the Team of Company Risk Analyst Officer (CRAO)

Risk Assessment Report

Recommendation Letter for CEO

Dear Dr. Salma

On behalf of the staff and management of the Company Risk Analysis ,We want to thank you for entrusting us with your Risk Assessment for ABC company.

we are pleased today to present to you the complete findings of the assessment, along with the Recommended that are required for reduce risk. This report is divided into tow Scenario as follows:

Scope statement

Context-specific questions

Loss Event Frequency LEF : Threat event frequency Vulnerability

Loss magnitude estimations: primary loss and secondary loss

1. Introduction

In this report we perform risk analysis for two Scenario at ABC company in Jeddah is doing so many community service to help people in need who cannot afford medicines and other medical expenses These services acknowledge several times by governmental authorities and media through use FAIR tool to Inform CEO the best possible information about loss exposure and options for dealing with it .

The first Scenario is talking about beneficiaries Database in ABC company .The management is most concerned about data confidentiality, but in past years the attacker is breaching beneficiaries Database who benefit from the free medicines service the company provide.

The second Scenario is talking about physical security at the company's warehouse is a potential area of concern and protection it and preventing it from stealing from the warehouse by internal employees but were being stolen from competitors' warehouses by internal employees and also by organized criminals

we show in more details for two Scenario : how to estimate the risk by Loss event frequency by TEF and Vulnerability and loss magnitude by primary and secondary loss and we provide the results and Suggested controls to reduce risk.

2. First Scenario

Asset: Data of the beneficiaries in DB.

Threat community: cybercriminals

Threat type: malicious

Effect: confidentiality

Scope table

Asset at Risk	Threat community	Threat Type	Effect
Data of the beneficiaries in DB	cybercriminals	malicious	confidentiality

2.1 Context-specific questions:

Scope statement: Analyse the risk associated with malicious cybercriminals impacting the confidentiality of the beneficiaries data in DB via attacker.

Threat event frequency: Over the next year, how many times will malicious cybercriminals attempt to impact the confidentiality of the of the beneficiaries data in DB via attacker?

Secondary loss event frequency: What percentage of confidentiality impact of the beneficiaries data in DB via attacker by malicious cybercriminals will result in further loss from the reactions of secondary stakeholders?

Vulnerability: Of the attempts over the next year by malicious cybercriminals to impact the confidentiality of the beneficiaries data in DB via attacker, what percent will be successful?

Threat Profile :

Cybercriminals : any group of criminal enterprises or loosely organized criminals. They are reasonably well-funded but not as well as a nation state.

Factor	Value
Motive	Financial
Primary intent	Engage in activities legal or illegal to maximize their profit.
Sponsorship	Non-state sponsored or recognized organizations (illegal organizations or gangs). The organization, however, does sponsor the illicit activities.
Preferred general target characteristics	Easy financial gains via remote means; prefer electronic cash transmission over physical crimes involving cards. Needs money mules or other intermediary to shield them from reversed transactions.
Preferred targets	Financial services and retail organizations.
Capability	Professional hackers. Well-funded, trained, and skilled. May employ relatively desperate actors with or without native skillsets.
Personal risk tolerance	Relatively high (criminal activities); however, willing to abandon efforts that might expose them.
Concern for collateral damage	Not interested in activities that expose themselves or others from their organization. Prefer to keep their identities hidden

2.2 Analysis

(a) Loss Event Frequency LEF

We will estimate the LEF indirectly form Threat Event Frequency TEF and Vulnerability

OR [depends on your readings of the provided data]

(a.1) Threat Event Frequency TEF

Min: 0

Max: 12

ML: 1

We assume the value of min and max and ml From (They further estimate that most likely 1 out of 12 attacks can overcome the security control and successfully access the beneficiaries DB) .

however, the most likely is 1 and the value of the maximum 12 , from the range between 1 to 12 , we assume the minimum is 0

Confidence level: High

Rational (how did you reach the above estimate and confidence level):

high, since multiple teams have found and corroborated with hard data.

(a.2) Vulnerability

We assume the value of min and max and ml From (They further estimate that most likely 1 out of 12 attacks can overcome the security control and successfully access the beneficiaries DB)

we estimate the vulnerability from(the number of attack can be occur successfully Dividing on the sum number of the attack can be occure, then the value of most likely is 1/12 = 8.3 %

Min: 0%

Max: 16%

ML: 8.3%

Confidence level: low.

Rational (how did you reach the above estimate and confidence level):

low since the appears to be well-informed conjecture but with hard evidence offered

. **(b) Secondary Loss event frequency SLEF**

Min: 80%

Max: 100%

ML: 95%

Confidence level :high

Rational (how did you reach the above estimate and confidence level):

……

(c) Loss magnitude estimations

First: primary losses

[1-Provide a different table for each different primary loss type, 2- for each min, max, most likely, and confidence, provide a rational (how did you reach the estimates and confidence level)]

we estimate the value of primary respons to

- **internal investigation team** from (The local database security team will also investigate the issue using internal security tool such as Wireshark. Around 5 to 8 team members will work on it that will cost a fixed amount of $200 per worker) then the value of

min = 5 * 200 = 1000

ml= 6* 200 = 1200

max= 8 * 200= 1600

- **External incident response from (**Based on the previous company's record, the attack on beneficiary database requires a third-party investigation team to collect evidences and resolve the issue. The average cost is $30,000 to pay to the investigation team.)

We assume the ml is 30,000

Primary response	Min	Ml	max	Confidence
Primary response; internal investigation team	1000$	1200$	1600$	high
External incident response	10,000	30,000	50,000	low
Total	11000$	31200$	51600	meduim

Second: secondary losses

[1-Provide a different table for each different secondary loss type, 2- for each min, max, most likely, and confidence, provide a rational (how did you reach the estimates and confidence level)]

we estimate the value of secondary response to

- **Notify the beneficiaries from** (The company has to notify the beneficiaries and GAZT about the event, which can cost maximum $10,000) then the value of Max is 10,000$ and we assume the ml is 5000 and min is 1000

Secondary response	Min	Ml	max	Confidence
Notify the beneficiaries	1000$	5000$	10,000$	medium
Total	1000$	5000$	10,000$	medium

---

we estimate the value of secondary reputation to

- **Reduce stock price from** (Due to TCP/UDP ports attack, the beneficiaries information might be revealed which could affect the confidentially of data. With this fact, their reputation in front of citizen and GAZT might be affected. Based on the discussion, in this event, the stock prices in the share market can reduce and loss up to 20,000$.) then the value of Max is 20,000$ and we assume the ml is 15000 and min is 5000
- **Reduce market share(lost market retailer from(**It can further create a situation where up to 50 market retailer can shift to other company due to reputation damage. Each retailer shift can cause $20,000 business loss to the ABC Company) then the value of

Max is 50 * 20,000 = 1000000

Ml= 20*20,000= 400000

Min= 10 * 20000=200000

Secondary reputation	Min	Ml	max	Confidence
Reduce stock price	5000$	15,000$	20,000$	medium
Reduce market share(lost market retailer)	200000$	40,0000$	1000000	high
Total	205.000	415.000	1020.000	medium

we estimate the value of secondary fines and judgements to

- **Fines by lawsuits** due to DB From (legal department has shown that fines by lawsuits due to DB breach can cause loss of $50,000 to $80,000.)

