is which technology will be used to provide access to CyberAI.

Specifically, the data of CyberAI can only be accessed by IT teams and senior management level, so even though it is integrated into the data system, access is very limited. In addition, CyberAI aims to provide a platform that can be integrated into SingHealth and still comply with the regulations of the Ministry of Health. Therefore, Citrix Virtual Application is a suitable option - managed by IHis (under MoH).

4.5. Data Transmission

An additional layer that needs to be considered here is that SingHealth manages all branch hospitals in the eastern region, so what is the supporting tool for data transmission?

Singapore's healthcare system is a tightly centralized system with close supervision from the Ministry of Health and government. Therefore, to control medical operations in 3 different regions, one shared patient cloud data is regulated as H-Cloud.

Intending to comply, being transparent with MoH, and transmitting data between hospitals, H-Cloud meets security standards (Synapxe n.d.).

5. Organizational Capability

5.1. Strengths in the Data Set, Research Culture, and Hospital Budget

In terms of organizational capability for adopting new AI cybersecurity tools, SingHealth demonstrated several strengths.

The most notable strength is owning a large, high-quality digitalized dataset accumulated over 20 years (Ang 2022; Toh 2022). This confers benefits to AI adoption, including a specialized IT workforce, robust digital infrastructure for patient profiles (SCM system), and a cultural acceptance - a readiness to adopt new technologies.

Secondly, SingHealth has a strong culture of AI research, evidenced by numerous organized AI research projects (e.g. SELENA+, JARVIS-DHL, CAPE, etc.) (Rani 2022; Tomorrow's Medicine 2021; Koh 2020). This signifies that conveying the concept of this recommended cybersecurity AI tool should not be too difficult as the hospital already possesses a certain level of baseline expertise, and the project is believed to be well-managed.

Thirdly, regarding budget, the COI report (2019) stated that SingHealth approved all budget requests relating to cybersecurity. This demonstrates that SingHealth's sound financial backing and funding are not a hindrance to AI implementation.

5.2. Weaknesses in IT Staff Mindset and Cybersecurity Expertise of Senior Management Level

However, SingHealth's current resources could potentially obstruct the adoption of this report's recommended AI tool. Firstly, cultural complacency, as evidenced by IT staff only notifying superiors of cybersecurity incidents after full resolution (COI 2019). Finally, SingHealth lacks cybersecurity expertise at senior management levels, as shown by wholly outsourcing IHiS (COI 2019).

While this report proposes AI cybersecurity tools, ongoing senior management oversight, and awareness remain crucial, as AI tools cannot be solely responsible for all cybersecurity incidents. Hence, these two factors need to be addressed in the Change Management strategy.

6. Change Management

Integrating AI into SingHealth's cybersecurity framework required meticulous consideration of various factors, with a particular emphasis on change management. Below are some important points that need attention:

First, applying AI needs to ensure buy-in from all stakeholders, including upper management, IT staff, and end users. For a large enterprise, effectively communicating the benefits that AI brings to cybersecurity, such as enhanced threat detection and mitigation, is integral to gaining this support (Corrigan 2022). Furthermore, the delineation of responsibilities is essential for seamless AI implementation. Clearly defining which individuals are tasked with AI model training, system integration, and ongoing AI maintenance will help businesses minimize the risks and costs of applying AI. may arise (Malamateniou et al 2021).

Following that, comprehensive training programs for appropriate employees are another extremely important aspect. Ensuring that all employees understand how to effectively use the AI system, including understanding its output and responding competently to various threat alerts, is essential.

IV. BUSINESS CANVAS MODEL ANALYSIS

The Business Model Canvas **(Figure 8)** illustrates how CyberAI can create, deliver and capture value from customers.

