Company: My Inc.

Team: IT Department

Amul Ghodasara

Problem: My Inc. is facing a threat relating to their IT system and infrastructure by unauthorized access and cyber-attacks.

Opportunity Statement: Due to increasing cyber security breaches in North America, My Inc. has risk of cybersecurity threats and unauthorized access to the system, we will work on user interface tracking to achieve system capabilities resulting in fewer security breaches, which will achieve confidentiality within data and enhanced systems that will be a significant factor for its long-term growth.

Company Objectives: The objective of My Inc. is to keep developing mobility for everyone and everything. By facilitating better movement throughout the world, our technologies improve how people live. By enhancing cleanliness, safety, and smartness, we are enabling mobility for more people. All the while making sure that we continue to reduce our impact on the environment.

Business Case Objective:

- Reduce cybersecurity risk
- Enhance IT systems and infrastructure
- Enhance workplace security

Preliminary Metrics:

Reduce cybersecurity risk

- Number of different cyber attacks
- Number of unidentified devices on network
- System uptime and downtime

Enhance IT systems and Infrastructure

- Mean time to detect issue
- Mean time to resolve issue
- Volume of backup data
- Volume of encrypted data

Enhance workplace security

- Number of unauthorized entry attempts
- Number of days to deactivate former employee access
- Number of third-party access control

Stakeholders List:

- Employees
- Workers
- Security team
- Cybersecurity department's manager
- Cybersecurity department's team members
- IT administrator

List of Alternatives:

- Secure network and databases.
- Make security policies and procedures.
- Taking frequent feedback from employees.
- Upgrading security software and firewalls.
- Ask users to avoid connecting their system with any outside network or unknown network and devices.
- Collaborate with cybersecurity firms to protect our IT system and infrastructure.
- Enhancing the biometrics to enter into the infrastructure.
- Prevent bringing external portable devices into plants and offices.
- Provide secured phones or devices to their employees for communication and connectivity.
- Enhance antivirus software and firewalls.
- Keep backups and encrypt data.
- Maintain System and Software Updates.
- Monitor the network traffic, which would help identify malicious viruses.

List of Intermediate Alternatives:

- Collaborate with cybersecurity firms to protect our IT system and infrastructure.
- Keep backups and encrypt data.
- Monitor the network traffic, which would help identify malicious viruses.
- Upgrading security software and firewalls.
- Prevent bringing external portable devices into plants and offices.

List of Final Alternatives:

- Collaborate with cybersecurity firms to protect our IT system and infrastructure.
- Keep backups and encrypt data.
- Monitor the network traffic, which would help identify malicious viruses.

Alignment of Business case objective and Alternatives: -

By collaborating with a cybersecurity firm, we will reduce cybersecurity risk which helps us to stay competitive.

Data backups and encrypted data will help us to enhance IT systems and infrastructure and we will achieve confidentiality of data.

By monitoring network traffic, we will enhance workplace security and we will achieve high security and safety.

Evaluation Plan:

Metric variables	Description	Data Source	Baseline data
Number of different cyber attacks	The number of cyber-attacks that have been experienced in the past one year.	Company internal data	Yes
Number of unidentified devices on network	The number of devices that are unknown on the network.	Company internal data	Yes
System uptime and downtime	System uptime and down is the amount of time that your machine has been working reliably as part of your computer network and IT environment.	IT database	Yes
Mean time to detect issue	The average time that has been taken to detect an issue in last one year.	Company internal data	No
Mean time to resolve issue	The average time that has been taken to resolve an issue in last one year.	Company internal data	No
Volume of backup data	Every day, the average size of the data that has been backed up.	Company internal data	Yes

Metric variables	Description	Data Source	Baseline data
Volume of backup data	Every day, the average size of the data that has been backed up.	Company internal data	Yes
Number of unauthorized entry attempts	The number of people who gained entry and access without valid credentials in the previous week.	Company internal data	Yes
Number of days to deactivate former employee access	The average number of days to deactivate former employees' access in the past one year.	Company Internal data	Yes
Number of third-party access control	The number of third-party access controls that have been provided by My Inc. in the past one year.	Company internal data	No

