Strategic Project Management
COMP8790

Assignment 1: Strategic Digital Transformation Project Report

Jhanvi Vasudev Thakkar

48214159

Contents

INTRODUCTON

This report offers a strategic assessment of two digital transformation projects for Westmead Hospital: (1) a cybersecurity improvement program intended to fix vulnerabilities after a recent ransomware attack, and (2) an AI-based patient flow management system intended to shorten lengthy ED lines. Both programs have the potential to enhance operational effectiveness and protect patient outcomes, especially considering Westmead's status as a significant public teaching hospital within the Western Sydney Local Health District. Key strategic project management tools, such as SWOT analysis, ROI, Net Present Value (NPV), Cost-Benefit Analysis (CBA), and a thorough risk assessment, are used in the research to evaluate these projects. The outcomes offer evidence-based recommendations for choosing the program that provides the most value and is in line with Westmead Hospital's strategic goals.

ORGANIZATION BACKGROUND:

Westmead Hospital is a prominent public teaching hospital in Sydney that is managed by the Western Sydney Local Health District. The University of Sydney is associated with it, and it serves more than 1.5 million citizens. The hospital is one of the biggest hospital campuses in the Southern Hemisphere and offers a range of area of expertise medical services, including as intensive care, trauma, emergency, and cancer (NSW Health, 2024). It is a leader in healthcare innovation because of its central position as a hub for research and teaching.

In 2024, staff members publicly complained about patients with emergency departments who had to wait more than 41 hours for a room, calling the situation "unsafe" and demanding action (Sky News Australia, 2024). Staff, frontline operators, and the length of therapy that follows are all significantly impacted by the overcrowding situation.
One cyberattack at the beginning of 2024 claimed to have access to private patient data at the Crown Princess Mary Cancer Centre in Westmead (Yahoo News AU, 2024). This example demonstrated the vulnerability of the public health system to cyberattacks and revealed the shortcomings of the cybersecurity architecture.

These challenges, like other extreme system barriers, create a tactical necessity.

Addressing these challenges necessitates a strategic digital transformation to enhance operational efficiency and safeguard patient information. Implementing advanced technologies can streamline patient flow, reduce waiting times, and fortify cybersecurity measures, aligning with the hospital's commitment to providing high-quality healthcare services.

Initiative Overview

To tackle the identified challenges, two digital transformation initiatives are proposed:

1. **AI-Driven Patient Flow Management System**: Deploying artificial intelligence to optimize patient triage and bed allocation processes can significantly reduce waiting times in the Emergency Department. AI algorithms can predict patient admission rates and streamline resource allocation, improving overall patient care.

2. **Enhanced Cybersecurity Infrastructure**: Upgrading the hospital's cybersecurity framework, including implementing advanced threat detection systems and staff training programs, will protect sensitive patient data and ensure compliance with healthcare data protection regulations.

FEASIBILITY & STRATEGIC EVALUATION

AI driven patient flow management system

SWOT Analysis

STRENGTHS	WEAKNESS
• Reduced waiting times • Improved Resource efficiency • Scalable Solution • Better Patient Experience	• High Initial Cost • Staff skill gap • Data dependency • Integration Complexity
OPPORTUNITES	THREATS
• Future expansion • Predictive care pathways • Operational cost savings	• Cybersecurity threats • Ethical considerations • System downtime risks • Regulatory Challenges

An AI-powered patient flow management system is a based-on data approach to Westmead Hospital's operational issues, including overcrowding in the emergency department and delays of more than 41 hours, reported by Sky News Hospital. AI may greatly cut wait times, increase resource efficiency, and improve the satisfaction of patients by real-time optimizing priority, bed distribution, and personnel deployment.

But, the success of the project depends on solving key weaknesses, including need for AI using skills and adoption of AI by hospital personnels. Also, integration issues with the present system can be a challenge.

The opportunities of the project are very significant. Westmead hospital is a major public teaching institute, they can further continue AI research and training mission in association with University of Sydney. Scaling to other hospitals in the Western Sydney LHD is possible with the correct approach.

Threats like security vulnerabilities (particularly in considering Westmead's recent ransomware attack on their cancer unit-5】) and governmental hurdles must be carefully addressed despite the project's ability to succeed and comply to Australian privacy regulations and NSW Health.

Risk Assessment

There can be both technical like model failure and organizational like adoption resistance risks in deploying an AI system.

Following are the possible risks and their mitigation strategies

ID	RISK DESCRIPTION	MITIGATION STRATGIES
R1	Cyber security breach/ ransomware attack	Implementing a 14/7 monitoring endpoint protection
R2	AI model inaccuracy	Use wide training data, conduct regular audits
R3	Integration Failure	Conduct phased pilots, involve westmead hospital's IT team
R4	Adoption resistance	Early stakeholder engagement, training programs
R5	Legal non-compliance with patient data laws	Involve legal/privacy teams early
R6	Operational cost overruns	Include 15% contingency buffer in budget
R7	Tech failure	Design & maintain high availability and maintain 25/7 tech support
R8	Data quality issues affecting AI accuracy	Pre-clean & validate data sets
R9	Misalignment with clinical workflows	Co-design interfaces and use iterative feedback

RISK MATRIX

Likelihood/impact	Low Impact	Medium Impact	High Impact
High Likelihood		R6	R4
Medium Likelihood		R8	R1,R3
Low likelihood	R2,R7	R5	

An extensive risk analysis was done for the AI-based patient flow system of Westmead Hospital. A standard 3x3 matrix was utilized to classify the risks on their likelihood and impact. Cyber-attack (R1), issues in integrating existing EMR systems (R3), and resistance to change from clinical staff (R4) are high-priority risks. Because they tend to disrupt hospital processes, these are put into high-risk categories.