Min= 50,000

Ml= 65.000

Max=80.000

- **To pay to the regulatory agency** From (In both cases (warehouse incident or beneficiaries data lost) the company has to pay to the regulatory agency from $50,000 to $100,000)

then the value of max is 100,000 and the value of min= 50,000 and we assume of ml is value between 50,000 to 100,000 is 80.000

Secondary fines and judgements	Min	Ml	max	Confidence
fines by lawsuits	50,000	65,000	80,000	High
To pay to the regulatory agency	50,000$	80,000$	100,000$	medium
Total	100,000	145,000	180,000	medium

2.3 FAIR-U tool

[Insert a snapshot of the FAIR ontology after inserting the relevant estimations]

Scope Inputs

Analysis Scope

A description of the asset, threat, and effect related to the scenario being analyzed. A well-defined scope is essential to accurate analysis.

Analysis Purpose

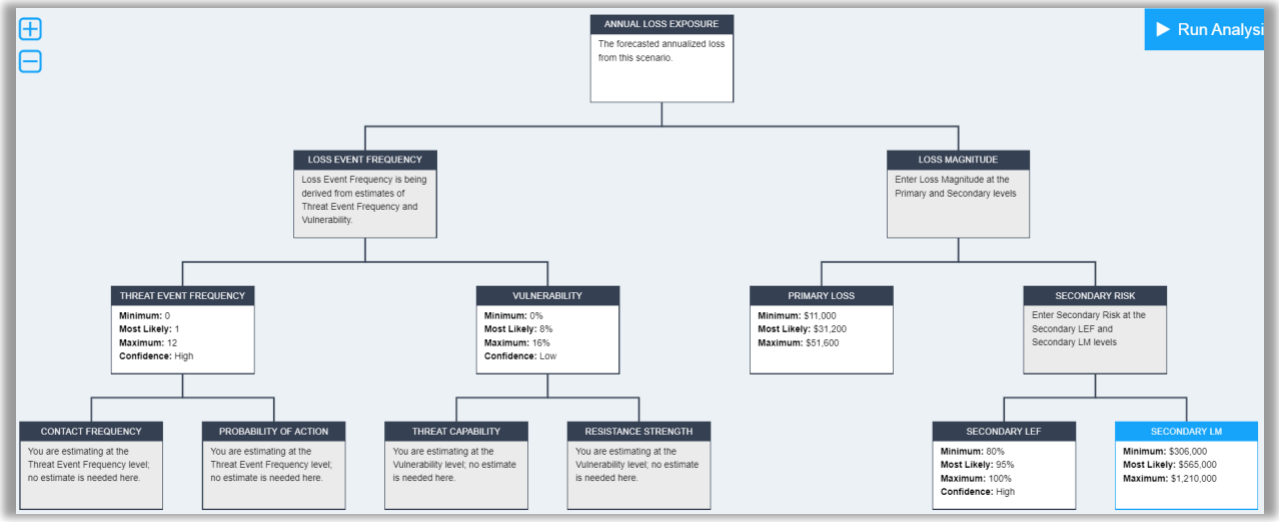
Analyze the risk associated with malicious cybercriminals impacting the confidentiality of the beneficiaries data in DB via

Asset(s)

