|  |
| --- |
| Cyber risk report for boutique hospital  Risk Assessment Report |
| RA2 |



**CIS 650 – RA2 Utsav Khatiwada**

Contents

[1](#_Toc116331728)

[Overview: 3](#_Toc116331729)

[Scenario of Hospital before the attacks 4](#_Toc116331730)

[Risk Assessment Report Scenario 1: 4](#_Toc116331731)

[Analysis report for Phishing attack (S1): 4](#_Toc116331732)

[Control measures 7](#_Toc116331733)

[SSL certificate 7](#_Toc116331734)

[Automated anti-phishing solution 7](#_Toc116331735)

[SETA program: 7](#_Toc116331736)

[Scenario of Phishing attack after the control measures: 7](#_Toc116331737)

[Scenario 2 – Social Engineering (S2 a): 9](#_Toc116331738)

[Risk Analysis report of Social Engineering before control measures: 9](#_Toc116331739)

[Control Measures for social engineering: 10](#_Toc116331740)

[SETA Program: 10](#_Toc116331741)

[Identity verification: 11](#_Toc116331742)

[Risk analysis of social engineering after control measures (S2 a): 11](#_Toc116331743)

[Future Actions: 12](#_Toc116331744)

# Overview:

The following risk assessment report is based on the cyber attacks happening in boutique hospital. This hospital has a huge reputation because of high end patient involved. This hospital is famous for individuals including celebrities, politicians, business executives and movie stars. This hospital has capacity of holding 40 patients per week and offers various treatment options including top-notch surgeons. But currently, this hospital is getting victimized by different cyber-attacks including Social Engineering attacks and Phishing attacks. According to last year’s CISO data, the organization was being probed somewhere between twice a week for social engineering attacks and thrice a day for Phishing attacks.

Prior investment to control these attacks was between $100k and $500k, with an average of $300k. Regardless of this budget, the probability of getting this kind of cyber-attack is higher. Therefore, the top leadership of the organization is concerned about the factor of financial loss and reputational loss. As some competitors have been already victimized by legal action which has led to the likelihood of getting a law action with a monetary value of $2M to $50M. So, to prevent this situation risk assessment is performed with the best control measure to preserve the financial and reputational loss of the organization

PROBLEM

Assets Threat

1. Patient Health Information
2. Hospital Reputation
3. Employee information
4. Health Records

The boutique hospital has been the victim of phishing attacks and social engineering attacks. The hospital has very critical data on different high-profile persons including their PHI. If this data is compromised using the attacks, it can create critical damage to the hospital’s reputation and finance. Due to hampering in reputation and finance top leadership of the hospital is concerned to control the threats coming from these attacks. Top leadership has also increased the initial budget before these security breaches to eliminate this risk.

# Scenario of Hospital before the attacks

The boutique hospital has allocated 100k to 500k budget for the mitigating any cybercrime related issues. This budget was correspondingly allocated on the basis to the last years report from CISO (Chief information security officer). Even though the budget was allocated for that purpose, due to much more vicious attacks by hackers including social engineering and Phishing attacks, the reputation and financial aspects are in danger.   
  
A scenario of the Hospital after the attacks:  
 After Phishing and social engineering, attacks increased thrice a day and twice a week respectively. The company’s top leaders are concerned about finding a proper solution to uplift the financial and reputational damage done by these cybercrimes. The reputational damage done could go from 2M to 50M as per the data.

# Risk Assessment Report Scenario 1:

# Analysis report for Phishing attack (S1):

Text

Description automatically generated

The following table is delivered from the fair risk analysis tool. It shows the representation of the CISO report of current scenario. Threat capability includes the power of attackers to attack on hospital data through phishing, and resistance strength shows the strength of a hospital that can defend the possible attacks

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Threat Event Frequency describes the number of Phishing attacks performed by the attacker monthly. Moreover, the probability of action simulates the percentile ratio of attacker according to the number of attacks performed on a monthly basis

Graphical user interface, text

Description automatically generated

Table

Description automatically generatedGraphical user interface

Description automatically generated with medium confidence

Following is the diagrammatic representation of the loss exposure of the hospital derived from the above data. It shows the minimum, average, and maximum loss in a month if all the phishing attacks are successful. If we calculate on yearly basis the results are  
Minimum = 583.8M \* 12 = 7.056B/ Yr.

Average = 3.3B \* 12 = 39.96B / Yr.

Maximum = 8.7B\*12 = 104.40B / Yr.