Mitigation measures have been put in place, including phased trials of integration, timely employee participation through co-designing and training, and the incorporation of strong cybersecurity. Taking this proactive approach ensures the project is well-equipped to face organizational and technological issues.

Cost Benefit Analysis

	A	B	C	D	E	F	G	H	I
1									
2	DEVELOPMENT COSTS								
3	PERSONNEL								
4									
5	2	Business Analyst (600 hours/ea @ $70/hr)					$84,000.00		
6	3	AI / Data specialist (500 hours/ea @$100/hr)					$1,50,000.00		
7	4	Software developer (400 hours/ea @ $75/hr)					$1,20,000.00		
8	2	Integration specialist (300 hours/ea @$85/hr)					$51,000.00		
9	2	Testing specialist (200 hours/ea @ $65/hr)					$26,000.00		
10	1	Training specialist (160 hours/ea @ $60/hr)					$9,600.00		
11	1	Project manager (800 hours/ea @$80/hr)					$64,000.00		
12	1	System Administrator (200 hours/ea @$75/hr)					$15,000.00		
13		Total personnel costs					$5,19,600.00		
14									
15	EXPENSES								
16		Specialist training					$30,000.00		
17									
18	NEW HARDWARE & SOFTWARE								
19		Servers					$3,00,000.00		
20		Integration with exsisting system					$2,00,000.00		
21		Data Migration					$1,00,000.00		
22		AI Software development/Licensing					$10,00,000.00		
23		Mobile app development					$2,00,000.00		
24									
25		Total					$18,00,000.00		
26									
27		TOTAL DEVELOPMENT COSTS					$23,49,600.00		
28									

28			
29	ANNUAL OPERATING COSTS:		
30	PERSONNEL		
31		System administrator	$1,20,000.00
32		AI model maintenance	$60,000.00
33			
34	SOFTWARE & LISCENSES		
35		Software maintenance and support	$1,00,000.00
36		Cloud hosting	$70,000.00
37			
38	HARDWARE		
39		Hardware maintenance	$30,000.00
40			
41	OTHER COSTS		
42		Electricity & cooling	$50,000.00
43		Network/Internet costs	$40,000.00
44			
45		TOTAL ANNUAL OPERATING COSTS	$4,70,000.00

	A	B	C	D	E	F	G	H	I
1									
2			accumulated		accumulated	Payback period			
3	year	costs	costs	benefits	benefits				
4	0	$23,49,600.00	$23,49,600.00	$0.00	$0.00	-$23,49,600.00			
5	1	$4,70,000.00	$28,19,600.00	$7,00,000.00	$7,00,000.00	-$21,19,600.00			
6	2	$15,000.00	$28,34,600.00	$8,00,000.00	$15,00,000.00	-$13,34,600.00			
7	3	$20,000.00	$28,54,600.00	$9,00,000.00	$24,00,000.00	-$4,54,600.00			
8	4	**$20,000.00**	**$28,74,600.00**	**$10,00,000.00**	**$34,00,000.00**	**$5,25,400.00**	Break even point		
9	5	$22,000.00	$28,96,600.00	$11,00,000.00	$45,00,000.00	$16,03,400.00			
10	6	$25,000.00	$29,21,600.00	$12,00,000.00	$57,00,000.00	$27,78,400.00			
11									
12									
13									
14									

Point of Break-Even:

The Payback Period is positive by $70,800 in Year 4 because the Accumulated Benefits ($3,400,000) surpass the Accumulated Costs ($24,00,000). This suggests that the project reaches a break-even point in the fourth year.

The payback period for Westmead Hospital's AI-powered patient queue management system is anticipated to be four years based on these cost and benefit estimates.

	A	B	C	D	E	F	G	H	I	J	K
1		Year 0	1	2	3	4	5	6			
2	Benefits		$7,00,000.00	$8,00,000.00	$9,00,000.00	$10,00,000.00	$1,10,000.00	$1,20,000.00			
3	Factor(8%)	1	0.925925926	0.85733882	0.793832241	0.735029853	0.680583197	0.63016963			
4	Present Value		$6,48,148.15	$6,85,871.06	$7,14,449.02	$7,35,029.85	$74,864.15	$75,620.36	$29,33,982.58		
5	Dev Costs	$23,49,600.00									
6	Ongoing Costs		$4,70,000.00	$15,000.00	$20,000.00	$20,000.00	$22,000.00	$25,000.00			
7	Factor(8%)	1	0.925925926	0.85733882	0.793832241	0.735029853	0.680583197	0.63016963			
8	Present Value	$23,49,600.00	$4,35,185.19	$12,860.08	$15,876.64	$14,700.60	$14,972.83	$15,754.24	$28,58,949.58		
9	Net Present Value	-$23,49,600.00	$2,12,962.96	$6,73,010.97	$6,98,572.37	$7,20,329.26	$59,891.32	$59,866.11	$75,033.00		
10	Cumulative NPV	-$23,49,600.00	-$21,36,637.04	-$14,63,626.06	-$7,65,053.69	-$44,724.44	$15,166.89	$75,033.00			
11											
12	NPV=	$75,033.00									
13											
14	Payback period	4.746759869									
15											
16	ROI	262.45%									
17											
18											
19											
20											
21											
22											
23											

To determine the economic feasibility of the AI-powered patient queue management system deployed at Westmead Hospital, in combination with the relative stability of Australia's healthcare industry, along with the appropriate accounting for project risks and opportunity costs—which demonstrates the time value of money—I used the Net Present Value (NPV) method using an 8% discounting rate.

