


A thick blue vertical bar runs down the left side of the slide. A blue arrow points to the right from the bar, containing the date.

10/4/2022

Social Engineering attack in Boutique Hospital

RA #2

Several thin, curved lines in blue and grey originate from the bottom left and sweep upwards and to the right.

Ninglekhu, Kendra B
CIS - 650

Overview

Boutique hospitals in Midwest is catering to numerous wealthy and famous individuals including politicians, business executives, and celebrities. The boutique hospital has a capacity for about 40 patients per week and provides various treatments with skilled specialist surgeons. Last year according to CISO, it was reported that the hospital was exploited through social engineering and phishing. The incidents were resolved using a trusted regional investigation firm and the was around 300,000 dollars with a minimum of 100,000 dollars and a maximum of 500,000 dollars. Due to the incident, the organization found itself in the middle of a class action suit and was listed on HHS's "wall of shame" which the executive board of directors thinks is disastrous to the organization for its reputation and legal risks. The organization has estimated that the cost for legal and reputational would be around 10,000,000 dollars, with a low of 2,000,000 dollars and a high of 50,000,000 dollars.

Different attacks on the hospital

There were two different attacks on the Boutique hospital. The first attack was a social engineer attacking the hospital worker to get them to share PHI information and the second was attack was tricking the hospital worker to click a fake link or opening an attachment of fake emails. These attacks were done on the targeted group of people.

Risk Analysis

The risk analysis was done using FAIR analysis to bring more detailed information on the damage done by the attacks on the Boutique hospital. To analyze the loss taken due to the attack and the magnitude of the attack, the tree diagram of FAIR analysis was used, and the values were added to the tree diagram.

The FAIR analysis has loss event frequency and loss magnitude

Loss event frequency contains

Threat event frequency – How many times over the next year is the threat event likely to occur? How many times will the asset face a threat action? [2]

Vulnerability – What percentage of threat events are likely to result in loss events? [2]

Loss magnitude contains

Primary loss – How much money are we likely to lose from each loss event? [2]

Secondary risk – How much loss will the organization likely experience because of secondary stakeholders' reactions to the primary loss event? [2]

Loss due to attacks

The attacks on the Boutique hospital have made a huge loss for the organization in resolving the issue and the damage following the attack, assuming the loss taken by the organization is the same in both of scenarios. The following loss is assumed for a monthly basis on average.

Primary loss

These are the loss taken by the organization on the bases that damage done by the social engineering attack is most likely \$1,918,666 with a low of \$1,128,500 and a high of \$3,629,666.

Secondary loss

These are the loss taken by the stakeholder of the organization after the social engineering attack. The secondary LEF confidence is medium, most likely 73% with a low of 60% and a high of 80% while secondary LM is most likely \$1,143,3000 with a low of \$544,500 and a high of \$5,938,660.

First Attack (Scenario 1)

Threat event frequency

The attack was done twice a week so regarding it monthly the most likely attack would be 8 ($2 * 4$) with a low of 4 and a high of 12.

Vulnerability

The threat capability is more than the resistance strength since most hospital workers are not equipped with the knowledge to protect themselves from social engineering attacks and security only works if any malicious threat is found. For this situation, the threat capability confidence is medium and most likely would be 65% with a low of 35% and a high of 99% while resistance strength confidence is medium and most likely would be 55% with a low of 25% and a high of 75%.

Based on the above FAIR analysis data the loss exceedance curve and simulation summary were created as shown in Fig 1 and Fig 1a.