The following report cast the final analysis report of the hospital loss from Phishing attack according to above data. These reports simulate the data comparing threat capability and resistance strength of hackers and hospital. It shows the monthly loss magnitude. This data shows the primary loss and secondary loss for the hospital created by attacks. It also shows the vulnerability in the hospital in current scenario. This data is based on monthly scenario

*Note: Above analysis is done in monthly basis because the phishing attacks occurred in yearly basis could not be added to Fair U analysis input. Fair u analysis maximum occurrence in a year is limited to 1000 but according to the question the maximum Phishing attack tends to be 1440. Therefore, the following analysis is done monthly and later converted on a yearly basis.*

Data Inputs for Primary loss:

|  |  |  |  |
| --- | --- | --- | --- |
| Inputs | Minimum | Most Likely | Maximum |
| Productivity | 300,000 | 500,000 | 800,00 |
| Response | 100,000 | 300,000 | 500,00 |
| Replacement | 1,000,000 | 5,000,000 | 10,000,000 |
| Competitive Advantage | 100,000 | 125,000 | 250,000 |
| Fines and Judgement | 2,000,000 | 5,000,000 | 10,000,000 |
| Reputation | 2,000,000 | 5,000,000 | 10,000,000 |

The above values in the table are assumed according to the data provided.

Data Inputs for Secondary Loss:

|  |  |  |  |
| --- | --- | --- | --- |
| Inputs | Minimum | Most Likely | Maximum |
| Productivity | 100,000 | 150,000 | 200,000 |
| Response | 60,000 | 68,000 | 100,000 |
| Replacement | 100,000 | 300,000 | 500,00 |
| Competitive Advantage | 60,000 | 120,000 | 300,000 |
| Fines and Judgement | 100,000 | 150,000 | 300,000 |
| Reputation | 100,000 | 150,000 | 300,000 |

The above values in the table are assumed according to the data provided.

According to the current scenario, Phishing attacks is being probable twice a day. The following values are calculated as twice a day is the minimum attack, thrice a day is most likely and four times a day is the maximum attack. This leads to 60 times a month as a minimum, 90 times a month being the most likely, and 120 times a month being the maximum. By implementing the following values on FairU analysis, the results show the loss for the hospital within the year which comes to a minimum loss of $7.05 billion, an average loss of $ 39.6 billion dollars, and a maximum loss of $104.04 billion dollars on yearly basis. The analysis also shows the vulnerability of a hospital getting attacked which comes to around 66.5%. This number shows that the hospital system is quite vulnerable. Therefore, to defend from this situation there should be good control measures to reduce the financial and reputational loss.

# Control measures

## SSL certificate

SSL certificate enables website to move from HTTP to HTTPS. By doing this it enables the encrypted communication between the web browser and webserver. This will reduce the chance of Phishing attacks sent from the attackers.

Automated anti-phishing solution:

Automated anti-phishing solution refers to third-party software like Abnormal security trustifi etc. This software detects Phishing emails and other malicious content sent by an attacker and removes it automatically before it gets to the company system. These will also help to reduce the malicious content reaching on company’s system.

## SETA program:

SETA program refers to the awareness program against cyber-attacks. In such a big hospital which has data on high-end personnel like celebrities and politicians. The security should be very tight, Implementing the SETA program and providing awareness about the possible cyber-attack can make employees aware of phishing attacks. So, whenever they see such an email, they can directly report to the security team of the hospital. Doing this can prevent the vulnerable data of the hospital and increase the resistance strength.

Fair U analysis report after control measures:

After applying the control measures the resistance strength of the hospital has increased. So, the attacker’s strength is weaker than the defensive strength of the hospital security. This shows the number of times the attacker trying to get in the system is unsuccessful because of implementation of the control measures. This helps the hospital to reduce the financial loss as well as reputational loss. More importantly the PHI of the celebrity and politician in safe.

Text

Description automatically generatedText

Description automatically generated

# Scenario of Phishing attack after the control measures:

Risk analysis report for phishing attack after the control measures (S1 a)

Graphical user interface

Description automatically generated with medium confidenceGraphical user interface

Description automatically generated with medium confidence

This diagram represents the loss exceedance cure. This curve shows the probable loss of the hospital after applying the control measures. If we compare this curve with the previous loss exceedance curve before the control measures we can see a huge drop in the probable loss for the hospital. The data shows that there is a minimum of $254.1M, an average of $1.3B, and a maximum of $3.7B. This is the monthly probable loss to the company after control measures. If we do yearly calculation

These reports simulate the data comparing threat capability and resistance strength of hackers and hospitals. It shows the monthly loss magnitude. This data shows the hospital’s primary and secondary losses created by attacks. It also shows the vulnerability in the hospital after the control measures. As our previous data before control measures show the hospital was 66.5%vulnerable to Phishing attacks whereas, after the control measures it dropped to 27% which means that getting victimized by phishing attacks is less likely than before.