The total net present value (NPV) of the project, as computed by using an 8% discount rate for six years, is $75,033.

A positive NPV indicates that the project will be financially viable, with the present value of the future benefits exceeding the present value of its cost. This indicates that the artificial intelligence system is a potentially high expenditure for Westmead Hospital, which is expected to have a positive net financial benefit over its working life, based on the time value of money and the given discount rate. Additional sensitivity testing with various discount rates would also be advisable with respect to assessing how robust this result is.

An ROI of approximately 262.45% over the six-year period suggests that for every dollar invested in the AI-powered patient queue management system, Westmead Hospital is projected to generate a return of about 262.45% above the initial investment. This indicates a fairly a profitable investment.

Work breakdown structure (WBS)

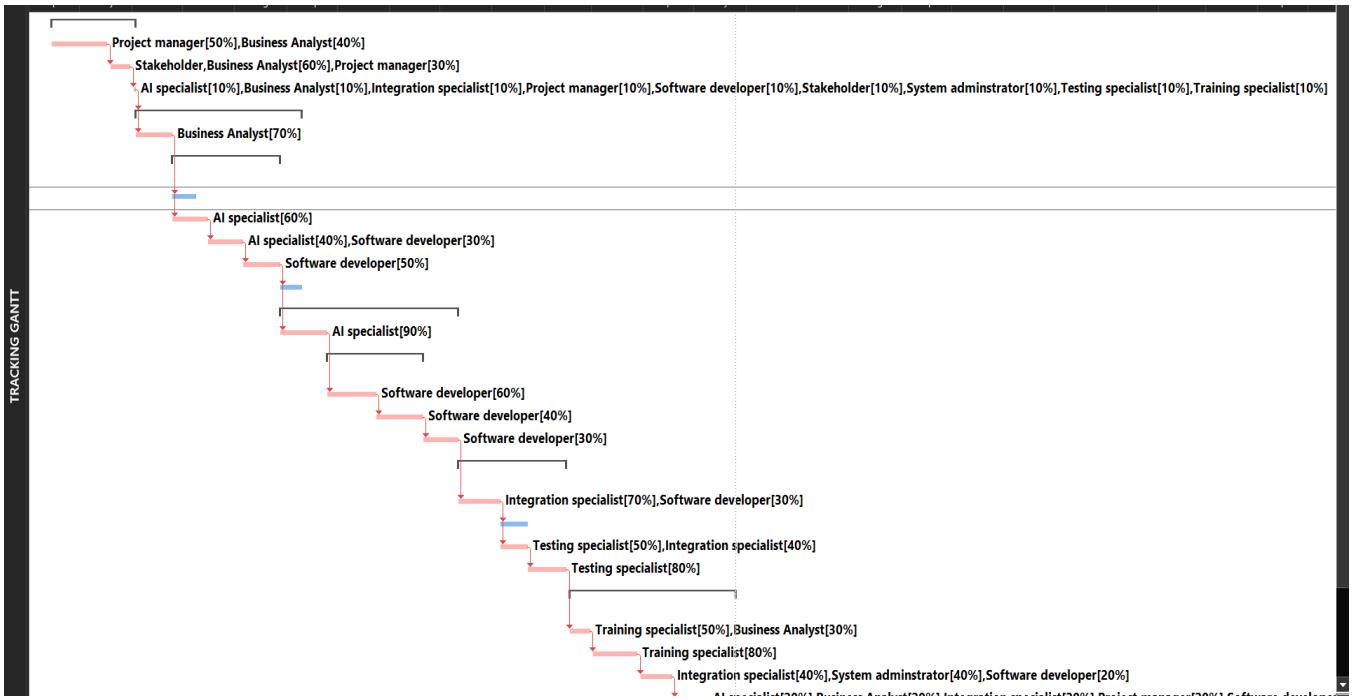
TRACKING GANTT

	ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	**1**		**Project initiation**	**36 days**	**Mon 14-04-25**	**Mon 02-06-25**		
2	2		Project Charter develc	25 days	Mon 14-04-25	Fri 16-05-25		Project manager[5
3	3		Stakeholders analysis	10 days	Mon 19-05-25	Fri 30-05-25	2	Stakeholder,Busine
4	4		Project kick-off meeti	1 day	Mon 02-06-25	Mon 02-06-25	3	AI specialist[10%],
5	**5**		**Requirements Analysis**	**71 days**	**Tue 03-06-25**	**Tue 09-09-25**	**4**	
6	6		Current System Analys	16 days	Tue 03-06-25	Tue 24-06-25	4	Business Analyst[7
7	**7**		**Functional requirements**	**46 days**	**Wed 25-06-25**	**Wed 27-08-25**		
8	8		Patient Check-in	10 days	Wed 25-06-25	Tue 08-07-25	6	Business Analyst[3
9	9		Queue Managemen	15 days	Wed 25-06-25	Tue 15-07-25	6	AI specialist[60%]
10	10		Appointment Sched	15 days	Wed 16-07-25	Tue 05-08-25	9	AI specialist[40%],
11	11		Mobile Integration	16 days	Wed 06-08-25	Wed 27-08-25	10	Software develope
12	12		Non - Functional requi	9 days	Thu 28-08-25	Tue 09-09-25	11	Business Analyst[3
13	**13**		**AI Model development**	**76 days**	**Thu 28-08-25**	**Thu 11-12-25**		
14	14		Algorithm design and t	20 days	Thu 28-08-25	Wed 24-09-25	11	AI specialist[90%]
15	**15**		**Software development**	**41 days**	**Thu 25-09-25**	**Thu 20-11-25**		
16	16		Core Application	21 days	Thu 25-09-25	Thu 23-10-25	14	Software develope
17	17		Mobile Application	20 days	Fri 24-10-25	Thu 20-11-25	16	Software develope
18	18		Database developmer	15 days	Fri 21-11-25	Thu 11-12-25	17	Software develope
19	**19**		**System Integration and testing**	**39 days**	**Fri 12-12-25**	**Fri 13-02-26**		
20	20		System Integration	10 days	Fri 12-12-25	Mon 05-01-26	18	Integration special
21	21		Unit testing	12 days	Tue 06-01-26	Wed 21-01-26	20	Software develope
22	22		Integration testing	12 days	Tue 06-01-26	Wed 21-01-26	20	Testing specialist[5
23	23		System testing	17 days	Thu 22-01-26	Fri 13-02-26	22	Testing specialist[8
24	**24**		**Training and**	**71 days**	**Mon**	**Mon**		

	ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
24	**24**		**Training and deployment**	**71 days**	**Mon 16-02-26**	**Mon 25-05-26**		
25	25		Training Material deve	10 days	Mon 16-02-26	Fri 27-02-26	23	Training specialist[
26	26		Staff training	20 days	Mon 02-03-26	Fri 27-03-26	25	Training specialist[
27	27		System deployment	15 days	Mon 30-03-26	Fri 17-04-26	26	Integration special
28	28		So-Live support	15 days	Fri 17-04-26	Fri 08-05-26	27	AI specialist[20%],