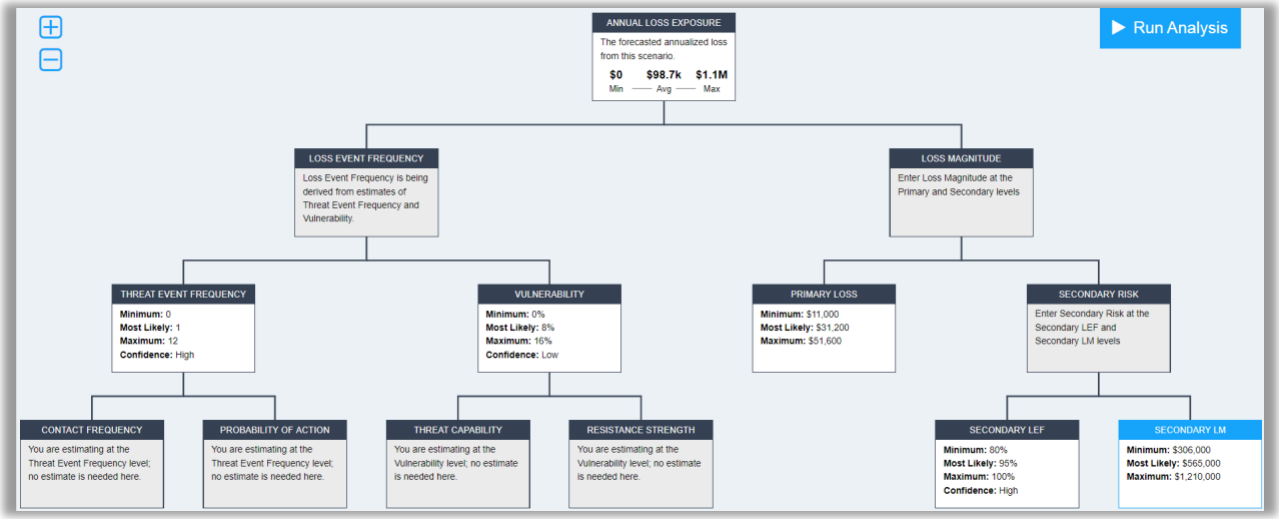
Data of the beneficiaries in DB

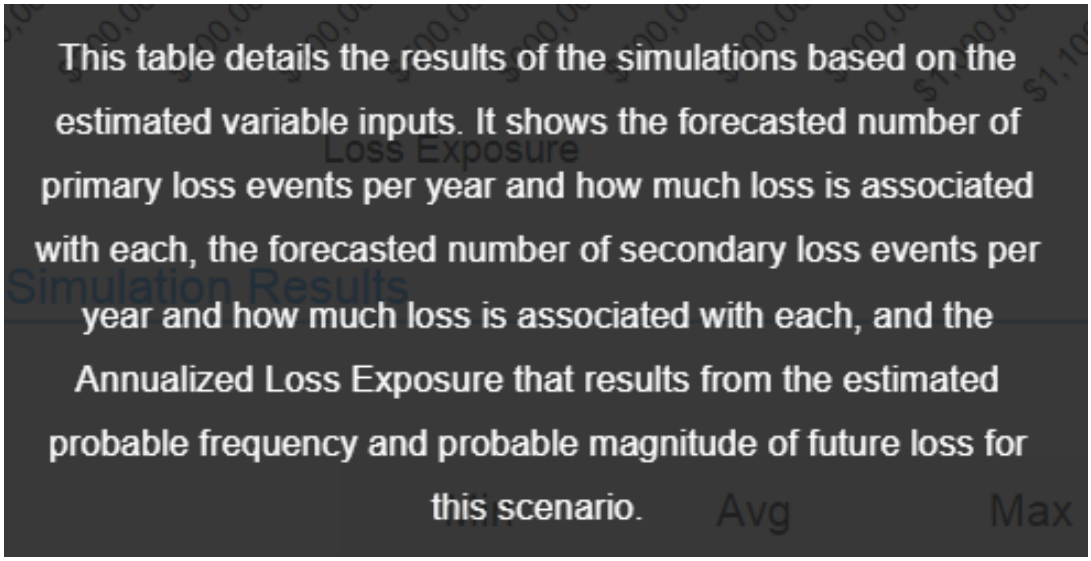
Threat Actor(s)

malicious cybercriminals



[Insert a snapshot of primary, secondary, and total loss exposure results]





Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.16	1
Loss Magnitude	$12.0k	$31.3k	$50.3k

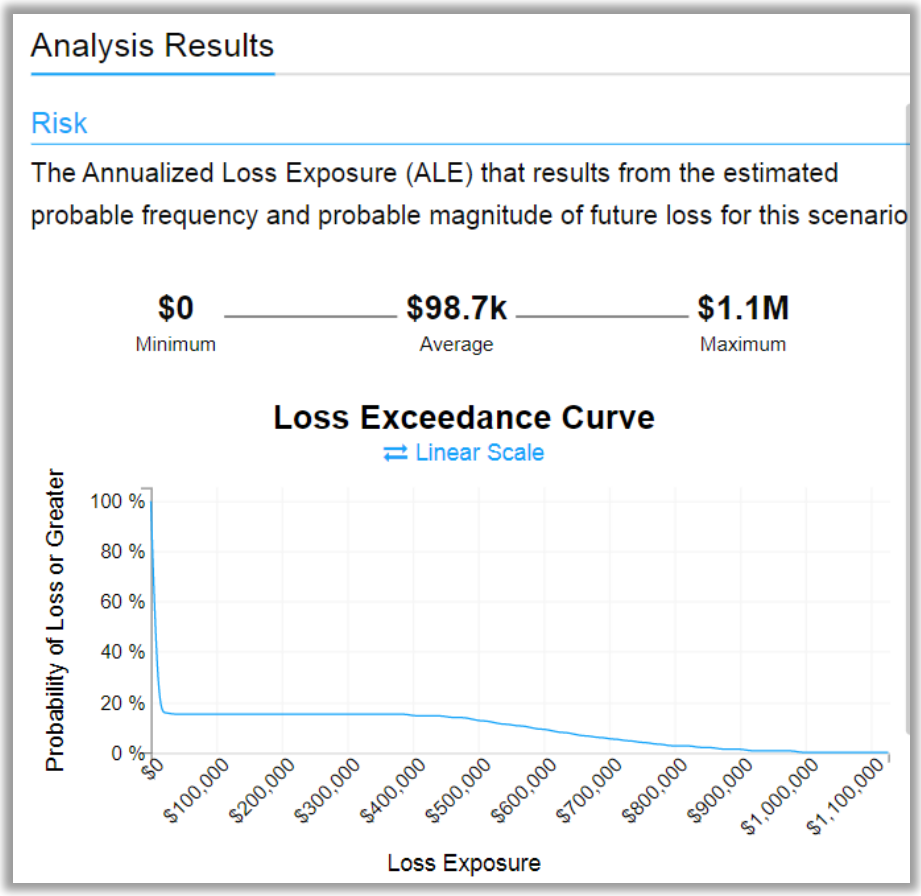
Secondary

	Min	Avg	Max
Loss Events / Year	0	0.15	1
Loss Magnitude	$335.2k	$632.3k	$1.1M

Vulnerability

7.85%

[Insert the loss Exceedance Curve]



2.4 Analyzing results

The risk annualized loss exposure (ALE) the minimum will be happened $ 0 and the average will be happened up to $98.7K and the maximum is$ 1.1M and **Vulnerability=7.85**

- we estimate the minimum loss exposure from **minimum value of primary +minimum value of secondary:**

the value primary of minimum loss events/year is 0 X of the minimum value of loss magnitude is 12.0 then add to the minimum value secondary of loss events/year is 0 X of the minimum value of loss magnitude is 335.2 =0

ALE min= (0 X 12.0 + 0 X 335.2 = 0)

- We estimate the average loss exposure from **average value of primary +average value of secondary:**

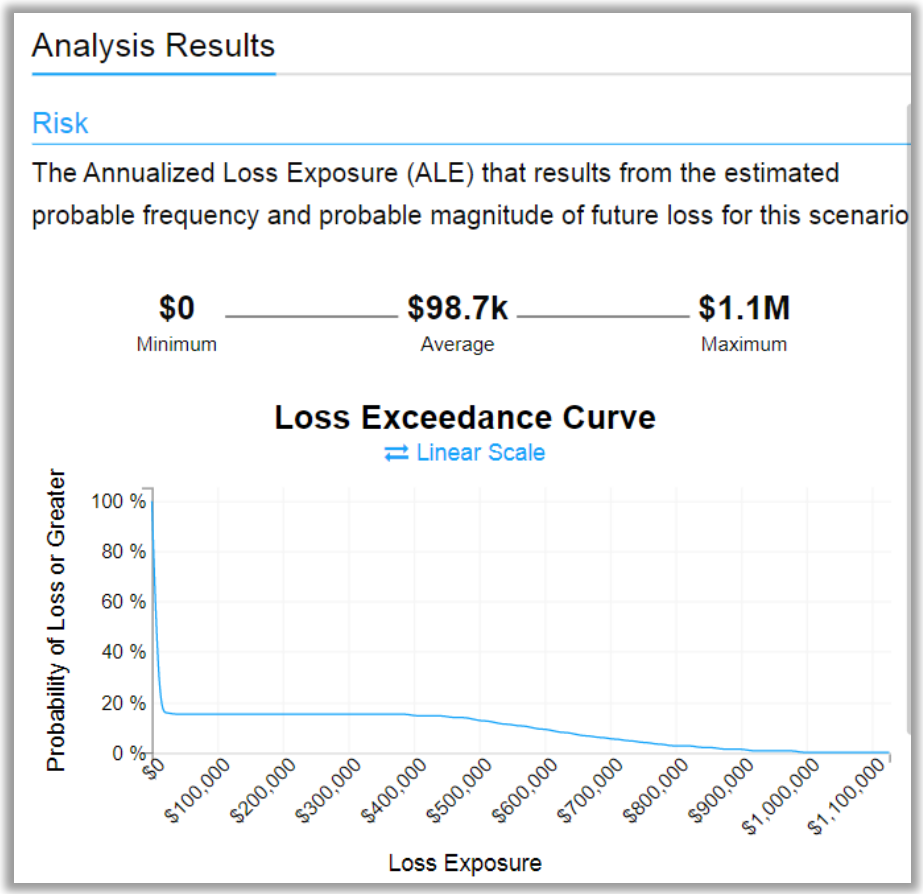
the value primary of average loss events/year is 0.16 **X** of the average value of loss magnitude is 31.3 then add to the average value secondary of loss events/year is 0.15 **X** of the average value of loss magnitude is 632.3 =