<table>
<tr><td colspan="2"><u>Company:</u> TensorFlow</td><td colspan="2"><u>Client:</u> SINGHEALTH Hospital</td><td><u>Date:</u> Jan-2024</td></tr>
<tr><td><u>Key Partners:</u>
Government agencies - must comply with and receive support from.
Vendors/ Suppliers of hardware.</td><td><u>Key Activities:</u>
Empathise SingHealth’s problems and develop a customized AI software solution.
Help deploy the software integrated with SingHealth’s current system.</td><td><u>Value Propositions:</u>
An AI-based solution that transforms the way SingHealth stores and protects customers’ data.</td><td><u>Customer Relationship:</u>
Offer 60-day free-of-charge trial access to the Minimum Viable Product of CyberAI.</td><td><u>Customer Segment:</u>
Business-to-business: Hospitals.
Firmographics: located in Eastern Singapore, leading the Eastern network of healthcare.
Technographics: highly digitalized,</td></tr>
</table>

<table>
<tr>
<td rowspan="2"></td>
<td>

Train security staff to adapt to the new software.
Maintenance and keep the software up-to-date.

</td>
<td rowspan="2"></td>
<td rowspan="2"></td>
<td rowspan="2">operate collaboratively in a cloud-based suite.
• Needs-based: quality-focused segment.
• Sophistication-based: never used AI for security before.</td>
</tr>
<tr>
<td><u>Key Resources:</u>
Powered by Google exclusive intelligence on phishing behaviours.</td>
<td><u>Channels:</u>
• AI Platform: TensorFlow.
• Cloud: H-cloud.</td>
</tr>
<tr>
<td colspan="3"><u>Cost Structure</u>
• Fixed costs: Proof-of-concept, Infrastructure, Cloud server, Professionals.
• Variable costs: Extra cloud storage if data increases in volume.</td>
<td colspan="2"><u>Revenue Streams</u>
• Software sales
• Support and Care service, including deployment and frequent maintenance.</td>
</tr>
</table>

Figure 8: CyberAI's Business Model Canvas

1. Customer Segment

CyberAI targets healthcare businesses with particular characteristics. Firstly, they should be large-sized healthcare organizations conscious of personal data security. Those are the most vulnerable prey to cyber attacks (Pitchkites and Leavitt 2024). Secondly, regarding the Technographics traits, the target organization should have a digitalized setup of cutting-edge technologies in diagnostics and medical R&D, demonstrating a strong capability of adopting AI. Lastly, on organizational needs, the target customers of CyberAI are willing to invest significantly in an application ensuring optimal protection for patients' EHR. Taking into consideration all the factors above, it is identified as a promising client likely to adopt the CyberAI solution.

2. Value Proposition

The key value proposed to SingHealth is an *operational efficiency solution* powered by AI that transforms the way the hospital handles its customers' data, including collecting and storing data that is robust against attacks, saving hospitals from losing $4 million in damage caused by data breaches (Pitchkites and Leavitt 2024).

3. Channels

An indispensable asset is the Healthcare Cloud (H-Cloud), a unified cloud computing platform that facilitates healthcare professionals at all public healthcare centers in Singapore to retrieve and access patient records (Synapxe n.d). The usage of this platform is mandatory for all tech-based solutions in the healthcare industry by the Singapore Government to ensure the centralization and accessibility of healthcare data.

4. Customer Relationships

The marketing strategy for the AI software involves providing a 60-day short-term free trial of the Minimum Viable Product (MVP) to healthcare organizations. This allows them to evaluate the product's effectiveness and compatibility before making a commitment.

5. Key Partners

- **Government Agencies:** Besides complying with the Government's regulation, SingHealth stands to gain from government support policies and funding opportunities (Tan et al. 2021).
- **Vendors/ Suppliers of Hardware:** In the realm of cybersecurity, CyberAI must procure essential resources from reputable vendors, including Firewall, Endpoint Security, Antivirus, Endpoint Detection and Response, Antivirus Software, Email Protection and Two-Factor Authentication (Miller 2021). The effectiveness of launching CyberAI is directly influenced by the quality of these hardware and software provisions since threats can penetrate SingHealth through third-party vendors if their system is not sufficiently resilient.