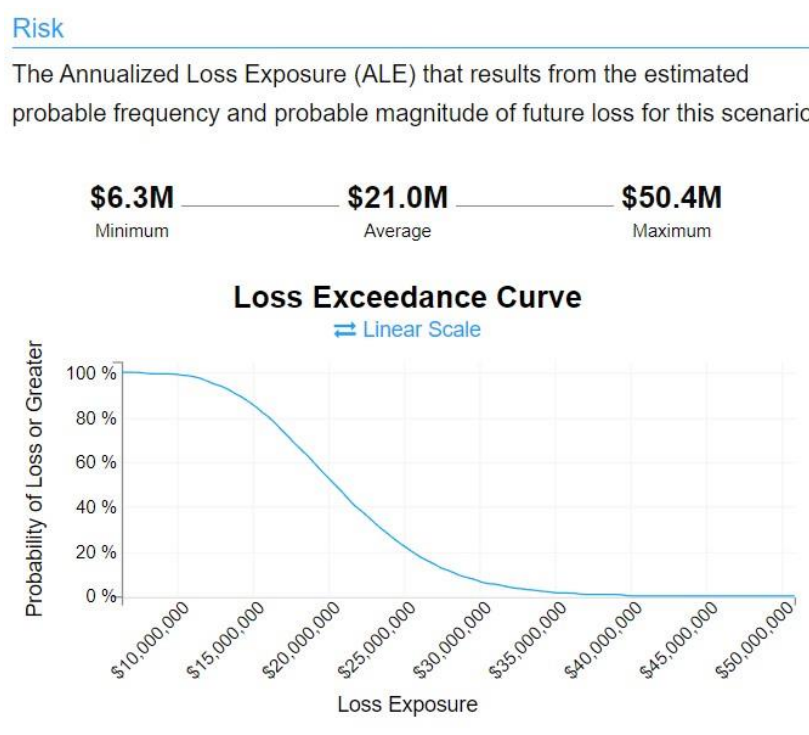


Fig 1.

Summary of Simulation Results



Primary

	Min	Avg	Max
Loss Events / Year	3	6.18	9
Loss Magnitude	\$1.4M	\$2.1M	\$2.9M

Secondary

	Min	Avg	Max
Loss Events / Year	0	4.45	9
Loss Magnitude	\$751.2k	\$1.8M	\$4.7M

Vulnerability

77.39%

Fig 1a.

Second Attack (Scenario 2)

Threat event frequency

The attack was done three times a day so regarding it monthly the most likely attack would be 12 (3 * 4) with a low of 6 and a high of 18. The probability of action such as clicking the fake links, assuming most likely would be 65% with a low of 35% and a high of 75%.

Vulnerability

The threat capability is more than the resistance strength since most hospital workers are not equipped with the knowledge to protect themselves from tempting fake links, and emails assuming the fake emails or link bypass the security of the hospital system. For this situation, the threat capability confidence is medium and most likely would be 65% with a low of 45% and a high of 99% while resistance strength confidence is medium and most likely would be 55% with a low of 35% and a high of 70%.

Based on the above FAIR analysis data the loss exceedance curve and simulation summary were created as shown in Fig 2 and Fig 2a.

Risk

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

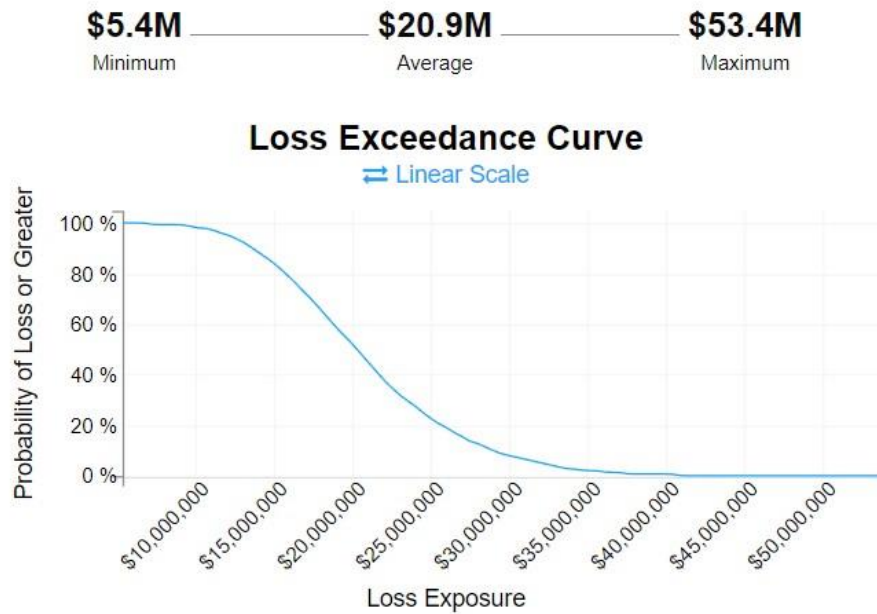


Fig 2.