29	**29**		**Project Closure**	**11 days**	**Mon 11-05-26**	**Mon 25-05-26**		
30	30		Project documentat	6 days	Mon 11-05-26	Mon 18-05-26	28	Business Analyst[4
31	31		Project review	5 days	Tue 19-05-26	Mon 25-05-26	30	AI specialist[10%],

The stages to deliver the AI-powered Patient Queue Management System are outlined in this WBS. Phases like software development and AI model development are used to create important deliverables. Starting with the fundamental Project Initiation and Requirements Analysis, the framework guarantees quality via System Integration and Testing and effective adoption through Training and Deployment.

Gantt Chart




Qtr 2, 2026
Qtr 3, 2026
Qtr 4, 2026
Qtr 1, 2027
Qtr 2, 2027
Qtr 3, 2027
Qtr 4, 2027
Qtr 1, 2028
Qtr 2, 2028
Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr
specialist[50%],Business Analyst[30%]
Training specialist[80%]
Integration specialist[40%],System adminstrator[40%],Software developer[20%]
AI specialist[20%],Business Analyst[20%],Integration specialist[20%],Project manager[20%],Software developer[20%],Stakeholder[20%],System adminstrator[50%],Testing specialist[20%],Training specialist[20%]
Business Analyst[40%],Project manager[40%]
AI specialist[10%],Business Analyst[10%],Integration specialist[10%],Project manager[20%],Software developer[10%],Stakeholder[10%],System adminstrator[10%],Testing specialist[10%],Training specialist[10%]

Cyber Security Enhancements

SWOT Analysis

STRENGTHS	WEAKNESS
• Robust security updates • Improved system integrity builds stakeholders & patient trust • Enhances compliance with health data regulations • Support hospital wide digitisation & future scalability • Very short payback period	• High initial cost • Possible downtime or workflow interruptions while system transition • Staff training needs may increase • Dependence on external vendors or consultants
OPPORTUNITES	THREATS
• Government grants & cybersecurity fundings • Integration of other smart healthcare innovations (IoT) • Positioning Westmead Hospital as a digital leader in healthcare	• Risk of reputational damage if enhancements are ineffective or fail post-deployment • Non-compliance fines if system still fails to meet regulations • Human errors

Strengths: Westmead becomes future-ready by improving cybersecurity, which increases protection, compliance, and trust.

Weaknesses: Expensive expenses and implementation difficulties could put a strain on resources and need team members change.

Possibilities: The project permits integration with state-of-the-art health technology and is in line with government goals.

Threats: Persistent and developing threats, combined with regulatory pressure and human mistake, are issues.

Risk Assessment

Risk ID	RISK	MITIGATION STRATEGIES
R1	System downtime during implementation	Schedule upgrades during off-peak hours
R2	Insider threats (staff negligence or misuse)	Regular cybersecurity awareness
R3	Cyberattack	Run regular penetration testing
R4	Non-compliance with healthcare data regulation	Conduct routine audits
R5	Resistance to change by staff	Involve staff early, use feedback
R6	Overdependence on third party	Choose vendors
R7	Budget Overruns	Maintain contingency budget

This risk matrix helps to prioritize what could go wrong during or after adopting cyber upgrades. Even though ransomware and staff carelessness are frequent worries, the hospital may be safe and functional during the update by prepping for staff training, secure contracting with suppliers, and system backups.