6. Key activities

In delivering value to the target customer, CyberAI must offer several activities as follows:

- Empathizing with SingHealth's challenges through a SWOT analysis **(Section II.2)**. Utilizing a profound understanding of the organization, the project team designs a CyberAI solution tailored to meet the specific needs and requirements of SingHealth **(Section III.2)**.

- After ideating the CyberAI solution, intelligence on the organizational capability is gathered **(Section III.4)** to develop a customized implementation plan, guiding SingHealth in successfully integrating the AI software with its existing system.
- Concurrently deploying the AI solution, a change management plan **(Section III.5)** is executed to prepare the employees for adopting this new technology.
- Regular maintenance and updates are essential to address cyber threats' increasing frequency and complexity, necessitating improved security solutions accordingly.

7. Key Resources

The TensorFlow platform is backed by Google, the most popular search engine and browser in the world, which has been collecting insightful data about phishing browsing behaviors (Sjouwerman 2024), informing the project team an advantage of knowledge in building an effective data strategy for CyberAI.

8. Cost Structure

In the cost structure of this CyberAI, fixed costs, including developing Proof of Concepts, renting Infrastructure and Cloud servers, and recruiting professionals, are the key components in developing an AI solution. However, if the volume of data increases as the number of patients registered to a hospital surges, the cost for the cloud server is subjected to changes, denoted as a variable cost.

Suppose it takes 3 years to fully develop a CyberAI program and note that the monthly investment in the solution is $25,380, the total cost to develop the program is $913,680 (Find detailed cost estimation in **Appendix A**).

9. Revenue Streams

With the outlined Key Activities, the primary revenue stream is derived from software sales, priced at $70,000 per package, excluding cloud costs and other Software as a Service (SaaS) expenses. To attain break-even, CyberAI is projected to sell approximately 13 packages and generate additional revenue from complementary services such as maintenance and upgrades.

V. CONCERNS

In developing a CyberAI for SingHealth, several critical considerations must be addressed to ensure the technology's effectiveness, compliance, and ethical use.

Incident response and reporting are paramount for a robust network security system. Building and maintaining an effective incident response plan for security breaches is indispensable. This plan should include clear procedures for reporting breaches to authorities and affected individuals, ensuring compliance with Singapore's data protection laws. Proactively handling security incidents minimizes legal consequences and builds trust with stakeholders, which is crucial for SingHealth's reputation (Ruefle et al. 2014; Habbal et al. 2024).

This AI project is designed to support the hospital in implementing cybersecurity practices and fostering a collaborative environment between humans and AI. Emphasizing compliance with the AI ethics framework, the goal is not to replace human control (Witzsche 2023). Moreover, integrating AI-based threat-hunting, replacing traditional techniques, can enhance the detection rate to approximately 95% (Segal 2020; Dekker 2022). However, this also implies a potential false positive rate of around 4-5%, necessitating the involvement of expertise and security personnel to monitor AI development and provide human confirmation in applicable situations.

This raises legal responsibility and accountability concerns**,** emphasizing the need for transparently defined comprehensive terms and conditions outlining AI capabilities (Leslie 2019, Teo et al. 2023). Specifically, in the event of an erroneous cyber attack prediction, accountability rests with the AI provider.

Additionally, staying informed about ***Government regulations and guidelines*** related to cybersecurity and AI in Singapore is crucial (Doshi-Velez et al. 2017). In accordance with the PDPA 2022, SingHealth is obligated to inform patients about how their personal data will be handled and provide insights into associated risks while operating CyberAI (Lui et al. 2022).

VI. CONCLUSION

To summarise, the CyberAI solution that has been suggested is a calculated reaction to the cybersecurity issues facing SingHealth. It utilizes artificial intelligence to enhance data security and reduce possible risks. This in-depth study examines organizational capacities, change management, and sustainable business models and offers an implementation roadmap. SingHealth can establish itself as a pioneer in healthcare cybersecurity and guarantee patient safety and confidence in the digital age by carefully evaluating the ideas presented and resolving the issues raised.

