

Social Engineering and Phishing Attacks against The Boutique Hospital

Risk Assessment Report

About the document

This analysis report demonstrates and analyzes the risk to The Boutique Hospital due to the regular Phishing and Social Engineering attacks. This document is built with minimal technical specifications to match the readability capacity of the executives in the organization.

Problem

The Boutique hospital is regularly being attacked by cybercriminals with social engineering and phishing attacks. The hospital is being targeted because of the client circle being high class personnel. This is potentially a huge problem due as the consequences of a data breach could be extremely high in terms of finance. The attacks are impacting staff randomly. The latest attacks suggest targeting 12 people at once with people on higher part of the organizational pyramid becoming primary targets.

Previous Year Cyberattack Report

In the previous year, the Chief Information Security Officer reported the social engineering attacks occurring 2 times a week on average. Moreover, the reports suggest that phishing attacks are attempted 3 times a day on average.

Financial and Reputational Risk

The organization is at risk of losing its reputation and pay hefty fines due to the cyberattacks. A successful attack led to a loss of at least \$2,000,000. On top of that, the organization is at risk of being listed in the HHS' "Wall of Shame" which is a disaster for the hospital.

Assets

Due to the nature of social engineering and phishing attacks along with the reports of competitors' breached data, the following are assets with potential risk:

- PHI Information
- Electronic Mail and attached documents.
- Network Servers
- Patient and Employee Databases
- Electronic Medical Records

Analysis Method: Fair-U Tool

The Fair-U tool developed by RiskLens is used for the analysis. This tool analyzes the inputs and generates a report. The datapoints used in this method are generated from previous risk reports and ongoing frequency of attempted attacks. The datapoints used in tool.

Loss Magnitude Datapoints

The loss magnitude datapoints used in all the scenarios in this document is inputted after careful consideration with the data analysts, financial analysts, finance managers and the security team. These data points are to be the same throughout the scenarios as each successful breach would result in similar loss magnitude.

Primary Loss

The primary losses include Productivity, response, replacement, reputation and legal costs for the hospital. The following datapoints are input in the primary loss section:

Productivity

Minimum	Most-likely	Maximum
\$100,000	\$500,000	\$1,000,000

Once the attack is successful, the servers would have to be shut down by the response team which will result in delays and loss of work. This also includes the employees being paid during the incident without any productivity.

Response

Minimum	Most-likely	Maximum
\$100,000	\$300,000	\$500,000

The response is derived from a report from previous year. Prior security problems were handled by a reputable regional investigation firm, and the cost ranged from \$100k to \$500k with a cost of roughly \$300k being the most likely. The reported data is used for response as datapoints for accuracy.

Replacement

Minimum	Most-likely	Maximum
\$50,000	\$80,000	\$120,000

The replacement costs are accumulated with the help of purchase records of the servers and network hardware. Replacement of these devices will be needed in case of a severe attack damaging the equipment.

Reputation and Legal Fees

Reputation


Minimum	Most-likely	Maximum
\$2,000,000	\$10,000,000	\$50,000,000

Legal Fees

Minimum	Most-likely	Maximum
\$2,000,000	\$10,000,000	\$50,000,000

The hospital has a high reputation to maintain. The reputational cost of goodwill is practically uncountable. Looking at the reported data, the organization believes that both reputation and legal fees would be around \$10M each. Both have a minimum of \$2M and a maximum of \$50M.

Cumulation

PRIMARY LOSS	
Minimum: \$4,250,000	
Most Likely: \$20,880,000	
Maximum: \$101,620,000	

The datapoints in all the four aspects of the Primary Loss Magnitude cumulates to a minimum of \$4.25M and a maximum of \$101.62M while the most likely loss would be around \$20.88M for each incident.

Risk Analysis: Social Engineering (S1)


Description

The Boutique Hospital, being a high standard organization, holds PHI information for higher class individuals and organizations. This database of information should not be anywhere near the reach of untrusted individuals. With social engineering, the attacker tries to manipulate employees who have authorization to this database into giving them access.