Summary of Simulation Results



Primary

	Min	Avg	Max
Loss Events / Year	3	6.16	10
Loss Magnitude	\$1.4M	\$2.1M	\$3.0M

Secondary

	Min	Avg	Max
Loss Events / Year	0	4.42	9
Loss Magnitude	\$776.4k	\$1.8M	\$4.9M

Vulnerability

85.75%

Fig 2a.

Control Measures

SETA (Security Education Training and Awareness) program should be introduced for the social engineering and phishing attack for the Boutique Hospital. The SETA program educates and trains the hospital employees regarding the attacks, aware them regarding on the attack or suspicious calls, emails, links, and messages [1]. The SETA program is not enough as there is always a risk of employees falling for attacks so, different cybersecurity policies and procedures should be implemented to minimize the risks.

Some of the controls for the different attacks are as follows:

- Simulated Phishing Emails – This tool can be implemented as part of the SETA program to see from an organizational perspective who will fall victim to fake phishing attacks and who will avoid them. This will help to create a standard for security awareness for the organization and plan the program to train the employees accordingly. This can be used again after training the employees with the SETA program to see if the employees are able to avoid fake phishing attacks or not.
- Update cybersecurity awareness featuring phishing and social engineering attacks on a monthly basis – Focus on real-world examples of attacks to aware the employees of their dangers and threats.
- Multifactor authentication – Using this tool to user accounts can keep malicious threats from stealing the login and password credentials.
- Minimize the user account privileges – Limiting the effectiveness of attacks designed to steal account credentials that have minimum privileges to what they need so, even in the scenario of the attack being successful, no heavy damage is done.
- Regular updates and installation of security programs – Weekly updates and maintenance of the security software in the devices after installing it will help avoid suspicious emails, messages, and links and notify the employees regarding malicious threats present in them.

First attack with controls (Scenario 1a)

The scenario is based on the first attack on Boutique hospital so the data on FAIR analysis will remain the same for the threat event frequency. The vulnerability data will change due to the controls implemented for damage control.

Vulnerability

The resistance strength is more than the threat capability in this scenario. The hospital implemented controls against social engineering attacks and strong computer security in place to fight against such attacks. For this situation, resistance strength confidence is medium and most likely would be 75% with a low of 45% and a high of 90% while threat capability confidence is medium and 65% most likely with a low of 35% and a high of 99%.

Based on the above FAIR analysis data the loss exceedance curve and simulation summary were created as shown in Fig 3 and Fig 3a.

Risk

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

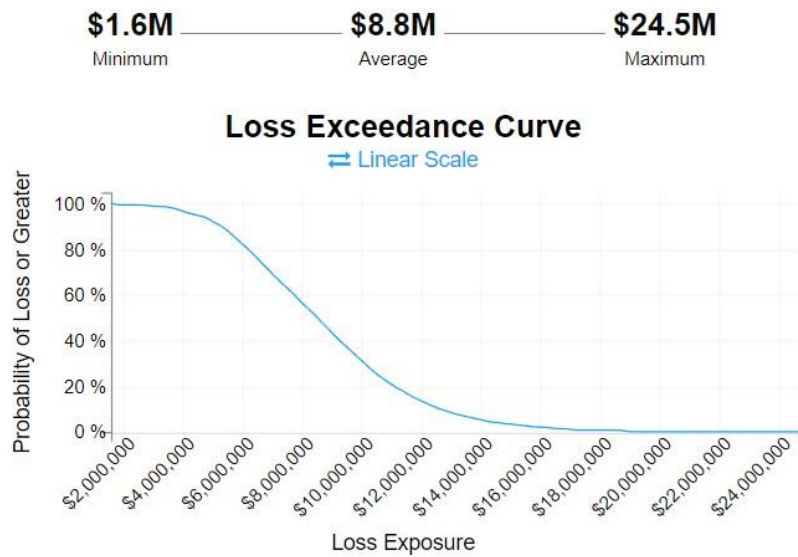


Fig 3.