Impact/ Likelihood	Low	Medium	High
High	R4	R1, R2	R3
Medium	R6	R5, R7	
Low			

The risk matrix assists in prioritising risks according to their impact and likelihood. Through worker training and multilayer protection, high-risk problems like ransomware and insider threats are controlled. Scheduling, change management, and communication are used to mitigate medium risks, such system outages and change aversion, and guarantee the safe and seamless implementation of cyber upgrades.

Cost benefit Analysis

The total development cost for the cybersecurity project is **$4,02,000**, covering personnel, hardware, software, and professional services. Key areas include:

- **Personnel ($1,14,100):** Skilled professionals including analysts, engineers, and managers for system design and implementation.
- **Hardware ($1,30,000):** Firewalls, secure servers, network equipment, and backups for secure infrastructure.

- **Software & Licensing ($82,000/year):** Tools for endpoint protection, SIEM, MFA, password management, backup, and email security.
- **Professional Services ($1,90,000):** Includes audits, penetration testing, MSSP, and staff training. **MSSP (Managed Security Service Provider)** includes 24/7 threat monitoring, Alert triage and incident escalation, Basic patch management support, Regular reporting, Security configuration checks

Annual ongoing costs total **$2,31,500**, primarily for licensing, MSSP support, training, and incident response readiness. This investment ensures a robust, secure, and compliant cybersecurity framework

	A	B	C	D	E	F	G	H	I
1									
2	Development costs								
3	personnel								
4	2	Cybersecurity analysts 400hours/ea@ $50/hr						$40,000.00	
5	2	IT Supprt technicians 300hours/ea@ $40/hr						$24,000.00	
6	1	Cybersecurity Project Manager 200 hours/ea@$80/hr						$16,000.00	
7	1	System Architect 150 hours/ea @$60/hr						$9,000.00	
8	1	Penetration Tester 100 hours @$70/hr						$7,000.00	
9	1	Network Security engineer 120 hours @$55/hr						$6,600.00	
10	1	Training Specialist 100 hours@ $45/hr						$4,500.00	
11	1	Compliance officer 80 hours@ $50/hr						$4,000.00	
12	1	Documentation Specialist 100 hours @$30/hr						$3,000.00	
13									
14		Total personnel cost						$1,14,100.00	
15									
16									
17	Hardware								
18									
19	qty	item			description			cost	
20	3	Enterprise firewalls			with intrusion prevention			$45,000.00	
21	5	Secure servers			for hosting SIEM,EDR			$50,000.00	
22	10	Network switches & routers			secure nw infrastricture			$20,000.00	
23	2	backup appliances			encrypted backups			$10,000.00	
24		Cabling & installation costs			nw & data centre wiring setup			$5,000.00	
25									
26					Total Hardware cost			$1,30,000.00	
27									

	A	B	C	D	E	F	G	H
27								
28	Software & licensing							
29								cost per year
30	Endpoint detection & response (EDR)				eg: CrowdStrike			$18,000.00
31	SIEM Platform				eg:Azure sentinel			$30,000.00
32	MFA				eg: Microsoft Authenticator			$5,000.00
33	Password Vault				eg: CyberArk			$10,000.00
34	Backup & recovery tools				eg:Cloud			$12,000.00
35	Email Security				eg:Anti-phising			$7,000.00
36								
37					Total software cost/year:			$82,000.00
38								
39	Professional services & support							
40								
41	Security Audit & risk Assessment							$25,000.00
42	Penetration Testing							$20,000.00
43	Compliance & Policy Consulting							$15,000.00
44	Managed Security Services Provider(MSSP)							$1,20,000.00
45	Staff cybersecurity training							$10,000.00
46								
47					Total services cost:			$1,90,000.00
48								
49								
50				Total development cost:				$4,02,000.00
51								

	A	B	C	D	E	F	G	H	I	J
51										
52										
53	Annual Ongoing Costs:									
54										
55	Software & liscensing							$82,000.00		
56	Maintenance & support provider(MSSP)							$1,20,000.00		
57	Training							$12,500.00		
58	Contingency & IR Support							$17,000.00		
59										
60				Total Annual cost				$2,31,500.00		
61										
62										
63										
64										
65										

	A	B	C	D	E	F	G	H
1								
2			Accumulated		Accumulated	Payback		
3	Year	Costs	Costs	Benefits	benefits	period		
4	0	$4,02,000.00	$4,02,000.00	$0.00	$0.00	-$4,02,000.00		
5	1	$2,31,500.00	$6,33,500.00	$16,80,000.00	$16,80,000.00	**$10,46,500.00**	Break Even point	
6	2	$2,20,000.00	$8,53,500.00	$31,30,000.00	$48,10,000.00	$39,56,500.00		
7	3	$2,46,500.00	$11,00,000.00	$36,00,000.00	$84,10,000.00	$73,10,000.00		
8	4	$2,19,000.00	$13,19,000.00	$40,60,000.00	$1,24,70,000.00	$1,11,51,000.00		
9	5	$2,35,500.00	$15,54,500.00	$41,20,000.00	$1,65,90,000.00	$1,50,35,500.00		
10	6	$2,00,000.00	$17,54,500.00	$41,20,000.00	$2,07,10,000.00	$1,89,55,500.00		
11								
12								
13								

Break-even point

The cybersecurity initiative requires a $402,000 initial expenditure, with subsequent yearly costs ranging from $200,000 to $246,500. In Year 1 alone, the benefits exceed the costs by $1.05 million. By Year 6, these benefits, when combined with the $1.755 million invested, total $2.07 million. The ROI, quick return, and strategic value of the initiative all attest to its substantial worth.