ALE average= **(0.16 X 31.3 + 0.15 X 632.3)= $99**

- We estimate the maximum loss exposure from **maximum value of primary +maximum value of secondary:**

the value primary of maximum loss events/year is 1 **X** of the maximum value of loss magnitude is 50.3 then add to the maximum value secondary of loss events/year is 1 **X** of the maximum value of loss magnitude is 1000000 =

ALE maximum = (1X50.3 +1 X100000000)= $10000050



- **The probability 90% no loss at all based on monte carlo**
- **When The probability is1% the loss exposure is Decreasing**
- **The probability 20 %is less than $100000**

2.5 Suggested controls

we is suggestion of security controls from "NIST SP 800-53, Recommended:

- **System and Communication Protection**(Technical): through provide a high degree of security in the DB of company by providing antivirus programs such as the trend micro and firewall
- **Audit and Accountability(Technical) :**Include accountability, showing who has accessed data, when and from which device
- **Access control(Technical):** The protection DB from unathorization access
- **Contingency Planning (Operational):**Provide daily backup copies of information that stored in DB

Also we is suggestion of containment Response controls:

- Use IDS and NIPS device deploy on the ontology network to detect and prevent any malicious traffic.

- Blocking an attacker's IP address after they' d already breached the network (contact)

- Use encryption of data when it is storing in DB and also transmission

we is suggesting of minimization controls

- Limiting negative secondary stakeholder reactions through data monitoring for the beneficiaries whose information was compromised.

Based on effectiveness of the control's (effect reduction in vulnerability and reduction in threat event frequency and reduction in loss magnitude)and priority for ABC company. We Recommended the following:

- Use IDS and NIPS device deploy on the ontology network to detect and prevent any malicious traffic.

- Blocking an attacker's IP address after they' d already breached the network (contact)

- Use encryption of data when it is storing in DB and also transmission

3. Second Scenario

Asset: Medicines stealing via warehouse

Threat community: privileged insiders

Threat type: malicious

Effect: availability

Scope table

Asset	Threat community	Threat type	Effect
Medicines stealing via warehouse	privileged insiders (employees)	malicious	availability
Medicines stealing via warehouse	privileged insiders (employees)	Human error	availability
Medicines stealing via warehouse	privileged insiders (Suppliers)	Human error	availability

3.1 Context-specific questions:

Scope statement: Analyze the risk associated with malicious privileged insiders impacting the availability of the Medicines stealing via warehouse

Threat event frequency: Over the next year, how many times will malicious privileged insiders attempt to impact the of the availability of the Medicines stealing via warehouse?

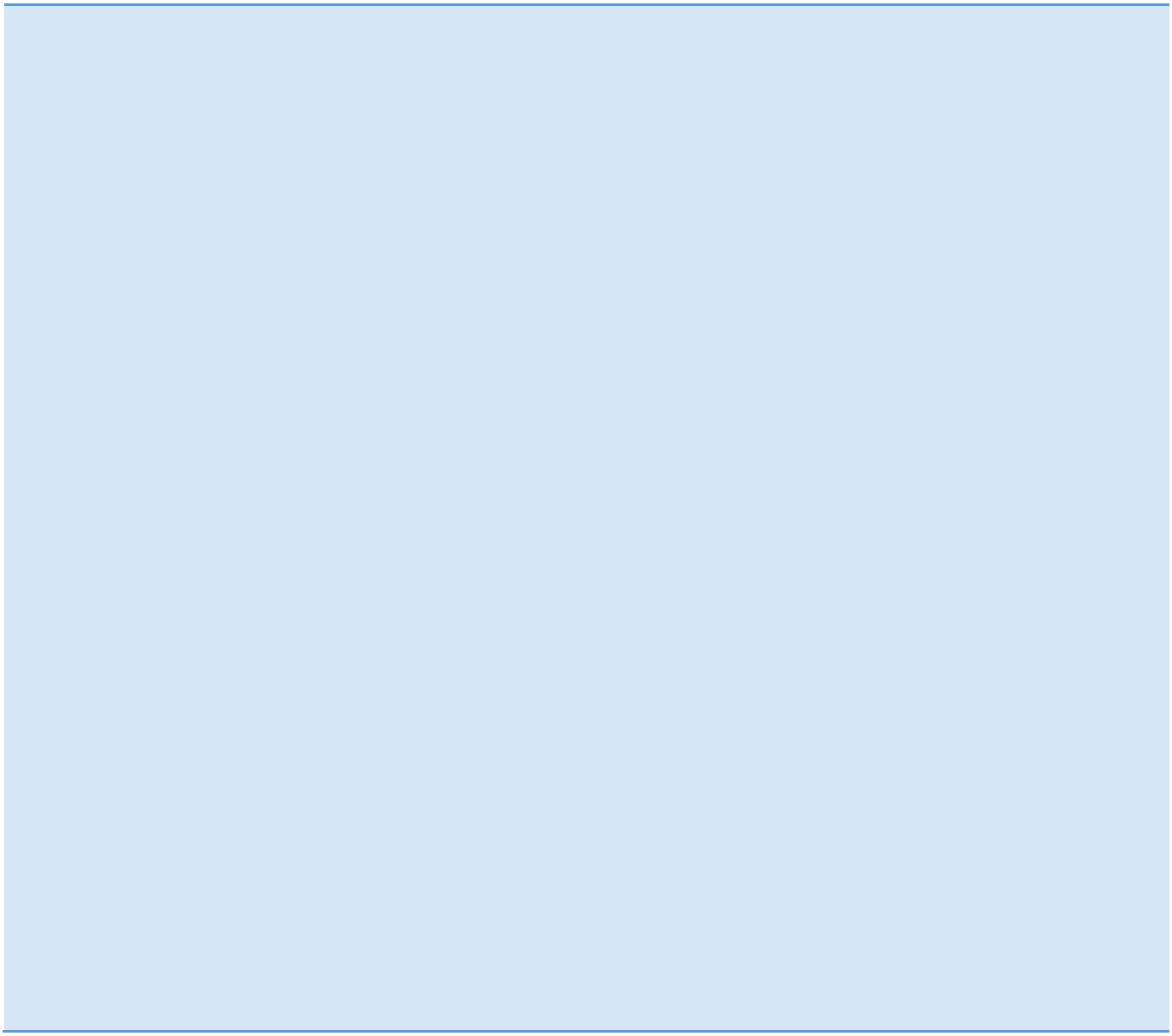
Secondary loss event frequency: What percentage of availability impact of the Medicines stealing via warehouse by malicious privileged insiders ,will result in further loss from the reactions of secondary stakeholders?