Summary of Simulation Results



Primary

	Min	Avg	Max
Loss Events / Year	1	2.58	4
Loss Magnitude	\$1.4M	\$2.1M	\$3.0M

Secondary

	Min	Avg	Max
Loss Events / Year	0	1.86	4
Loss Magnitude	\$727.5k	\$1.8M	\$5.1M

Vulnerability

32.5%

Fig 3a.

Second attack with controls (Scenario 2a)

The scenario is based on the second attack on Boutique hospital so the data on FAIR analysis will remain the same for the threat event frequency. The vulnerability data will change due to the controls implemented for the prevention and safety of the attack.

Vulnerability

The resistance strength is more than the threat capability in this scenario. The hospital implemented controls against fake links, and emails attack, with strong computer security in place to fight against such attacks. For this situation, resistance strength confidence is medium and most likely would be 75% with a low of 45% and a high of 95% while threat capability confidence is medium and 65% most likely with a low of 35% and a high of 99%.

Based on the above FAIR analysis data the loss exceedance curve and simulation summary were created as shown in Fig 4 and Fig 4a.

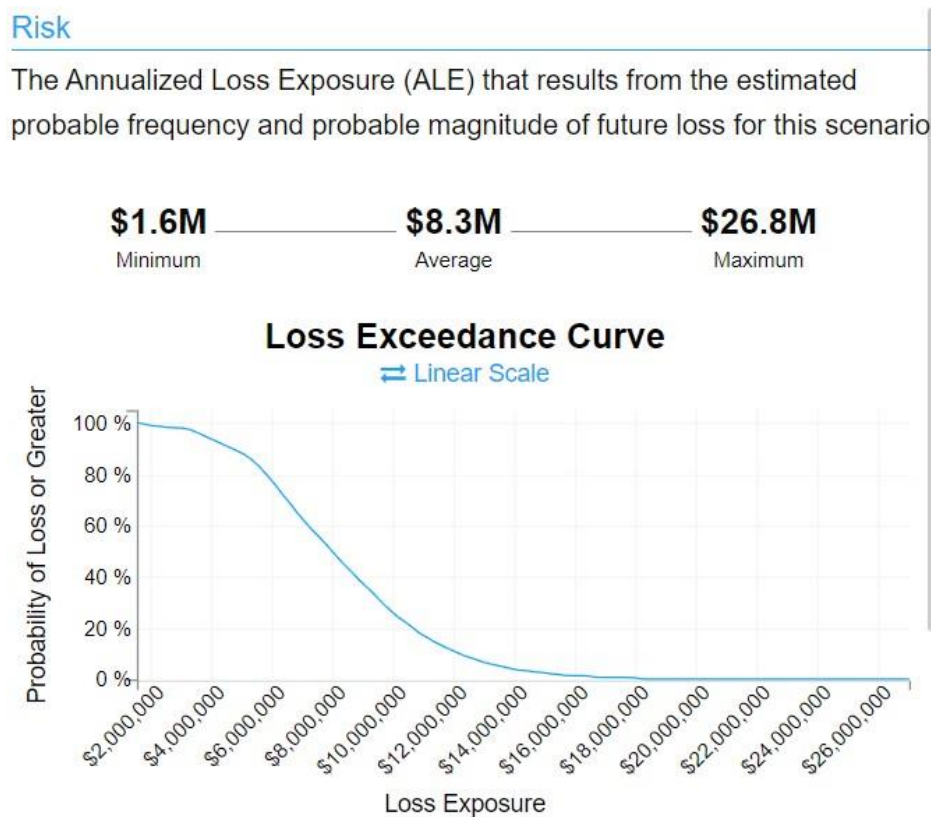


Fig 4.

Primary

	Min	Avg	Max
Loss Events / Year	1	2.43	4
Loss Magnitude	\$1.3M	\$2.1M	\$3.0M

Secondary

	Min	Avg	Max
Loss Events / Year	0	1.76	4
Loss Magnitude	\$687.4k	\$1.9M	\$4.8M

Vulnerability

32.72%

Fig 4a.

References

- [1] What is Phishing, and How Can SETA Programs Help? Retrieved October 10, 2022 from <https://www.compuquip.com/blog/seta-programs-and-phishing>
- [2] FAIR-U. Retrieved October 10, 2022 from <https://app.fairu.net/analysis/>