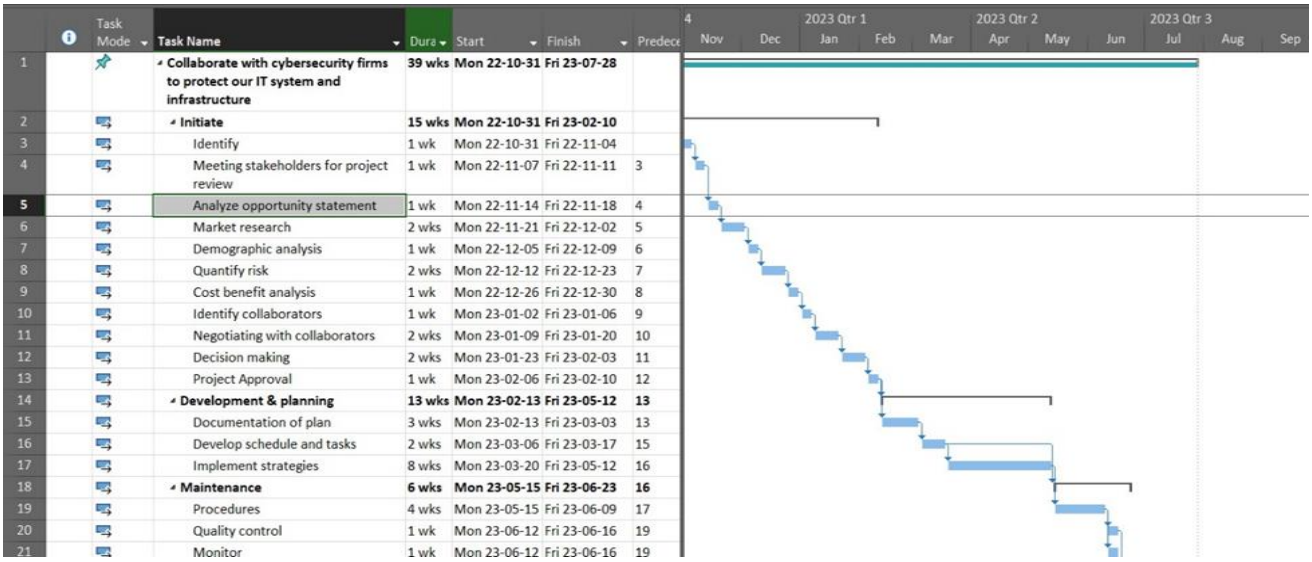
Information Gathering Plan:

What Information	Source	Method	Sequence
What encryption tools and methods does the organization currently use?	IT department	Meeting, Interview	1
Which cloud technology is used to get backup of data?	IT department	Meeting, Interview	3

What Information	Source	Method	Sequence
How frequently are internal security audits conducted?	Security department	Interview	1
How many third parties got access control?	Security department	Interview	4
What are the procedures to deactivate former employee access?	HR department	Meeting	4
What kind of unidentified devices have been tracked on the network in the past	IT department	Meeting, Interview	3
How frequently is the system's downtime and uptime recorded?	Database Administrator, IT Department	Meeting, Interview	2
Who is permitted entry into server rooms?	Security Department, every department head	Meeting, Interview	2