Loss Event Frequency Datapoints

Threat Events


As per the reports, the hospital has been getting constant probe alerts with a frequency of 2 social engineering attacks per week. Therefore, the most likely attack frequency would be 104 times per year. If the attackers decide to double their attack their frequency, the maximum attacks would be 208 times a year. However, if they initiate the attack one time per week on average, the attack frequency would still be 52 times a year.

THREAT EVENT FREQUENCY	
Minimum: 52	
Most Likely: 104	
Maximum: 208	
Confidence: Medium	

Vulnerabilities


Threat Capability

The capability of an attacker is mostly dependent on how smart and skillful the attacker is. As a high-class organization, we would not want to underestimate the skills of an attacker. The attacker, assuming would have good skills and resources, the minimum capability is input to 60%. If the highly skilled attacker with perfect charming abilities and communication skills decides to attack, we assume that there is a 99% chance that the attack is capable of a breach. For the sake of accuracy, we assume the most likely capability of the threat is somewhere around 85%.

THREAT CAPABILITY	
Minimum: 60%	
Most Likely: 85%	
Maximum: 99%	
Confidence: Medium	

Resistance

Contrary to the threat capability, the resistance strength represents the hospital's resistance to the threat. The control of resistance strength is entirely dependent on how much effort we have put into the organization's cyber-defense mechanism.

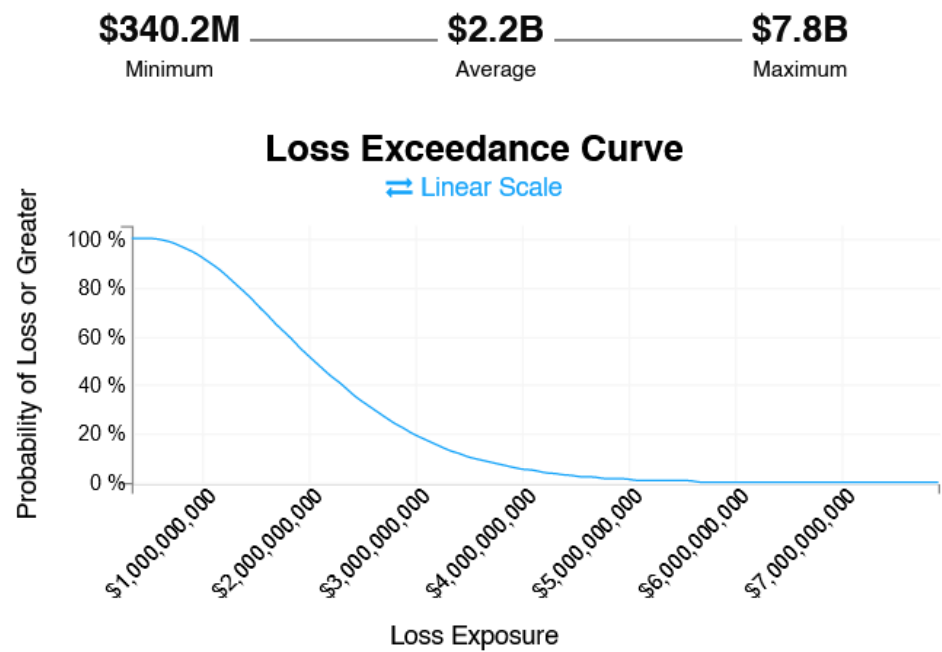
RESISTANCE STRENGTH	
Minimum: 25%	
Most Likely: 85%	
Maximum: 95%	
Confidence: Medium	

With the previous reports and security implementation, the above inputs have been decided. At least 25% of the employees have already been to SETA programs. Another factor that is considered while inputting these values is that more than 45% of the employees have been through a social engineering attack as most of the time, a dozen employees are being impacted. The previous year's security team implemented a multi-factor authentication to the database, which we consider a good technique to reduce the threat. But implementing this technique would not be enough if a highly authorized entity is compromised. Therefore, we input 85% resistance strength most likely with 25% of minimum strength.

Analysis Report

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario



With the current situation of social engineering attacks in the organization and without the control measures, the anticipated successful social engineering attacks would reach an average of 70.02 per year and could lead up to \$77.5M per event. If all these attacks are successful, the hospital will be facing an average of \$2.2B per year which could also reach up to \$7.8B per year.