	A	B	C	D	E	F	G	H	I	J
1		Year0	1	2	3	4	5	6		
2	Benefits		$16,80,000.00	$31,30,000.00	$36,00,000.00	$40,60,000.00	$41,20,000.00	$41,20,000.00		
3	Factor(7%)	1	0.934579439	0.873438728	0.816297877	0.762895212	0.712986179	0.666342224		
4	Present Value		$15,70,093.46	$27,33,863.22	$29,38,672.36	$30,97,354.56	$29,37,503.06	$27,45,329.96	$1,60,22,816.62	
5	Dev Costs	$4,02,000.00								
6	Ongoing Costs		$2,31,500.00	$2,20,000.00	$2,46,500.00	$2,19,000.00	$2,35,500.00	$2,00,000.00		
7	Factor(7%)	$1.00	0.934579439	0.873438728	0.816297877	0.762895212	0.712986179	0.666342224		
8	Present Value	$4,02,000.00	$2,16,355.14	$1,92,156.52	$2,01,217.43	$1,67,074.05	$1,67,908.25	$1,33,268.44	$14,79,979.83	
9	Net Present Value	-$4,02,000.00	$13,53,738.32	$25,41,706.70	$27,37,454.93	$29,30,280.51	$27,69,594.81	$26,12,061.52	$1,45,42,836.79	
10	Cumulative NPV	-$4,02,000.00	$9,51,738.32	$34,93,445.02	$62,30,899.95	$91,61,180.46	$1,19,30,775.27	$1,45,42,836.79		
11										
12	NPV	$1,45,42,836.79								
13										
14	Payback Period	0.30	3 months							
15										
16	ROI	98263.75%								
17										
18										

This financial study uses a 7% discount rate to assess the cybersecurity investment over a six-year period.
The project's overall net present value (NPV) of $1,45,42,837 shows significant long-term value generation and good financial viability.
The $4,02,000 initial expenditure is fully recouped in 0.30 years, or roughly 3.5 months, demonstrating quick cost recovery.
Return on Investment (ROI): An impressive ROI of 98,263.75% demonstrates significant cost-effectiveness due to high predicted benefits and optimised operational spending.

According to this analysis, the cybersecurity project is not only strategically important but also financially attractive, providing exceptional long-term profits and a quick recovery.

Work Breakdown Structure (WBS)

TRACKING GANTT

	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names	Add New Co
1		**Planning & Assessment**	**58 days**	**Mon 14-04-25**	**Wed 02-07-25**			
2		**Project initiation & kick off**	**9 days**	**Mon 14-04-25**	**Thu 24-04-25**			
3		Organize Kickoff Me	2 days	Mon 14-04-25	Tue 15-04-25		Cybersecurity Proj	
4		Define Project Char	7 days	Wed 16-04-25	Thu 24-04-25	3	Cybersecurity Proj	
5		**Risk & Vulnerability Assessment**	**29 days**	**Fri 25-04-25**	**Wed 04-06-25**			
6		Review exsisting inf	10 days	Fri 25-04-25	Thu 08-05-25	4	Cybersecurity anal	
7		Conduct Threat Ana	14 days	Fri 09-05-25	Wed 28-05-25	6	Compliance office	
8		Prepare Risk assess	5 days	Thu 29-05-25	Wed 04-06-25	7	Cybersecurity anal	
9		**Finalize requirements & KPI**	**20 days**	**Thu 05-06-25**	**Wed 02-07-25**			
10		Define KPIs & succe	6 days	Thu 05-06-25	Thu 12-06-25	8	System architect[4	
11		Obtain stakeholder	14 days	Fri 13-06-25	Wed 02-07-25	10	Cybersecurity Proj	
12		**Design & procurement**	**16 days**	**Thu 03-07-25**	**Thu 24-07-25**			
13		**Cybersecurity Architecture Design**	**15 days**	**Thu 03-07-25**	**Wed 23-07-25**			
14		Design zero trust ar	10 days	Thu 03-07-25	Wed 16-07-25	11	System architect[8	
15		Develop Access co	5 days	Thu 17-07-25	Wed 23-07-25	14	Cybersecurity anal	
16		**Vendor evaluation & Procurement**	**16 days**	**Thu 03-07-25**	**Thu 24-07-25**			
17		Prepare Request for	3 days	Thu 03-07-25	Mon 07-07-25	11	Cybersecurity Proj	
18		Evaluate & select ve	7 days	Tue 08-07-25	Wed 16-07-25	17	Cybersecurity Proj	
19		Finalize contracts &	6 days	Thu 17-07-25	Thu 24-07-25	18	Cybersecurity Proj	
20		**Implementation**	**62 days**	**Thu 24-07-25**	**Fri 17-10-25**			
21		**Hardware Installation**	**40 days**	**Fri 25-07-25**	**Thu 18-09-25**			
22		Installl enterprise fir	30 days	Fri 25-07-25	Thu 04-09-25	19	IT Support staff[40	
23		Setup Backup Applia	10 days	Fri 05-09-25	Thu 18-09-25	22	IT Support staff[40	
24		**Software deployment & Configuration**	**31 days**	**Fri 05-09-25**	**Fri 17-10-25**	**22**		