APPENDIXES:

The breakdown costs of developing the CyberAI application are provided in Appendix A below.

Tasks	Tools/ Infrastructure	Price ($/month)
Data Collecting	IDS/IPS (Cisco Secured IDS)	$3,000
	SIEM (Log360)	$200
	EDR (Cisco AMP)	$1,680
Data Storage	EHR database by SCM	$1,000
	H-cloud	$1,500
Data Analysis and Processing	TensorFlow	$0.00
Providing Access to Data	Citrix	$7,000
Deployment		
Developers Salary	_ 2 Developers	$4,000
Project Manager Salary		$3,000
Maintenance		
Developers + Data Scientist	_ 3 months	$4,000
Total		**$25,380**

Appendix 1: The Budget Plan

REFERENCE:

Alder S (2023) *Editorial: Why Do Criminals Target Medical Records*, HIPAA Journal website, accessed 23 January 2024. https://www.hipaajournal.com/why-do-criminals-target-medical-records/

Amos Z (2023) AI Is Crucial for Healthcare Cybersecurity, Unite.AI website, accessed 23 January 2024, https://www.unite.ai/ai-is-crucial-for-healthcare-cybersecurity/

Ang A (2022) *SingHealth extends Sunrise contract with Altera Digital Health for interoperability*, Healthcare IT News website, accessed 22 January 2024. https://www.healthcareitnews.com/news/asia/singhealth-extends-sunrise-contract-altera-digital-health-interoperability

Armerding T (2018) *SingHealth hit with 'unprecedented' cyber attack*, Synopsys website, accessed 23 January 2024. https://www.synopsys.com/blogs/software-security/singhealth-cyber-attack.html

Chong C (2021) S'pore's health science innovations get AI boost in SingHealth, SGInnovate tie-up. The Straits Times. https://www.straitstimes.com/singapore/spores-health-science-innovations-get-boost-from-artificial-intelligence-in-singhealth. Accessed 24 Jan. 2024.

Committee of Inquiry (2019) *Public Report of the Committee of Inquiry into the cyber attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018*, Government Technology Agency, Singapore Government, accessed 22 January 2024. https://file.go.gov.sg/singhealthcoi.pdf

Corrigan CC (2022) Lessons learned from co-governance approaches–Developing effective AI policy in Europe. In *The 2021 Yearbook of the Digital Ethics Lab* (pp. 25-46). Cham: Springer International Publishing, accessed 22 January 2024.

Darktrace (n.d.a) *Protecting Hospitals From Ransomware*, accessed 26 January 2024. https://darktrace.com/resources/protecting-hospitals-from-ransomware

Darktrace (n.d.b) *Darktrace AI: Combining Supervised and Unsupervised Machine Learning*, Darktrace website, accessed 24 January 2024. https://darktrace.com/resources/darktrace-ai-combining-supervised-and-unsupervised-machine-learning

Dekker N (2022) *33 Emerging Artificial Intelligence Statistics*, eftsure website, accessed 26 January 2024. https://eftsure.com/statistics/artificial-intelligence-statistics/#source-wrapper

Doshi-Velez F, Kortz M, Budish R, Bavitz C, Gershman S, O'Brien D, Scott K, Schieber S, Waldo J, Weinberger D and Weller A (2017) Accountability of AI under the law: The role of explanation. *arXiv preprint arXiv:1711.01134*, accessed 23 January 2024.