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	33	70.02	125
Loss Magnitude	\$5.1M	\$31.5M	\$77.5M

Secondary

	Min	Avg	Max
Loss Events / Year	30	67.95	124
Loss Magnitude	\$0	\$0	\$0

Vulnerability

62.04%

With the current control measures, the organization is still 62.04% vulnerable to these attacks. These vulnerabilities lie within the hospital's employees and the security system.

Control Measures

SETA Program

Security Education Training Awareness program for the employees would be the key factor into increasing the hospital's resistance against social engineering attacks.

ID Verification

Verification could be of many means. The verification of Employee ID would not be enough. For authorized data access, a different encrypted verification form should be required.

Network Zoning

The access of a database should be allowed only for the devices within a certain network. The zoning of the network would be helpful in reducing the access to limited devices with certain mac addresses only.


Risk Analysis: Social Engineering After Implementation of Control Measures (S1a)

Description

After the implementation of control measures, some of the datapoints for resistance rises while the threat capability remains the same. This implementation suggests that the attacker's capability would remain the same with the same frequency of attempts, but the threat resistance of the hospital increases significantly.

Resistance Strength

In this case, the resistance strength goes significantly higher than the S1 scenario.

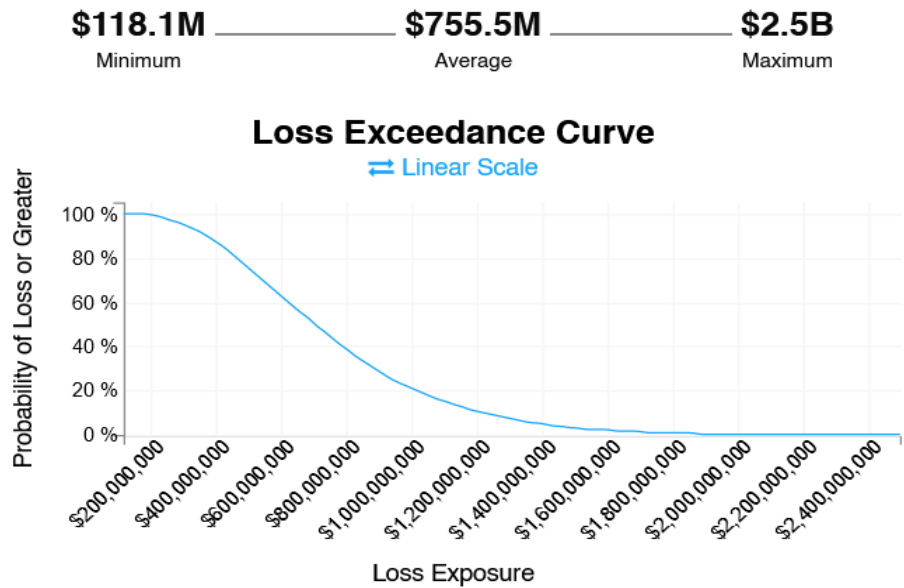
RESISTANCE STRENGTH	
Minimum: 75%	
Most Likely: 92%	
Maximum: 99%	
Confidence: Medium	

Since all the employees have been in a SETA program, the likelihood of them being compromised is significantly reduced so the most likely resistance increases. The minimum resistance is also increased to 75%, which would be the least resistance for every threat event.

Analysis Report

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario



With just three control measures adopted, the average loss exposure decreased from \$2.2B to \$755.5M. This is a significant drop of more than 70% of exposure. The maximum loss exposure would be \$2.5B which is around the average of the uncontrolled scenario.

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	11	23.91	43
Loss Magnitude	\$5.9M	\$31.6M	\$77.8M

Secondary

	Min	Avg	Max
Loss Events / Year	10	23.19	43
Loss Magnitude	\$0	\$0	\$0

Vulnerability

21.26%

With the Control measures in effect, the vulnerability decreases to 21.26%. The Average loss event per year also decreases to 23.91 with a maximum of 43 and a minimum of 11 per year. The

main target is to reduce the vulnerability which goes down from 62.04% to 21.26% with a difference of more than 40%. This is significantly lower and would help us get closer to our goal.