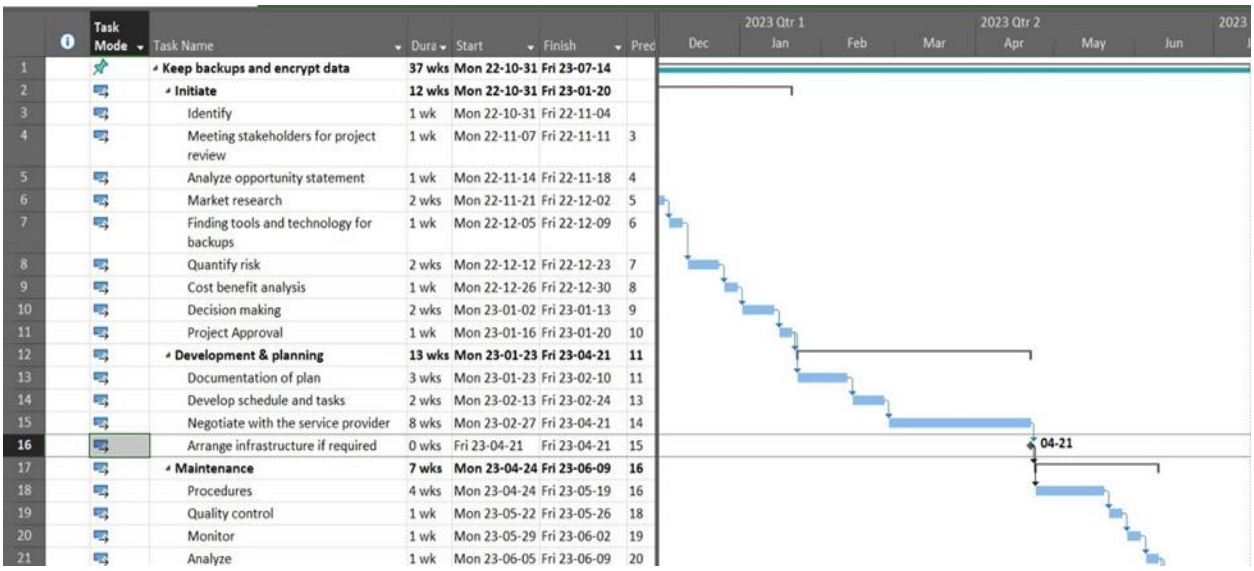
Gantt chart: -

Alternative 1: - Collaborate with cybersecurity firms to protect our IT system and infrastructure.



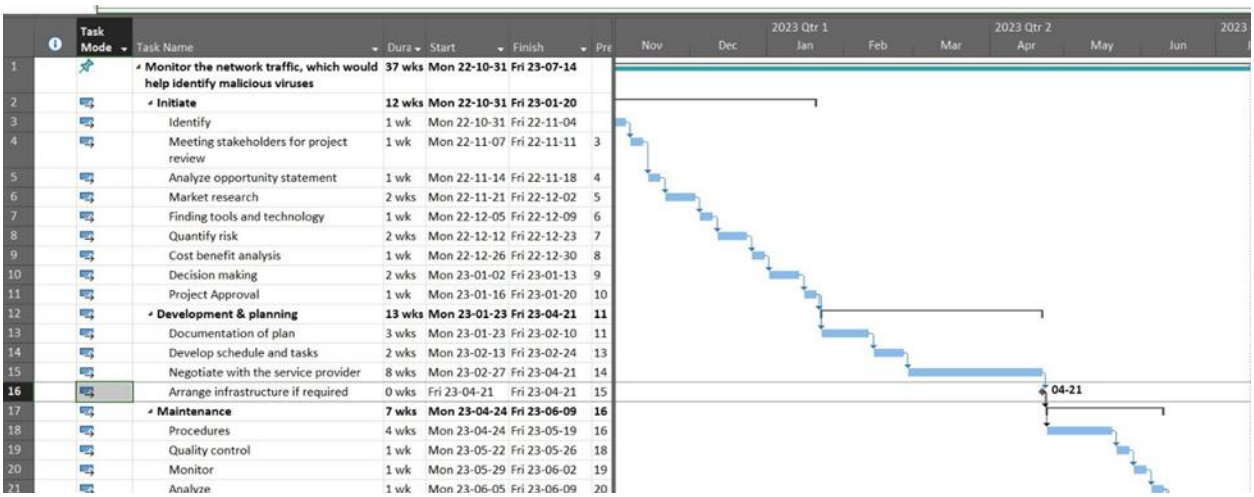
	Task Mode	Task Name	Dura	Start	Finish	Predec
1		**Collaborate with cybersecurity firms to protect our IT system and infrastructure**	**39 wks**	**Mon 22-10-31**	**Fri 23-07-28**	
2		**Initiate**	**15 wks**	**Mon 22-10-31**	**Fri 23-02-10**	
3		Identify	1 wk	Mon 22-10-31	Fri 22-11-04	
4		Meeting stakeholders for project review	1 wk	Mon 22-11-07	Fri 22-11-11	3
5		Analyze opportunity statement	1 wk	Mon 22-11-14	Fri 22-11-18	4
6		Market research	2 wks	Mon 22-11-21	Fri 22-12-02	5
7		Demographic analysis	1 wk	Mon 22-12-05	Fri 22-12-09	6
8		Quantify risk	2 wks	Mon 22-12-12	Fri 22-12-23	7
9		Cost benefit analysis	1 wk	Mon 22-12-26	Fri 22-12-30	8
10		Identify collaborators	1 wk	Mon 23-01-02	Fri 23-01-06	9
11		Negotiating with collaborators	2 wks	Mon 23-01-09	Fri 23-01-20	10
12		Decision making	2 wks	Mon 23-01-23	Fri 23-02-03	11
13		Project Approval	1 wk	Mon 23-02-06	Fri 23-02-10	12
14		**Development & planning**	**13 wks**	**Mon 23-02-13**	**Fri 23-05-12**	**13**
15		Documentation of plan	3 wks	Mon 23-02-13	Fri 23-03-03	13
16		Develop schedule and tasks	2 wks	Mon 23-03-06	Fri 23-03-17	15
17		Implement strategies	8 wks	Mon 23-03-20	Fri 23-05-12	16
18		**Maintenance**	**6 wks**	**Mon 23-05-15**	**Fri 23-06-23**	**16**
19		Procedures	4 wks	Mon 23-05-15	Fri 23-06-09	17
20		Quality control	1 wk	Mon 23-06-12	Fri 23-06-16	19
21		Monitor	1 wk	Mon 23-06-12	Fri 23-06-16	19