Exabeam (n.d.) *Threat Detection and Response: Technologies and Best Practices*, Exabeam website, accessed 24 January 2024. https://www.exabeam.com/explainers/next-gen-siem/threat-detection-and-response-technologies-and-best-practices/

Förster M (n.d.) *Intellectual Property Protection*, ASEAN Briefing website, accessed 25 January 2024. https://www.aseanbriefing.com/doing-business-guide/singapore/company-establishment/intellectual-property-protection

Frontegg (2022) *What Is Attribute-Based Access Control (ABAC)?,* Frontegg website, accessed 24 January 2024. https://frontegg.com/guides/abac

Habbal A, Ali MK and Abuzaraida MA (2024) Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*, p.122442, accessed 23 January 2024.

https://www.moh.gov.sg/hpp/all-healthcare-professionals/programmes/ProgrammeDetails/health-manpower-development-plan-visiting-experts

IBM (n.d.a) *Artificial Intelligence (AI) Cybersecurity*, IBM website, accessed 23 January 2024. https://www.ibm.com/ai-cybersecurity

Kar A, Wreesmann VB, Shwetha V, Thakur S, Rao VU., Arakeri G and Brennan PA (2020) Improvement of oral cancer screening quality and reach: The promise of artificial intelligence. *Journal of Oral Pathology & Medicine*, *49*(8), pp.727-730, accessed 23 January 2024.

Keary T (27 February 2024) *The Best SIEM Tools for 2024: Vendors & Solutions Ranked*, Comparitech website, accessed 26 January 2024. https://www.comparitech.com/net-admin/siem-tools/

Knowledge Bank (n.d) *Singapore's Journey to Build a National Electronic Health Record System,* Hospital & Healthcare Management website, accessed 23 January 2024. https://www.hhmglobal.com/knowledge-bank/articles/singapores-journey-to-build-a-national-electronic-health-record-system

Koh D (2020) *CGH & IHiS develop AI tool to predict severity of pneumonia in patients*, Healthcare IT News website, accessed 22 January 2024. https://www.healthcareitnews.com/news/asia/cgh-ihis-develop-ai-tool-predict-severity-pneumonia-patients

Krishnappa T (2023) 'A REVIEW ON ARTIFICIAL INTELLIGENCE TECHNIQUES IN PREVENTING CYBER THREATS', *International Journal of Engineering Applied Sciences and Technology*, 8(1):185-189, doi:10.33564

Kuppuswamy N (2023) *AI and Threat Intelligence: Staying Ahead of Cyber Threats*, RTInsights website, accessed 24 January 2024. https://www.rtinsights.com/ai-and-threat-intelligence-staying-ahead-of-evolving-cyber-threats/

Leslie D (2019) Understanding artificial intelligence ethics and safety. *arXiv preprint arXiv:1906.05684*, accessed 23 January 2024.

Lim CK (2022) *Singapore: Privacy*, Global Data Review website, accessed 24 January 2024. https://globaldatareview.com/insight/handbook/2023/article/singapore-privacy#:~:text=The%20Personal%20Data%20Protection%20Act%202012%20%28PDPA%29%20is,individuals%E2%80%99%20personal%20data%20by%20all%20private%20sector%20organisations.

Lui B, Ng V, Ng G and HIRSCH WR (2022), *SINGAPORE PERSONAL DATA PROTECTION ACT CHANGES HAVE IMPLICATIONS FOR HEALTHCARE SECTOR*, Morgan Lewis website, accessed 25 January 2024. https://www.morganlewis.com/pubs/2022/08/singapore-personal-data-protection-act-changes-have-implications-for-healthcare-sector

Malamateniou, C., Knapp, K.M., Pergola, M., Woznitza, N. and Hardy, M., 2021. Artificial intelligence in radiography: where are we now and what does the future hold?. *Radiography*, *27*, pp.S58-S62, accessed 23 January 2024.

Mallick CB (2022) *Top 10 Endpoint Detection and Response Tools in 2022*, Spiceworks website, accessed 26 January 2024. https://www.spiceworks.com/it-security/endpoint-security/articles/best-edr-tools/

Mallick CB (2022) *Top 10 Intrusion Detection and Prevention System Software in 2022* , Spiceworks website, accessed 26 January 2024. https://www.spiceworks.com/it-security/vulnerability-management/articles/best-idps-software/

Marr B (2017) *Data strategy: how to profit from a world of big data, analytics and the internet of things*, Kogan Page, London.