Risk Analysis: Phishing Attacks (S2)

Description

According to the reports, Phishing attack attempts are more frequent occurrences for the hospital. Being probed more than 2 times a day, the phishing attacks are also targeting high-authority individuals.

Current Security Measure

An Email Security protocol is implemented on the email server to hash out the potential spam and fraud emails which reduces the phishing attack.

Threat Event Frequency

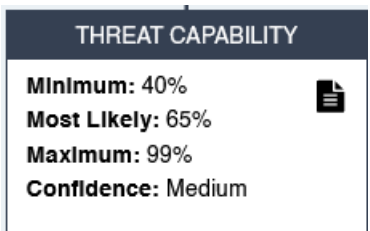


At this point, the number of phishing attacks are averaging 3 per day. With the security measure intact, the most likely events that employees have to deal with is calculated to 598 per year with a maximum of 1000 and a minimum of 200 phishing attacks. These are the events that the employees need to handle themselves.


Vulnerabilities

Threat Capability

Phishing attacks are coming through email more than any other platform. Since the previous control method is added, the threat capability would be a minimum of 40% and most likely at 65%. In case of a bad link click of an employee and a malware installation in our servers, things could take a turn and the assets could be 99% vulnerable.



Threat Resistance

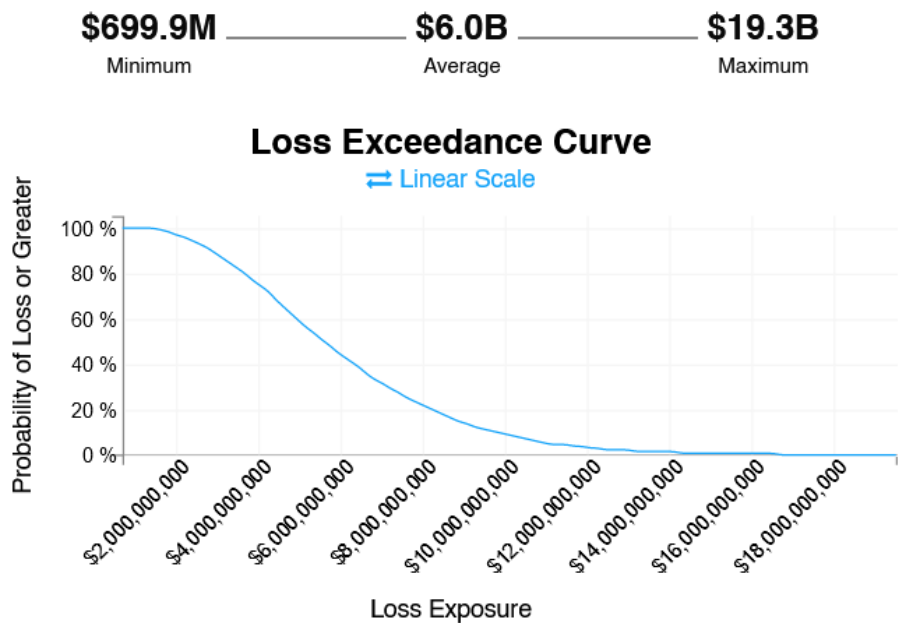
RESISTANCE STRENGTH	
Minimum: 60%	
Most Likely: 70%	
Maximum: 95%	
Confidence: Medium	

The Email servers have a high-level security protocol which directly removes junk and phishing attacks. Therefore, we have a higher resistance than the social engineering attacks. The most likely resistance is put at 70% by analyzing the previous reports and the attacks. There is always a residual risk for the integrity and accessibility of data which leaves 5% room over maximum resistance of 95%.

Analysis Report

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario



With the datapoints mentioned above, the Average Loss Exposure under the current security measures is still at \$6B with a maximum of \$19.3B and a minimum of \$699.9M per year.