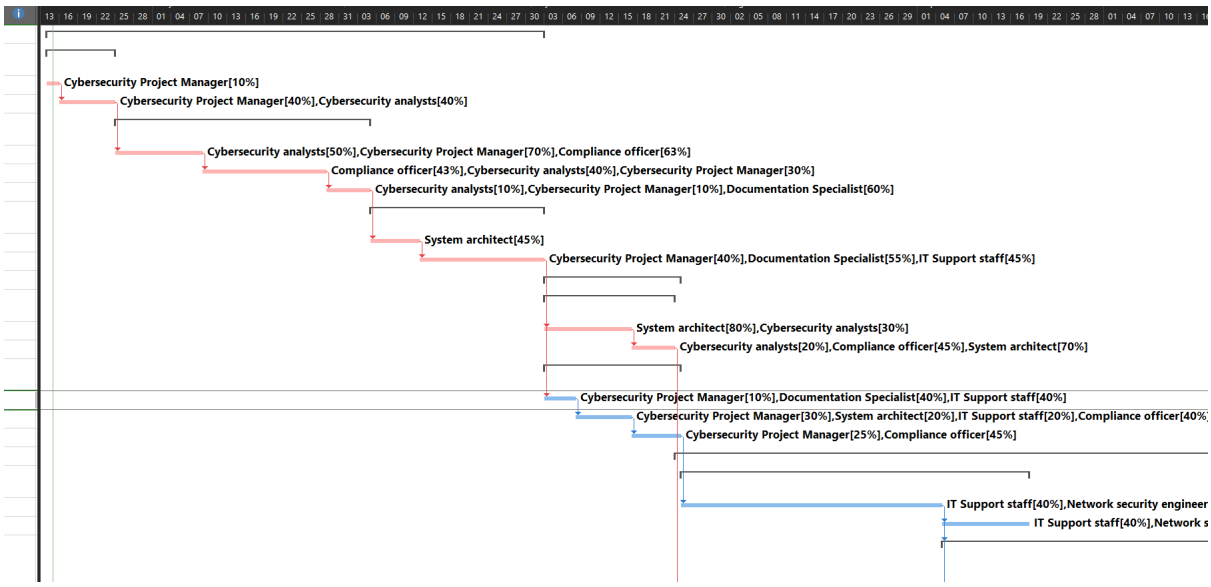
TRACKING GANTT

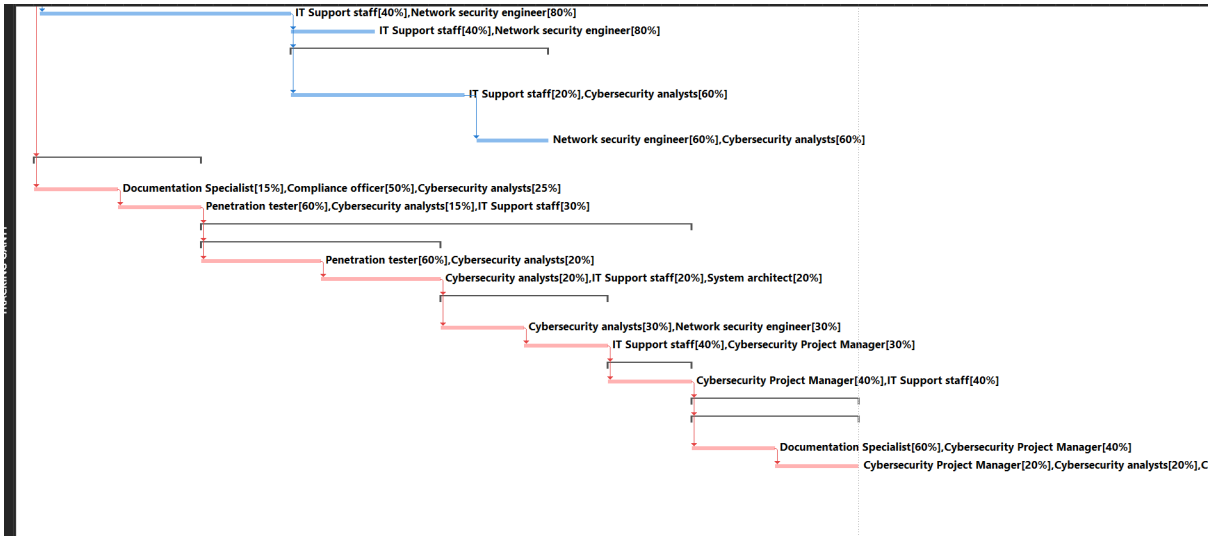
	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names	Add N
24		**Software deployment & Configuration**	**31 days**	**Fri 05-09-25**	**Fri 17-10-25**	**22**		
25		Deploy & Configure SIEM,EDR,MFA & PAM	21 days	Fri 05-09-25	Fri 03-10-25	22	IT Support staff[20%] Cybersecurity	
26		Integrate software	10 days	Mon 06-10-25	Fri 17-10-25	25	Network security e	
27		**Policy & Procedure Implementation**	**20 days**	**Thu 24-07-25**	**Wed 20-08-25**	**15**		
28		Develop & impleme	10 days	Thu 24-07-25	Wed 06-08-25	15	Documentation Sp	
29		Setup & configure Ir	10 days	Thu 07-08-25	Wed 20-08-25	28	Penetration tester	
30		**Testing**	**58 days**	**Thu 21-08-25**	**Mon 10-11-25**	**29**		
31		**Security testing**	**28 days**	**Thu 21-08-25**	**Mon 29-09-25**	**29**		
32		Conduct external pe	14 days	Thu 21-08-25	Tue 09-09-25	29	Penetration tester	
33		Remediate Vulnerat	14 days	Wed 10-09-25	Mon 29-09-25	32	Cybersecurity anal	
34		**System optimization & Integration testing**	**20 days**	**Tue 30-09-25**	**Mon 27-10-25**	**33**		
35		Validate system inte	10 days	Tue 30-09-25	Mon 13-10-25	33	Cybersecurity anal	
36		Final system optimi	10 days	Tue 14-10-25	Mon 27-10-25	35	IT Support staff[40	
37		**Go-live Preparation**	**10 days**	**Tue 28-10-25**	**Mon 10-11-25**	**36**		
38		Confirm final readin	10 days	Tue 28-10-25	Mon 10-11-25	36	Cybersecurity Proj	
39		**Project Closure**	**20 days**	**Tue 11-11-25**	**Mon 08-12-25**	**38**		
40		**Final documentation & lessons learned**	**20 days**	**Tue 11-11-25**	**Mon 08-12-25**	**38**		
41		Compile final docs &	10 days	Tue 11-11-25	Mon 24-11-25	38	Documentation Sp	
42		Final review meetin	10 days	Tue 25-11-25	Mon 08-12-25	41	Cybersecurity Proj	