Miller J (2021) *THE COST OF CYBERSECURITY AND CREATING AN ACHIEVABLE SECURITY BUDGET*, ByLift website, accessed 25 January 2024. https://www.bitlyft.com/resources/the-cost-of-cybersecurity-and-creating-an-achievable-security-budget

Ministry Of Health (MOH) (n.d.) *Health Manpower Development Plan (HMDP) - Visiting Experts*, moh.gov.sg, accessed 23 January 2024.

Perdana, A. and Mokhtar, I.A., 2023. Leveraging digital technologies for information technology-enabled healthcare transformation at SingHealth. *Journal of Information Technology Teaching Cases*, *13*(1), pp.97-103. Accessed 17 Jan. 2024.

Pitchkites M and Leavitt J (2024) *Top Cyber Security Statistics, Facts & Trends in 2024*, Cloudwards website, accessed 25 January 2024. https://www.cloudwards.net/cyber-security-statistics/

Rani T (2022) *Transforming healthcare with artificial intelligence*, SingHealth website, accessed 22 January 2024. https://www.singhealth.com.sg/news/singapore-health/transforming-healthcare-with-artificial-intelligence

Ruefle R, Dorofee A, Mundie D, Householder AD, Murray M. and Perl SJ, (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy*, *12*(5), pp.16-26, accessed 23 January 2024.

Salesforce (2021) *Artificial intelligence (AI) readiness index score of Singapore in 2021, by sector*, Statista website, accessed 25 January 2024. https://www.statista.com/statistics/1298923/singapore-ai-readiness-by-sector/

SBR (Singapore Business Review) (2020) *More than half of Singaporeans worried about data privacy: report*, sbr.com.sg, accessed 25 January 2024. https://sbr.com.sg/information-technology/news/more-half-singaporeans-worried-about-data-privacy-report

Segal D (2020) *The Impact of AI on Cybersecurity*, IEEE Computer Society website, accessed 26 January 2024. https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity

Selvadurai N, and Matulionyte R (2020) Reconsidering creativity: copyright protection for works generated using artificial intelligence. *Journal of Intellectual Property Law & Practice*, *15*(7), pp.536-543, accessed 23 January 2024.

SingHealth (2022) *SingHealth Duke-NUS Academic Medical Centre Annual Report 2021/2022*, SingHealth website, accessed 23 January 2024. https://www.singhealth.com.sg/about-singhealth/newsroom/Pages/annual-reports.aspx

SingHealth (2023) *Vision & Mission*, SingHealth website, accessed 23 January 2024. https://www.singhealth.com.sg/rhs/about-us/vision-mission

SingHealth (n.d.a) *History of our acute hospitals*, SingHealth website, accessed 23 January 2024. https://www.singhealth.com.sg/about-singhealth/newsroom/medsg200/acute-hospital-history

SingHealth (n.d.b) *Personal Data Protection Act (PDPA)*, SingHealth website, accessed 23 January 2024. https://www.singhealth.com.sg/pdpa

Sjouwerman S (2024) *Google Finds an Alarming Thousands of Phishing Sites Everyday in 2020*, KnowBe4 website, accessed 26 January 2024. https://blog.knowbe4.com/google-finds-an-alarming-thousands-of-phishing-sites-everyday-in-2020#:~:text=Google%20discovered%20a%20record%20number%20of%20phishing%20sites,the%201.69%20million%20phishing%20sites%20discovered%20in%202019.