Vulnerability: Of the attempts over the next year by malicious privileged insiders to impact the availability of the Medicines stealing via warehouse, what percent will be successful?

Threat Profile

privileged insiders is those with specific access levels, knowledge, or otherwise some other privilege which enables them to overcome any controls and cause harm.

factor	value
Motive	Vindictive or personal gain. These tend to be loyal, trusted employees who go bad in extreme conditions. مكاسب انتقامية أو شخصية. يميل هؤلاء إلى أن يكونوا موظفين مخلصين وموثوق بهم ويتعرضون للسوء في الظروف القاسية
Primary intent	Gain retribution for perceived wrongs or to acquire money for alleviating a personal stressor. كسب الانتقام من الأخطاء المتصورة أو للحصول على المال للتخفيف من ضغوط شخصية
Sponsorship	None. In rare cases, there is collusion between various bad actors, however, most are lone wolves. لا شيء. في حالات نادرة ، هناك تواطؤ بين مختلف الفاعلين السيئين ، ومع ذلك ، فإن معظمهم من الذئاب المنفردة.
Preferred general target characteristics	Easy yet hidden financial gains or high profile targets that offer vindication for the attacker. مكاسب مالية سهلة ومخفية أو أهداف بارزة تقدم تبرئة للمهاجم.
Preferred targets	Prefer to attack targets to which the attacker already has access. يفضل مهاجمة الأهداف التي يستطيع المهاجم الوصول إليها بالفعل
Capability	varies. Tends to be very well versed in the systems to which they have access. Could have very high general com- puter science skills, yet may not be well-skilled in hacking. يختلف. يميلون إلى أن يكونوا على دراية جيدة بالأنظمة التي يمكنهم الوصول إليها. يمكن أن يتمتع بمهارات عالية جدًا في علوم الكمبيوتر ، ومع ذلك قد لا يكون ماهرًا في القرصنة
Personal risk tolerance	Very low. Attacker typically pressured into scenario that com- pels them to act (backed into a corner). This could be work related pressure such as a layoff, demotion, or a personal pressure, such as an illness in the family or personal financial stress. منخفظ جدا. وعادةً ما يتم الضغط على المهاجم في سيناريو يدفعه إلى التصرف (في الزاوية). قد يكون هذا ضغطًا متعلقًا بالعمل مثل التسريح من العمل أو خفض الرتبة أو الضغط الشخصي ، مثل مرض في الأسرة أو ضغوط مالية شخصية
Concern for collateral damage	In highly cohesivė groups, there is very little tolerance for collateral damage, except in cases where the attacker feels wronged by the group. في المجموعات شديدة التماسك ، هناك القليل جدًا من التسامح مع الأضرار الجانبية ، باستثناء الحالات التي يشعر فيها المهاجم بالظلم من قبل المجموعة.



3.2 Analysis

(a) Loss Event Frequency LEF

We will estimate the LEF directly form (Medicines from the company warehouse have been stolen twice in past 5 years)

we assume the value of ml is

A most likely of one primary loss event every five years (2/5)= 0.4

Min: 0.1

Max:0.8

ML:0.4

Confidence level: medium.

Rational (how did you reach the above estimate and confidence level):

medium, since multiple teams have found and corroborated with hard data.

OR [depends on your readings of the provided data]

(a.1) Threat Event Frequency TEF

Min: ……..

Max: ……..

ML: ……..

Confidence level: ……..

Rational (how did you reach the above estimate and confidence level):

……

(a.2) Vulnerability

Min: ……..

Max: ……..

ML: ……..

Confidence level: ……..

Rational (how did you reach the above estimate and confidence level):

(b) Secondary Loss event frequency SLEF

Min: 80%

Max: 100%

ML: 95%

Confidence level: ……..

Rational (how did you reach the above estimate and confidence level):

……

(c) Loss magnitude estimations

First: primary losses

[1-Provide a different table for each different primary loss type, 2- for each min, max, most likely, and confidence, provide a rational (how did you reach the estimates and confidence level)]

we estimate the value of primary response to

- **Internal** Incident response investigating from (In the event of stealing incidents at the warehouse, a physical security team is likely to work on investigating the event to assist police and other law enforcement agencies. 3 to 6 team members will need 10 to 15 hours of work at a rate of $50/hr.) then the value of

min = 3 *10 *50= 1500

ml= 4*13*50=2600

max= 6*15*50=4500

- **Notified about possible in shipping medicines from(**Usually, as a results of stealing medicines from the warehouse, there will be a shortage of medicines and retailors has to be notified about a possible delay in shipping medicines due to availability issue. The notification cost is on average $8,000.**)**

We assume the ml is 8000

Min= 5000

Max=13,000

Primary response	Min	Ml	max	Confidence
Incident response	1500	2600	4500	high
Notified about possible in shipping medicines	5000	8000	13,000	low
Total	6500	10600	17,500	medium

- **from(**During the last two events of stolen medicines, the company has to close all doors (entry and exit points) during the investigation period. The company data shows that in time of incident, the warehouse closed for 10 to 15 hours which affects productivity as possible delay in supplying medicines to the market, which recorded up to 50,000$ loss . In addition, almost 150 employees are working on the warehouse building involve in different department such as account, shipment, payment, and administration. The outage period will not allow them to continue their work. Their per hour wage cost 60$.**)**
- **من (خلال الحدثين الأخيرين للأدوية المسروقة ، يتعين على الشركة إغلاق جميع الأبواب (نقاط الدخول والخروج) خلال فترة التحقيق. تظهر بيانات الشركة أنه في وقت الحادث ، تم إغلاق المستودع لمدة 10 إلى 15 ساعة مما يؤثر على إنتاجية تأخير ممكن في توريد الأدوية للسوق ، والذي سجل خسارة تصل إلى 50000 دولار.بالإضافة إلى ذلك ، يعمل ما يقرب من 150 موظفًا في مبنى المستودعات في أقسام مختلفة مثل الحساب والشحن والدفع والإدارة. وستكون فترة الانقطاع لا تسمح لهم بمواصلة عملهم ، فأجرهم في الساعة يكلف 60 دولارًا)**

we estimate the value of primary productivity to نحن نقدر قيمة الإنتاجية الأولية ل