The WBS outlines tentative boundaries of the work within a timeframe from April 14, 2025 up to December 24, 2025 equating to 256 days in total. The entire project scope is subdivided into major phases: Planning and Assessment 58 days (post project initiation and risk assessment), Finalize Req

and KPI 20 days (Agreement on defiined KPIs and stakeholders), Design and Procurement 16 days (cybersecurity architecture and vendor selection), Implementation 62 days (hardware and software gathering deployment), Software Deployment and Configuration 31 days (SIEM and MFAs), Policy Procedure Implementation 20 days (policy development and implementation), Testing 58 days (security systems and integration testing), Go Live Preparation 10 days (final checks), Project Closure 20 days (documentation), Final Document Lessons Learned 20 attached report and review sessions. Each of the activities specify duration and dependencies (for instance, Task 22 is a predecessor towards Task 25) Together with resources like IT Support, Cybersecurity Analyst and Documentation Expert the resource allocation for the tasks is streamlined to eliminate duplication and confusion on assignment, time, and order enabling smooth project execution.

Gantt chart





RECOMMENDATION & PROJECT PLAN

Final project Selection: Cybersecurity Enhancements

Justification: After an assessment of the two digital transformation projects, the Cybersecurity Enhancements project is suggested as it returns

Immediate ROI: By avoiding expensive breaches and protecting hospital data, this effort produces obvious benefits in just three months.

High Feasibility: Upgrading cybersecurity is simpler than rebuilding patient flow systems, which need intricate AI integration, and there are established technologies and vendors easily accessible.

High Business Value: The risk to patient data confidentiality and hospital operations following an attack by ransomware at the Crown Princess Mary Cancer Centre is too significant to overlook.

A strong cybersecurity foundation guarantees:
Defence against upcoming assaults adherence to laws governing the privacy of healthcare data (such as the Australian Privacy Act requirements), enduring confidence from clients, employees, and outside partners

Implementation Strategy

Over the course of three months, the cybersecurity improvements will be implemented. Westmead Hospital will choose appropriate cybersecurity suppliers and solutions after completing a thorough cybersecurity audit in the first month to find system weaknesses and compliance gaps. The emphasis will switch to improving the technological infrastructure in the second month, which will include network segmentation to safeguard vital assets, multi-factor authentication (MFA), and the installation of sophisticated threat detection systems. In the third month, hospital employees will receive cybersecurity awareness training, real-time monitoring and incident response procedures will be implemented, and regular threat simulations and audits will be started to guarantee system readiness and resilience.

CONCLUSION & NEXT STEPS

To sum up, improving cybersecurity provides instant benefits by safeguarding patient information and guaranteeing adherence to regulations. The three-month implementation must be finished, critical performance metrics must be tracked, and frequent security assessments must be carried out. Westmead Hospital may reliably and securely explore future digital initiatives thanks to this foundation.

REFERENCES:

1. Australian Digital Health Agency. (2023) *Cybersecurity in Healthcare*. Available at: https://www.digitalhealth.gov.au (Accessed: 23 March 2025).
2. Chatterjee, S., Bajaj, A., Ghosh, K. and Bhattacharyya, D. (2020) 'Security and privacy in healthcare', *Computers & Security*, 97, p.102006. https://doi.org/10.1016/j.cose.2020.102006
3. Office of the Australian Information Commissioner (OAIC). (n.d.) *Data Breaches Report*. Available at: https://www.oaic.gov.au (Accessed: 26 March 2025).
4. Sky News Australia. (2024) *Westmead Hospital staff call out for help due to 41-hour ER delays*. Available at: https://www.skynews.com.au (Accessed: 1 April 2025).
5. Yahoo News Australia. (2024) *Cancer patients targeted by hackers in Westmead Hospital ransomware attack*. Available at: https://au.news.yahoo.com (Accessed: 5 April 2025).