Primary

	Min	Avg	Max
Loss Events / Year	70	190.76	316
Loss Magnitude	\$6.5M	\$31.5M	\$82.2M

Secondary

	Min	Avg	Max
Loss Events / Year	67	185.05	309
Loss Magnitude	\$0	\$0	\$0

Vulnerability

32.01%

The probability of successful attacks simulation brings the hospital at a loss magnitude of \$31.5M per event with an average of 190.76 successful attacks. The vulnerability rate is around 32%.

Control Measures

Update E-Mail Server Protocols

The already added security protocols need regular updates to add more email addresses and AI to detect potential phishing emails. These updates will be needed regularly.

SETA Program

As of the previous scenario, the SETA program also helps in raising awareness to the employees within the hospital. Phishing attacks are mostly successful due to human errors and lack of awareness. Therefore, this program will minimize the risk of a breach due to a human error.

Enforce SSL within the hospital network

Enforcing SSL certification to the websites will make sure that the untrusted sites are not available to access within the hospital network. This helps in reducing the attack through fake links which are sent in phishing emails.

Install Anti Phishing Software

Anti-Phishing software constantly scans all emails within the email server to remove the potential phishing emails.

Risk Analysis: Phishing Attacks After Implementation of Control Measures (S2a)

Resistance Strength

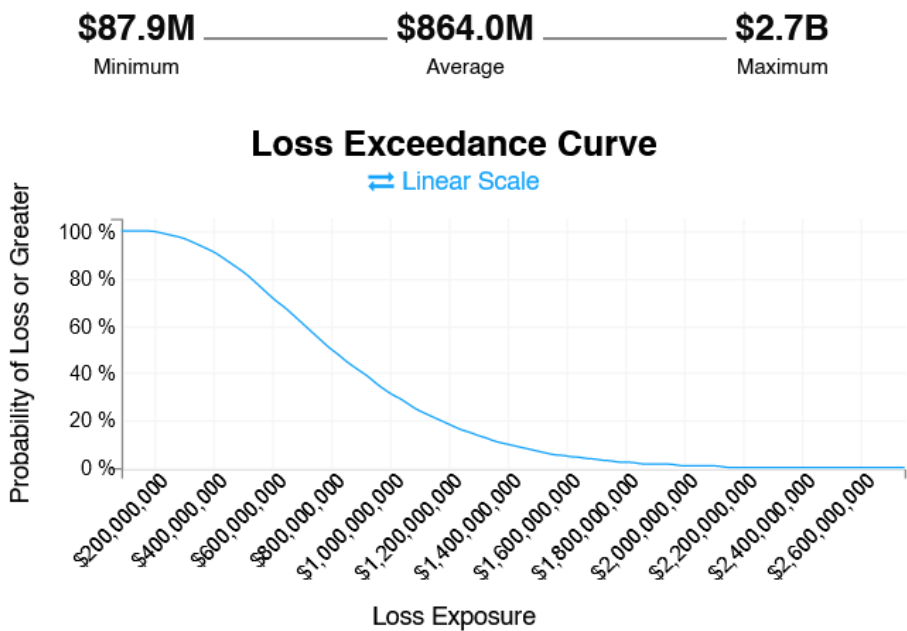
The resistance strength of the hospital significantly increases after implementation of the control measures. After the measures, the minimum resistance would reach 80% and the maximum to 97%. The resistance most likely would be at 85%.



Analysis Report

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario



The Annual Loss Exposure average significantly decrease after the implementation of control measures. The maximum exposure would reach \$2.7B and the minimum would be at \$87.9M. The average risk exposure would reach down to \$864M.

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	10	27.26	45
Loss Magnitude	\$5.9M	\$31.7M	\$80.1M

Secondary

	Min	Avg	Max
Loss Events / Year	9	26.44	45
Loss Magnitude	\$0	\$0	\$0

Vulnerability

4.54%

Even with the same frequency of attempts without controls, the loss magnitude would average to \$31.7M. The control measures decrease the vulnerability to 4.54% which is a reduction of around 28%.

Future Review

The analysis reports suggest a prominent level of difference between the scenarios with and without implementation of control measures. In the future, this process could be reviewed and analyzed again to implement more control measures according to the reports. The recommendation is to report every month to have a good understanding of where the organization stands to a security standpoint.