- **Loss revenue** (possible delay in supplying medicines to the market
- **خسارة الإيرادات (تأخير محتمل في توفير الأدوية للسوق**

Min:10,000

ML:30,000

Max:50,000

- **Loss wages**

Min= 150*10*60=90,000

Ml= 150*13*60=117,000

Max=150*15*60=135,000

Primary productivity	Min	Ml	max	Confidence
Loss revenue (possible delay in supplying medicines to the market خسارة الإيرادات (تأخير محتمل في توريد الأدوية إلى السوق	10000$	30000$	50000$	medium
Loss wages أجور الخسار	90,000$	117000$	135000	high
Total	100000$	147000	185000	high

Second: secondary losses

[1-Provide a different table for each different secondary loss type, 2- for each min, max, most likely, and confidence, provide a rational (how did you reach the estimates and confidence level)]

ثانياً: الخسائر الثانوية

[1 - قدم جدولًا مختلفًا لكل نوع خسارة ثانوي مختلف ، 2- لكل دقيقة ، والحد الأقصى ، والأرجح ، والثقة ، قدم سببًا منطقيًا (كيف وصلت إلى التقديرات ومستوى الثقة)]

we estimate the value of Secondary response to

- **extra working hours** from their suppliers from (Due to the outage of warehouse, the company requires extra working hours from their suppliers to overcome the shortage of medicine in the market. 2 to 5 teams of suppliers (each team will consist on 3 employees; a driver, a loader, a manager) will work over time for most likely 1 week, whereas per day the company will pay them 200$.)
- نحن نقدر قيمة الاستجابة الثانوية ل
- • ساعات عمل إضافية من مورديهم من (بسبب انقطاع المستودعات ، تطلب الشركة ساعات عمل إضافية من مورديها للتغلب على نقص الأدوية في السوق .2 إلى 5 فرق من الموردين (سيتألف كل فريق من 3 موظفين ؛ سائق أو محمل أو مدير) سيعمل بمرور الوقت على الأرجح لمدة أسبوع واحد ، بينما ستدفع لهم الشركة 200 دولار يوميًا.)

min= 2*200*7=2800$

Ml=3*200*7= 4200$

Max=5*200*7=7000$

- **call back From** (Usually, as a results of stealing medicines from the warehouse, there will be a shortage of medicines and retailors has to be notified about a possible delay in shipping medicines due to availability issue. The notification cost is on average $8,000. Whereas, call back and forth can further cost up to $5,000.)
- • معاودة الاتصال من (عادة ، كنتيجة لسرقة الأدوية من المستودع ، سيكون هناك نقص في الأدوية ويجب إخطار البائعين بالتأخير المحتمل في شحن الأدوية بسبب مشكلة توفرها. تبلغ تكلفة الإخطار في المتوسط 8000 دولار. حيث يمكن أن تصل تكلفة الاتصال مرة أخرى إلى 5000 دولار.)

We assume the max= 5000 and ml 3000 and min =0 نفترض أن الحد الأقصى = 5000 و مل 3000 و الحد الأدنى = 0

Secondary response	Min	Ml	max	Confidence
extra working hours from their suppliers	2800	4200	7000	high
call back	0	3000	5000	medium
Total	2800	7200	12000	medium

---

we estimate the value of Secondary response to Fines and judgements

- **Fines by HR** (In the past incidents on the warehouse medicines, the company HR department fines on average $2000 to the warehouse department.)
- نحن نقدر قيمة الاستجابة الثانوية للغرامات والأحكام
- - غرامات الموارد البشرية (في الحوادث السابقة على أدوية المستودعات ، غرامات قسم الموارد البشرية بالشركة في المتوسط 2000 دولار لقسم المستودعات.)

Min=800

Ml= 2000

Max=5000

- **From In both cases** (warehouse incident or beneficiaries data lost) the company has to pay to the regulatory agency from $50,000 to $100,000.
- في كلتا الحالتين (حادث مستودع أو فقدان بيانات المستفيدين) يتعين على الشركة أن تدفع للهيئة التنظيمية من 50.000 دولار إلى 100.000 دولار

Secondary Fines and judgement	Min	Ml	max	Confidence
Fines by HR الغرامات من قبل الموارد البشرية	800	2000	5000	medium
fines by lawsuits الغرامات عن طريق الدعاوى القضائية	50,000	60,000	100,000	medium
Total	50,800	62000	105,000	medium

---

we estimate the value of Secondary reputation

- **Stock price** From (In the event of the warehouse shutting down due to physical security incident, if the news goes out to the market, it will definitely create many questions on the company. The company records say that it will cost average $100,000 reduction in stock price due to reputation damage.)
- نحن نقدر قيمة السمعة الثانوية
- • سعر السهم من (في حالة إغلاق المستودع بسبب حادث أمان مادي ، إذا خرجت الأخبار إلى السوق ، فمن المؤكد أنها ستخلق العديد من الأسئلة حول الشركة. تقول سجلات الشركة أنها ستتكلف في المتوسط 100000 دولار في التخفيض سعر السهم بسبب تلف السمعة.)

we assume the ml=100,000 and min=50,000 and max= 200,000

نفترض أن ml = 100،000 و min = 50،000 و max = 200،000

Secondary reputation	Min	Ml	max	Confidence
Stock price سعر السهم	50,000	100,000	200,000	medium
Total	50,000	100,000	200,000	medium

3.3 FAIR-U tool

[Insert a snapshot of the FAIR ontology after inserting the relevant estimations]

Scope Inputs

effect related to the scenario being analyzed. A well-defined scope is essential to accurate analysis.