Alternative 2: - Keep backups and encrypt data.



	Task Mode	Task Name	Dura	Start	Finish	Pred
1		**Keep backups and encrypt data**	**37 wks**	**Mon 22-10-31**	**Fri 23-07-14**	
2		**Initiate**	**12 wks**	**Mon 22-10-31**	**Fri 23-01-20**	
3		Identify	1 wk	Mon 22-10-31	Fri 22-11-04	
4		Meeting stakeholders for project review	1 wk	Mon 22-11-07	Fri 22-11-11	3
5		Analyze opportunity statement	1 wk	Mon 22-11-14	Fri 22-11-18	4
6		Market research	2 wks	Mon 22-11-21	Fri 22-12-02	5
7		Finding tools and technology for backups	1 wk	Mon 22-12-05	Fri 22-12-09	6
8		Quantify risk	2 wks	Mon 22-12-12	Fri 22-12-23	7
9		Cost benefit analysis	1 wk	Mon 22-12-26	Fri 22-12-30	8
10		Decision making	2 wks	Mon 23-01-02	Fri 23-01-13	9
11		Project Approval	1 wk	Mon 23-01-16	Fri 23-01-20	10
12		**Development & planning**	**13 wks**	**Mon 23-01-23**	**Fri 23-04-21**	**11**
13		Documentation of plan	3 wks	Mon 23-01-23	Fri 23-02-10	11
14		Develop schedule and tasks	2 wks	Mon 23-02-13	Fri 23-02-24	13
15		Negotiate with the service provider	8 wks	Mon 23-02-27	Fri 23-04-21	14
16		Arrange infrastructure if required	0 wks	Fri 23-04-21	Fri 23-04-21	15
17		**Maintenance**	**7 wks**	**Mon 23-04-24**	**Fri 23-06-09**	**16**
18		Procedures	4 wks	Mon 23-04-24	Fri 23-05-19	16
19		Quality control	1 wk	Mon 23-05-22	Fri 23-05-26	18
20		Monitor	1 wk	Mon 23-05-29	Fri 23-06-02	19
21		Analyze	1 wk	Mon 23-06-05	Fri 23-06-09	20

Alternative 3: - Monitor the network traffic, which would help identify malicious viruses.



	Task Mode	Task Name	Dura	Start	Finish	Pre
1		**Monitor the network traffic, which would help identify malicious viruses**	**37 wks**	**Mon 22-10-31**	**Fri 23-07-14**	
2		**Initiate**	**12 wks**	**Mon 22-10-31**	**Fri 23-01-20**	
3		Identify	1 wk	Mon 22-10-31	Fri 22-11-04	
4		Meeting stakeholders for project review	1 wk	Mon 22-11-07	Fri 22-11-11	3
5		Analyze opportunity statement	1 wk	Mon 22-11-14	Fri 22-11-18	4
6		Market research	2 wks	Mon 22-11-21	Fri 22-12-02	5
7		Finding tools and technology	1 wk	Mon 22-12-05	Fri 22-12-09	6
8		Quantify risk	2 wks	Mon 22-12-12	Fri 22-12-23	7
9		Cost benefit analysis	1 wk	Mon 22-12-26	Fri 22-12-30	8
10		Decision making	2 wks	Mon 23-01-02	Fri 23-01-13	9
11		Project Approval	1 wk	Mon 23-01-16	Fri 23-01-20	10
12		**Development & planning**	**13 wks**	**Mon 23-01-23**	**Fri 23-04-21**	**11**
13		Documentation of plan	3 wks	Mon 23-01-23	Fri 23-02-10	11
14		Develop schedule and tasks	2 wks	Mon 23-02-13	Fri 23-02-24	13
15		Negotiate with the service provider	8 wks	Mon 23-02-27	Fri 23-04-21	14
16		Arrange infrastructure if required	0 wks	Fri 23-04-21	Fri 23-04-21	15
17		**Maintenance**	**7 wks**	**Mon 23-04-24**	**Fri 23-06-09**	**16**
18		Procedures	4 wks	Mon 23-04-24	Fri 23-05-19	16
19		Quality control	1 wk	Mon 23-05-22	Fri 23-05-26	18
20		Monitor	1 wk	Mon 23-05-29	Fri 23-06-02	19
21		Analyze	1 wk	Mon 23-06-05	Fri 23-06-09	20