*Note: Above analysis is done in monthly basis because the phishing attacks occurred in yearly basis could not be added to Fair U analysis input. Fair u analysis maximum occurrence in a year is limited to 1000 but according to the question the maximum Phishing attack tends to be 1440. Therefore, the following analysis is done by monthly and later converted on a yearly basis.*

# Scenario 2 – Social Engineering (S2 a):

## Risk Analysis report of Social Engineering before control measures:

Graphical user interface, text

Description automatically generatedGraphical user interface, text

Description automatically generatedGraphical user interface, text

Description automatically generated

Threat event frequency is accumulated from the data of contact frequency and probability of action. This explains the probability of social engineering attacks occurring within the year without control measures. As per the data, the probable social engineering attack was twice a week considering that, this data is counted yearly which is the minimum attack is 2\*4\*12 = 96, the most likely attack 2\*4\*12 = 144, and the maximum attack probable in a year is 4\*4\*12 = 196. This is the number of attacks that might occur within a year before applying the control measures.  
  
The threat capability is assumed to be higher than the resistance strength of the hospital because in the current scenario there is an occurrence of financial and reputational loss. If the threat capability was not higher than the resistance strength, then there would not be higher losses as of now.

Table

Description automatically generatedGraphical user interface

Description automatically generated

Data Inputs for Primary loss:

|  |  |  |  |
| --- | --- | --- | --- |
| Inputs | Minimum | Most Likely | Maximum |
| Productivity | 300,000 | 500,000 | 800,00 |
| Response | 100,000 | 300,000 | 500,00 |
| Replacement | 1,000,000 | 5,000,000 | 10,000,000 |
| Competitive Advantage | 100,000 | 125,000 | 250,000 |
| Fines and Judgement | 2,000,000 | 5,000,000 | 10,000,000 |
| Reputation | 2,000,000 | 5,000,000 | 10,000,000 |

The above values in the table are assumed according to the data provided.

Data Inputs for Secondary Loss:

|  |  |  |  |
| --- | --- | --- | --- |
| Inputs | Minimum | Most Likely | Maximum |
| Productivity | 100,000 | 150,000 | 200,000 |
| Response | 60,000 | 68,000 | 100,000 |
| Replacement | 100,000 | 300,000 | 500,00 |
| Competitive Advantage | 60,000 | 120,000 | 300,000 |
| Fines and Judgement | 100,000 | 150,000 | 300,000 |
| Reputation | 100,000 | 150,000 | 300,000 |

The above values in the table are assumed according to the data provided.

According to the current scenario, social engineering attacks is being probable twice a week. The following values are calculated as twice a week is the minimum attack, thrice a week is most likely and four times a week is the maximum attack. By implementing the following values on FairU analysis, The results show the loss for the hospital within the year which comes to a minimum loss of $1.4 billion, an average loss of $ 4.2 billion dollars, and a maximum loss of $10.4 billion dollars on yearly basis. The analysis also shows the vulnerability of a hospital getting attacked which comes to around 67.06%. This number shows that the hospital system is quite vulnerable. Therefore, to defend from this situation there should be good control measures to reduce the financial and reputational loss.

# Control Measures for social engineering:

## SETA Program:

SETA program refers to the awareness program against cyber-attacks. In such a big hospital which has data on high-end personnel like celebrities and politicians. Security should be very tight, Implementing the SETA program and providing awareness about the possible cyber-attack can make employees aware of Social-Engineering attacks. So, whenever they see a suspicious person or get suspicious phone calls, they can directly report it to the security team of the hospital. Doing this can prevent the vulnerable data of the hospital and increase the resistance strength.

## Identity verification:

Identity verification is most needed to control social engineering attacks. A person can impersonate somebody else and can gather information from the hospital. To not let it happen employees like security guards and the front desk should verify their identity. Implementing this can reduce the social engineering attack.  
  
Specific Authority to health care database:  
 The high-class data should be only authorized to specific personnel. The data should not be shared with all the employees. This will reduce the chance of leaking information.

# Graphical user interface, text Description automatically generatedRisk analysis of social engineering after control measures (S2 a):

After applying the control measures the resistance strength of the company has increased. This has created a positive impact on the company’s finances and reputational values. Before the control measures, the vulnerability of the hospital was 67.06% whereas, after implementing the above control measures the vulnerability has decreased to 26.82%. This shows that the chances of getting social engineering attack have dropped tremendously.

Graphical user interface, text

Description automatically generated

Table

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

# Future Actions:

After applying this mitigation in actions, with in every month there should be repeated risk assessments. According to the situation in future, other necessary actions and changes could be implemented.