Analysis Purpose

Analyze the risk associated with malicious privileged insiders impacting the availability of the Medicines stealing via warehouse

Asset(s)

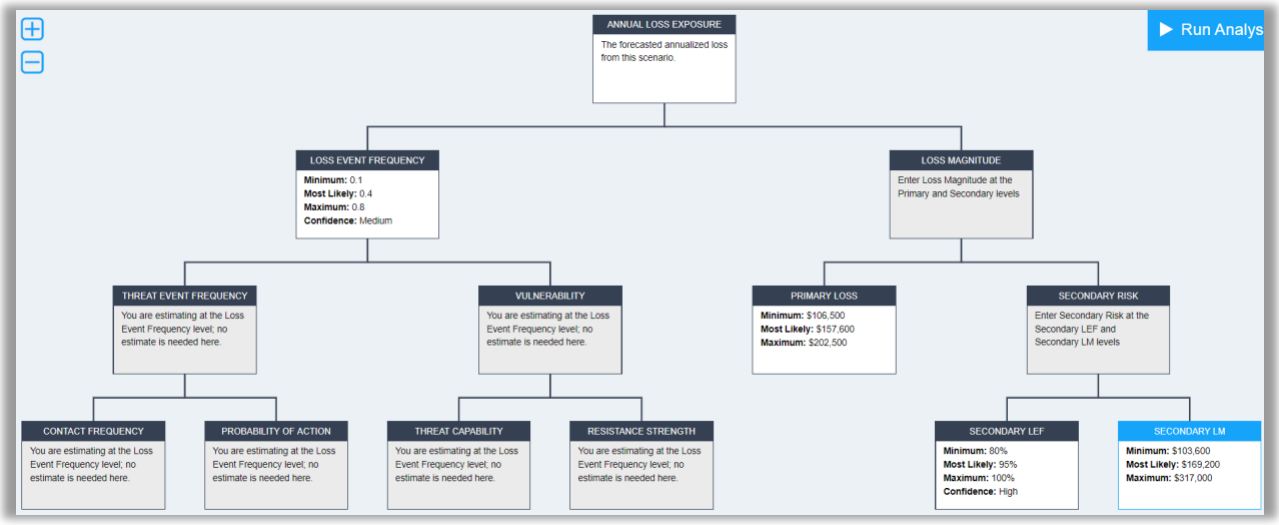
Medicines stealing via warehouse

Threat Actor(s)

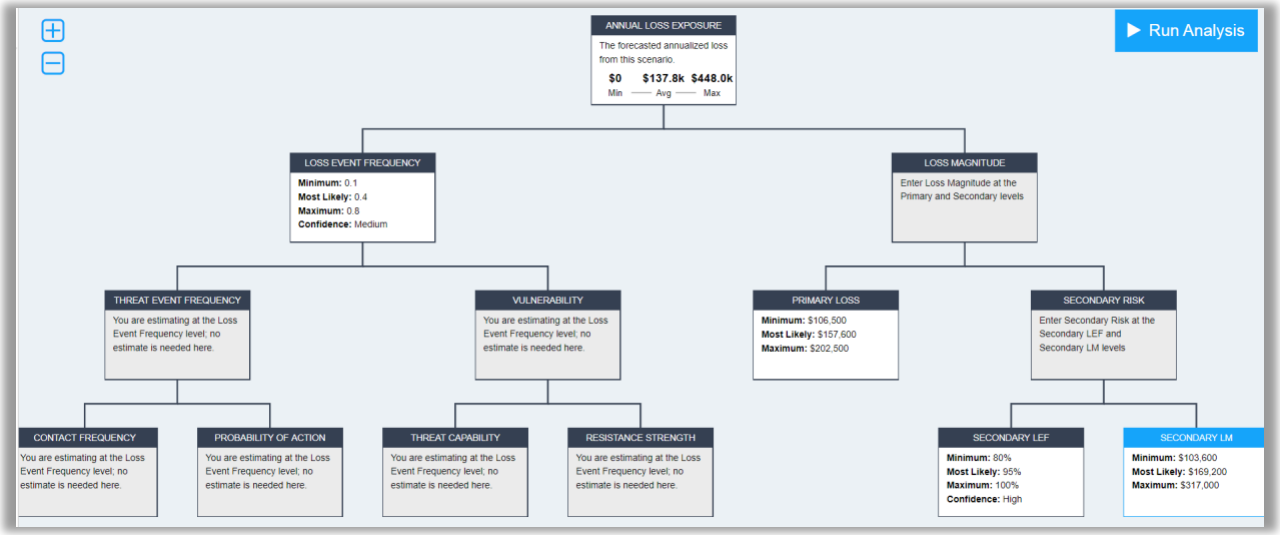
malicious
Human error

Threat Effect

Avaliability



[Insert a snapshot of primary, secondary, and total loss exposure results]



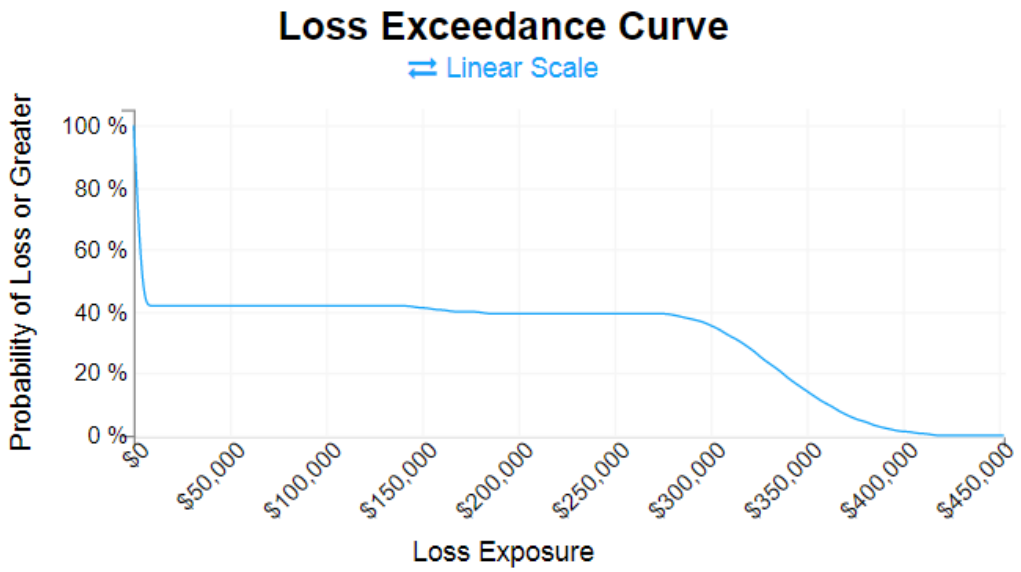
[Insert the loss Exceedance Curve]