Cost Benefit Analysis:

Alternative 1: - Collaborate with cybersecurity firms to protect our IT system and infrastructure.

Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Monitoring	50,000	55,000	60,000	65,000	70,000	300,000
Collaboration	125,000	0	0	0	0	125,000
Systems	80,000	2,500	2,500	2,500	2,500	90,000
Training	10,000	0	0	0	0	10,000
Maintenance	7,500	5,000	5,000	5,000	5,000	27,500
Services	10,000	1000	1000	1000	1000	14,000
Operations cost	12,000	12,000	12,000	15,000	15,000	66000
Insurance cost	250,000	275,000	300,000	300,000	300,000	1425000
Total cost	544,500	350,500	380,500	388,500	393,500	2,057,500
Benefits	360,000	378,000	396,900	436590	480249	2,051,739
Cash flow	-184,500	27,500	16,400	48090	86749	-5,761
NPV						
r=15%	-160434.78	20793.95	10783.27	27495.61	43129.58	-58232.37
Cumulative NPV	-160434.78	-139640.83	-128857.57	-101361.95	-58232.37	

Operating costs = listed operating cost + monitoring + training + maintenance + services + insurance cost

Investment = collaboration + systems

Cost Benefit Ratio (CBR) = (Benefits - Operations Cost)/ Investments

Operations costs = 1,842,500

Investment = 215,000

CBR = 0.97320

CF= Total cost – total benefits

NPV = (CF0/ (1+r) ^0) + (CF1/ (1+r) ^1) + (CF2/ (1+r) ^2) + (CF3/ (1+r) ^3) +…

r = discount rate = 15%

NPV = -$58232.37

Payback period > Year 5th

Alternative 2: - Keep backups and encrypt data.

Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Storage of backup	100,000	0	0	0	0	100,000
Frequency of backup	15,000	10,000	10,000	10,000	10,000	55,000
Systems to encrypt	150,000	0	0	0	0	150,000
Licensing	10,000	5000	5000	5000	5000	30,000
Training	10,000	1000	1000	1000	1000	14,000
Maintenance	10,000	10,000	10,000	15,000	15,000	60,000
Services	100,000	0	0	0	0	100,000
Operations cost	300,000	325,000	350,000	375,000	400,000	1,750,000
Total cost	695,000	351,000	376,000	406,000	431,000	2,259,000
Benefits	280,000	520,000	592,000	615,000	695,000	2,702,000
Cash flow	-415,000	169,000	216,000	209,000	264,000	443,000

Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
NPV						
r=15%	-380,733.945	142,243.9	166,791.6	148,060.9	171,581.9	247,944.4
Cumulative NPV	-380,733.945	-283,490.045	-71698.445	76362.455		

Operations cost = listed operating cost + training + licensing + maintenance + services

Investment = storage of backup + frequency of backup + systems to encrypt

Cost Benefit Ratio (CBR) = (Benefits - Operations Cost)/ Investments

Operations cost = 1,954,000

Investment = 305,000

CBR = 2.452459

CF= Total cost – total benefits

NPV = (CF0/ (1+r) ^0) + (CF1/ (1+r) ^1) + (CF2/ (1+r) ^2) + (CF3/ (1+r) ^3) +…

r = discount rate = 15%

NPV = $76362.455
Payback period = Year 4th

Alternative 3: - Monitor the network traffic, which would help identify malicious viruses (Amount in CAD)

Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Monitoring	75,000	80,000	85,000	90,000	95,000	425,000
Remodel	15,000	0	0	0	0	15,000
Systems	80,000	2,500	2,500	2,500	2,500	90,000
Anti-virus Installation	10,000	0	0	0	0	10,000
Licensing	7,500	5000	5000	5000	5000	27,500

Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Training	10,000	1000	1000	1000	1000	14,000
Maintenance	20,000	20,000	20,000	25,000	25,000	110,000
Services	100,000	0	0	0	0	100,000
Operations cost	300,000	325,000	350,000	375,000	400,000	1750000
Total cost	617,500	433,500	463,500	498,500	528,500	2,541,500
Benefits	282,500	520,500	592,500	615,100	695,500	2,706,100
Cash flow	-335,000	87,000	129,000	116,600	167,000	164,600
NPV						
r=15%	-291,304.35	65784.5	84819.59	66,666.43	83028.51	8994.69
Cumulative NPV	-291,304.35	-225519.85	-140700.25	-74033.83	8994.69	

Operation cost = Listed operating cost + Leasing + Training + Licensing + Insurance cost

Investments=Remodel + system + installation + infrastructure cost

Cost Benefit Ratio (CBR) = (Benefits - Operations Cost)/ Investments

Operations cost = 2,326,500

Investment = 215,000

CBR = 1.765581395

NPV = (CF0/ (1+r) ^0) + (CF1/ (1+r) ^1) + (CF2/ (1+r) ^2) + (CF3/ (1+r) ^3) +…

r = discount rate = 15%

NPV = $8994.69

Payback period = Year 5th

Multiple Objectives Analysis:

With Multiple Objective Analysis (MOA), we take value analysis one step further in order to quantify the intangible criteria. We will also score the tangible criteria to come up with a total score for each alternative.

Each alternative is evaluated based on the following qualities: -

Security, Confidentiality, Vulnerability, Cyber risk

Alternatives	Security	Confidentiality	Vulnerability	Cyber risk
Collaborate with cybersecurity firms to protect our IT system and infrastructure.	High	Medium	Low	Low
Keep backups and encrypt data.	Medium	Medium	High	High
Monitor the network traffic, which would help identify malicious viruses.	Medium	Medium	High	Medium

Alternatives	Security	Confidentiality	Vulnerability	Cyber risk
Collaborate with cybersecurity firms to protect our IT system and infrastructure.	0.9	0.7	0.5	0.4
Keep backups and encrypt data.	0.6	0.6	0.7	0.7
Monitor the network traffic, which would help identify malicious viruses.	0.6	0.6	0.8	0.6

Assigning Weights:

We document the worst and best measures for each criterion…

Criteria	Worst	Best
Security	Medium	High
Confidentiality	Medium	High
Vulnerability	Low	High
Cyber risk	Low	High

Assigning Weights: Most important down to least important

Criteria	Worst	Best	Assigned value
Security	Medium	High	100
Confidentiality	Medium	High	75
Vulnerability	Low	High	60
Cyber risk	Low	High	50
			285

Assigning Weights: Lowest to highest in importance

Criteria	Worst	Best	Assigned value
Cyber risk	Low	High	10
Vulnerability	Low	High	30
Confidentiality	Medium	High	60
Security	Medium	High	90
			190

Assigning Weights: Criteria Weighting

Criteria	High-Low	Low-High	Compromise
Security	0.35	0.47	0.41
Confidentiality	0.26	0.31	0.28
Vulnerability	0.21	0.15	0.18
Cyber risk	0.17	0.05	0.11

Value Score Calculation

Now we have a set of weights we can use to determine the importance of each criterion. We need to bring back our original scores as well. So, we modify our original score (between 0-1) by the weighting to come up with a final score.