Smart Nation (n.d.) *National AI Strategy - AI for the Public Good, for Singapore and the World*, smartnation.gov.sg, accessed 25 January 2024. https://www.smartnation.gov.sg/nais/

Synapxe (n.d) *ABOUT HEALTHCARE CLOUD (H-CLOUD),* Synapxe website, accessed 23 January 2024. https://www.synapxe.sg/healthtech/cloud/h-cloud/

Synapxe (n.d) *ABOUT NATIONAL ELECTRONIC HEALTH RECORD (NEHR),* Synapxe website, accessed 23 January 2024. https://www.synapxe.sg/healthtech/national-programmes/national-electronic-health-record-nehr/#NEHR-at-a-glance

Tan CC, Lam CSP, Matchar DB, Zee YK and Wong JEL (2021) 'Singapore's health-care system: key features, challenges, and shifts', *The Lancet*, 398(10305):1091-1104. https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)00252-X/fulltext

TensorFlow (n.d) *Why TensorFlow*, TensorFlow website, accessed 25 January 2024. https://www.tensorflow.org/about

Teo ZL, Kwee A, Lim JC, Lam CS, Ho D, Maurer-Stroh S, Wong TY and Chua R, (2023) Artificial intelligence innovation in healthcare: Relevance of reporting guidelines for clinical translation from bench to bedside. *Call for Papers*, *52*(4), pp.199-212, accessed 23 January 2024.

Tham I (20 July 2018) 'Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber-attack', *The Straits Times*, accessed 23 January 2024. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

The World Bank (n.d.) *Current health expenditure per capita (current US$) - Singapore*, *data.worldbank.org, accessed 25 January 2024.* https://data.worldbank.org/indicator/SH.XPD.CHEX.PC.CD?locations=SG

Toh J (2022) *From Paper to Digital*, SingHealth website, accessed 22 January 2024. https://www.singhealth.com.sg/news/stories-from-the-heart/from-paper-to-digital#:~:text=HIMS%20began%20the%20daunting%20task%20of%20going%20paperless,all%20new%20patients%20records%20were%20by%20default%2C%20digital.

Tomorrow's Medicine (2021) *A partnership for Singapore's healthcare towards becoming a Silicon Valley of the East*, SingHeallth website, accessed 22 January 2024. https://www.singhealth.com.sg/news/tomorrows-medicine/a-partnership-towards-becoming-a-silicon-valley-of-the-east

Utilities One (2023) *The Role of Security Information and Event Management SIEM in Network Security Management*, Utilities One, accessed 26 January 2024. https://utilitiesone.com/the-role-of-security-information-and-event-management-siem-in-network-security-management

Vectra (n.d.) *Mastering Threat Detection in Cybersecurity*, Vectra website, accessed 24 January 2024. https://www.vectra.ai/topics/threat-detection

Wetsman N, Dwyer D and Herndon S (2023), *Cyberattacks on hospitals are growing threats to patient safety, experts say*, ABC News, 10 May, accessed 23 January 2024. https://abcnews.go.com/Health/cyberattacks-hospitals-growing-threats-patient-safety-experts/story?id=99115898

Witzsche M (12 June 2023) 'The Challenge and Ethical Considerations of AI and ML in Cybersecurity [Part 2]', [LinkedIn post], Witzsche M, accessed 24 January 2024. https://www.linkedin.com/pulse/challenges-ethical-considerations-ai-ml-cybersecurity-witzsche/

Xiarch Solutions (3 August 2023) 'AI-Driven Threat Hunting: Enhancing Cyber Security through Intelligent Detection' [LinkedIn post], Xiarch Solutions, accessed 24 January 2024. https://www.linkedin.com/pulse/ai-driven-threat-hunting-enhancing-cyber-security-through-intelligent/

CONTRIBUTION SUMMARY

NAME	STUDENT ID	% CONTRIBUTION	SIGNATURE
Le Dieu Ha	s3979364	100%	Ha
Ngo Phuc Thinh	s3990389	100%	Thinh
Nguyen Tri Thuc	s2939515	100%	Thuc
Bui Thi Kim Thuy	s3903720	100%	Thuy
Nguyen Thuy Truc	s3972621	100%	Truc