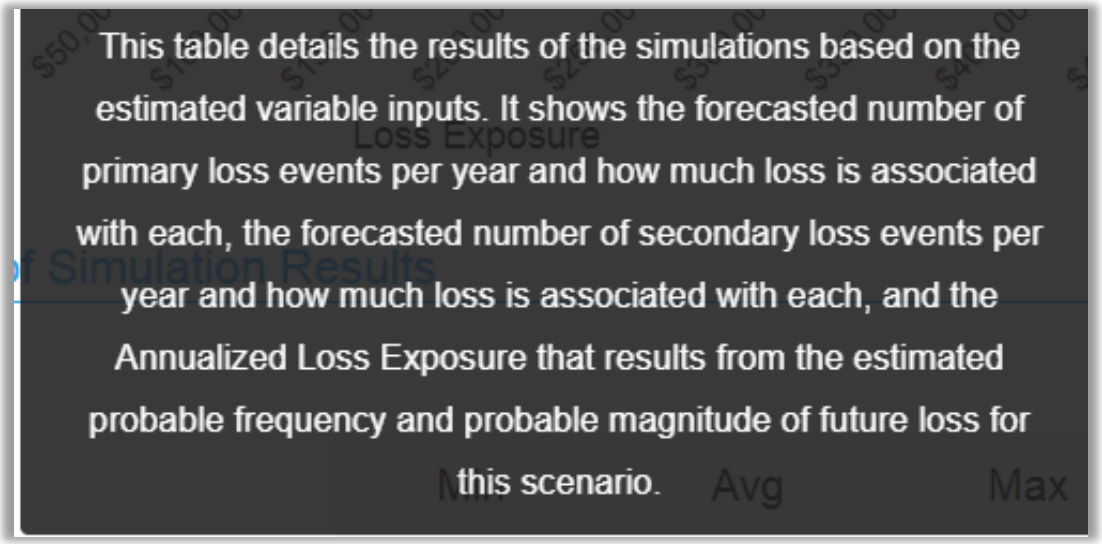
Analysis Results

Risk

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

$0	$137.8k	$448.0k
Minimum	Average	Maximum





Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.42	1
Loss Magnitude	$115.9k	$157.1k	$192.7k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0.39	1
Loss Magnitude	$113.9k	$183.0k	$281.0k

Vulnerability --

3.4 Analyzing results

The risk annualized loss exposure (ALE) the minimum will be happened $ 0 and the average will be happened up to $137.8 and the maximum is$ 448

- we estimate the minimum loss exposure from **minimum value of primary +minimum value of secondary:**

the value primary of minimum loss events/year is 0 X of the minimum value of loss magnitude is 115.9 then add to the minimum value secondary of loss events/year is 0 X of the minimum value of loss magnitude is 113.9 =0

ALE min= (0 X 115.9 + 0 X 113.9 = 0)

- we estimate the average loss exposure from **average value of primary +average value of secondary:**

the value primary of minimum loss events/year is 0.42 X of the average value of loss magnitude is 157.1 then add to the average value secondary of loss events/year is 0.39 X of the average value of loss magnitude is 183.0 =**137**

ALE average= **(0.42 X 157.1 + 0.39 X 183.0)= $137.5**

- we estimate the maximum loss exposure from **maximum value of primary +maximum value of secondary:**

the value primary of maximum loss events/year is 1 X of the maximum value of loss magnitude is 192.7 then add to the maximum value secondary of loss events/year is 1 X of the maximum value of loss magnitude is 281 =

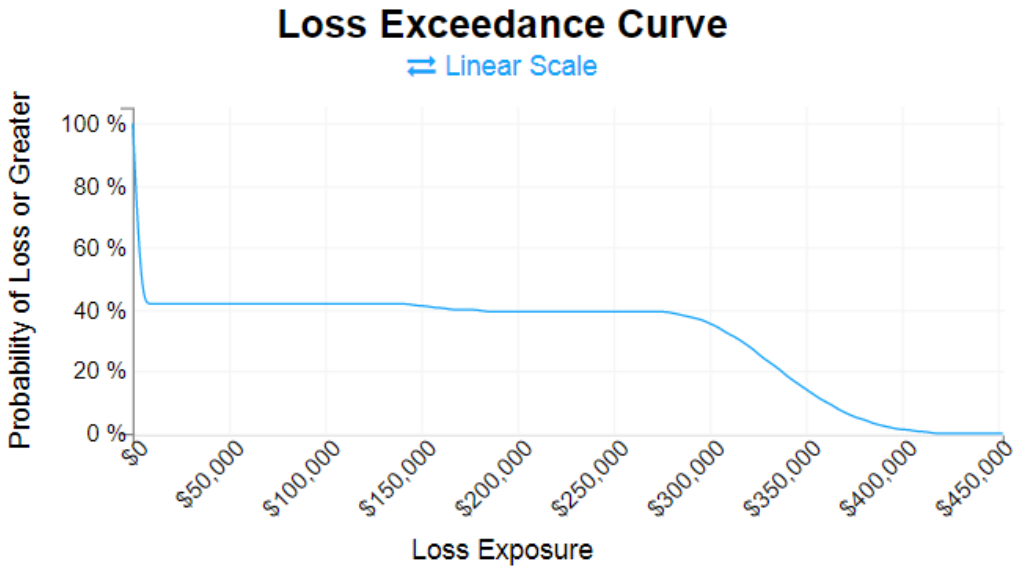
ALE maximum = (1X192.7 +1 X281)= $473.7

Analysis Results

Risk

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

$0	$137.8k	$448.0k
Minimum	Average	Maximum



- The probability 62% no loss at all based on monte carlo
- When The probability is 40% the loss exposure is Decreasing
- The probability is less than $50000

3.5 Suggested controls

we is suggestion of security controls from "NIST SP 800-53, Recommended:

- **Physical and Environmental Protection** (Operational): measures that can be utilized to protect an company resources and sensitive information physically. Includes perimeter security , use also CCTV system and use door locks.
- **Access control(Technical):** A set of mechanisms includes (two-factor authentication , Personal Identification Numbers [PINs], card readers, Biometric system.) that work in concert to create security architecture protecting Physical assets.

Also we is suggestion of containment controls

- should use policies control to enter warehouse to ensure access privileged insiders

- Firing an employee who acted maliciously (contact)

- education and awareness training for employee(includes guidelines for staff under various risk levels.)

Also we is suggesting of minimization controls

- Performing legal or other actions to recover property from perpetrators

Based on effectiveness of the control's (effect reduction in vulnerability and reduction in threat event frequency and reduction in loss magnitude)and priority for ABC company. We Recommended the following:

should use policies control to enter warehouse to ensure access privileged insiders

- Firing an employee who acted maliciously (contact)

- education and awareness training for employee(includes guidelines for staff under various risk levels.)

4. Conclusion

At the end of the report

It should be noted that risk management is only a tool available to individuals and institutions to use and activate in order to reduce the likelihood of loss and the degree of its risk. However, we must emphasize:

- The likelihood of any risk cannot be reduced to zero, as it is almost impossible.
- Under no circumstances can all risks be managed in a comprehensive manner, as we still live in a world full of doubts and doubts about the outcome of future decisions

But we recommend implementing recommendations for the proposed controls to reduce the incidence of loss in a company.