Criteria	Weight	Alternative 1	Alternative 2	Alternative 3
Security	0.41	0.369	0.246	0.246
Confidentiality	0.28	0.196	0.168	0.168
Vulnerability	0.18	0.09	0.126	0.144
Cyber risk	0.11	0.044	0.077	0.066
Total	0.98	0.669	0.617	0.624

Summary Table:

Alternatives	PROS	CONS
Collaborate with cybersecurity firms to protect our IT system and infrastructure.	• Low cost since no infrastructure cost for storage ($250,000) • Time effective since getting the solution by collaboration (5 weeks) • Payback time is the highest amongst other alternatives. (>5)	• It is a dependent solution on another firm. • No flexibility in working methods • Judgement complication or loss of control
Keep backups and encrypt data.	• Short development time (13 weeks). • NPV is the highest. ($76362.455) • Quality services to the customer	• Low competitive advantage • Medium investment cost ($310,000) • Payback time is the lowest. (4)
Monitor the network traffic, which would help identify malicious viruses.	• The customer satisfaction will be high in this alternative. • This alternative can be a factor of survival for the business. • This alternative will help in growth of revenue. • Payback year is better than alternative 2. (5)	• The operations cost is high ($1,750,000). • Initial investment is also high ($550,000). • Time consuming and requires loads of analysis – 25 weeks.

Sensitivity Analysis:

Alternative 1: - Collaborate with cybersecurity firms to protect our IT system and infrastructure.

Assume that Total Costs will be 1% higher than baseline values.

% Change in NPV = ($58232.37 – (-$57650.37)) / -$57650.37 = - 1.009%

Sensitivity of NPV = -1.11%/1% = -1.009

- This means that with an increase in total costs of 1%, the NPV of a project will decrease by 1.009%, and vice versa, if total costs are reduced by 1%, the NPV will increase by 1.009%.

% Change in IRR = (14% - 12%) / 12% = 0.14 %

Sensitivity of IRR = 0.14% / 1% = 0.14

This means that with an increase in total costs of 1%, the IRR of a project will decrease by 0.14%, and vice versa, if fixed costs are reduced by 1%, the IRR will increase by 0.14%.

Alternative 2: - Keep backups and encrypt data.

Assume that Total Costs will be 1% higher than baseline values.

% Change in NPV = ($76362.455 – (-$75599.195)) / -$75599.135 = - 0.99%

Sensitivity of NPV = -1.11%/1% = -0.99

- This means that with an increase in total costs of 1%, the NPV of a project will decrease by 0.99%, and vice versa, if total costs are reduced by 1%, the NPV will increase by 0.99%.

% Change in IRR = (15% - 12%) / 12% = 0.25 %

Sensitivity of IRR = 0.25% / 1% = 0.25

This means that with an increase in total costs of 1%, the IRR of a project will decrease by 0.25%, and vice versa, if fixed costs are reduced by 1%, the IRR will increase by 0.25%.

Alternative 3: - Monitor the network traffic, which would help identify malicious viruses.

Assume that Total Costs will be 1% higher than baseline values.

% Change in NPV = ($8994.69 – (-$8178.12)) / -$8178.12 = - 1.11%

Sensitivity of NPV = -1.11%/1% = -1.11

- This means that with an increase in total costs of 1%, the NPV of a project will decrease by 1.11%, and vice versa, if total costs are reduced by 1%, the NPV will increase by 1.11%.

% Change in IRR = (16% - 14%) / 14% = 0.14 %

Sensitivity of IRR = 0.14% / 1% = 0.14

- This means that with an increase in total costs of 1%, the IRR of a project will decrease by 0.14%, and vice versa, if fixed costs are reduced by 1%, the IRR will increase by 0.14%.

Risk Analysis

Alternative	Risk description	Consequences	Impact	Risk level
Collaborate with cybersecurity firms to protect our IT system and infrastructure.	Complexity in decision making and autonomy Stakeholder confusion	The involvement of different organizations can cause disputes in management. The list of stakeholder's changes with the collaboration.	Medium	Low
Keep backups and encrypt data.	End user conflict Confidential data leak	Data might be encrypted to the authorities too Unauthorized data encryption might lead to data leak	Medium	High
Monitor the network traffic, which would help identify malicious viruses	Security breach	Monitoring the network can lead to breaches.	Medium	Medium

Final recommendation/ Closing argument

Following the CBA, MOA, sensitivity analysis, and risk analysis, alternative 1 is the most reliable alternative amongst the three alternatives, which is as follows:

Collaborate with cybersecurity firms to protect our IT system and infrastructure.

The main reasons for this choice are:

- The collaboration cuts down a lot of extra costs that will result in finding an effective solution.
- Collaboration involves professionals who are experienced, and this brings reliability to the solution.
- Collaboration is going to save a lot of time as there is expertise already and this makes the alternative time efficient.
- This solution has the longest payback period, and this is a huge factor in selecting the alternative as the best one.

Thereby, with the above reasons in place and also the alternative having the lowest risk amongst the alternatives, a good MOA weightage, almost ideal sensitivity and less complexity of the implementation, alternative 1 becomes the best possible option for our problem.

Risk Register

Risks	Description	Consequences	Risks Probability	Risk Impact	Risk level	Risk Owner	Risk Mitigation Plan
Ransomware attack risk	Until ransomware, software that prohibits individuals from reaching the system or any other component of the software system is installed.	A business's ability to grow in a variety of areas, such as revenue, may be hampered by a failure to safeguard databases from ransomware attacks.	**0.3**	**0.8**	**High**	**Cyber security team**	The infrastructure must be updated with the most recent virus security software.
Data theft & Misuse risk	Data theft and data misuse can affect firms and clients simultaneously in various factors.	Through its misuse, data theft impacts the entire company in just one hour. For instance, rival businesses may profit by selling customer data	**0.3**	**0.7**	**High**	**Data server managing team**	The usage of firewalls and post-attack tactics should be continuous, day and night.

		on the illicit market.					
Risks	**Description**	**Consequences**	**Risks Probability**	**Risk Impact**	**Risk level**	**Risk Owner**	**Risk Mitigation Plan**
Denial of services	It'll delay and affect the company's work pace and waste the firm's precious time.	Due to the hacker, system access will terminate for all registered users, and they can lose their work and volatile with data.	**0.2**	**0.5**	**Medium**	**System administrators and securities department**	Auto freeze data or system if someone unauthorized tries to access it. Just the team leads to access and authenticate it.
Software-Hardware Malfunction	Use of the same old Software and hardware will be a risk to IT infrastructure in every possible phase.	Due to old technologies software and hardware, it can malfunction at any time while some important projects going on and can lose everything in the IT infrastructure.	**0.7**	**0.8**	**High**	**Maintenance and technical departments**	Upgrade the software and hardware with the latest technologies, day by day.

Implementation Plan

Phase	Task	Person/Group responsible	Resources required	Cost	Estimated weeks
Phase 1					
Initiate	1. Meeting stakeholders 2. Analyse opportunity statement 3. Negotiating with collaborators 4. Decision making	1. IT Manager 2.Collaborators 3. Finance Manager 4.Cybersecurity department's manager	1. Current stakeholder list 2. Risk analysis 3. The collaborator list	**$125,000**	**15 Weeks**
Phase 2					
Development	1. Documentation of plan 2. Develop schedule and tasks 3. Implement strategies	1. Project Manager 2. IT Executive / Administrator 3. Technical team of executives	1. Systems and software 2. a team of members, guidelines, and data of the solution 3. Analytical tools	**$166,000**	**13 Weeks**
Phase 3					
Maintenance	1. Procedures 2. Quality control 3. Monitor 4. Analyse	1. IT admin 2. IT team 3. Security team	1. Directory of the system 2. 6-member team, software's data, Received quotations	**$344,500**	**6 Weeks**

Communication Plan

MEETING TITLE	DESCRIPTION	INPUT	OUTPUT
Kick-off meeting	Brainstorming to identify the major problem for low sales and defining its opportunity statement and setting its objective.	Request for change (RFC)	preliminary metrics
Identify stakeholders	Defining the scope of requirements and identifying stakeholders	Request for change (RFC)	list of stakeholders
Identify Alternatives	Brainstorming potential solutions to the problem, Choosing the best alternatives.	Preliminary metrics	Final alternatives
Analyse Alternatives	Choosing the best alternatives through various levels of analysis.	Tangible and intangible costs, cost benefits, and discount rates. Predicting best/ worst case scenarios for sales	NPV, MOA, Total Net Income, CBA.
Analyse Risk	Identifying risks of final alternatives.	A final alternative, Impact analysis	Risk Register

MEETING TITLE	DESCRIPTION	INPUT	OUTPUT
Analysing implementation phases	Identifying milestones and associated tasks, as well as the resources and costs required	A final alternative, Stakeholders list, Cost	Implementation plan
Mitigation of risk	Identifying and modifying risk owners.	Risk register	Risk mitigation plan

MEETING TITLE	DESCRIPTION	INPUT	OUTPUT
Review meeting	Analysing implementation progress	Implementation plan	Progress report