Making Better Cyber and Technology Risk Decisions: Part 2

Jack Jones
Chairman
FAIR Institute

You have two security-related findings…

An audit discovered that privileges are not consistently being updated for user accounts with access to a customer service application containing PII.

A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.

Which of them is more important to fix first?

A review: Two fundamental truths about prioritization

Prioritization is always based on some form of comparison

Comparisons are always based on some form of measurement

Three criteria for reliable risk measurement…

1. Clarity about what's being measured
2. An accurate risk model
3. Data

Had you clearly defined in your own mind what you just measured?

What model did you use?

What data did you use?

Inappropriate Access Privileges

Scoping this analysis…

- What is the asset at risk? Customer information
- Who/what is the threat actor(s)? Personnel with inappropriate access
- What type of action Malicious
- What type of event is it (C, I, or A)? Confidentiality
- What is the loss event scenario? The confidentiality of customer data is maliciously compromised by personnel with inappropriate access

Using NIST 800-30

Step 1: "Likelihood of Threat Event Initiation"

In FAIR this is referred to as "Threat Event Frequency"

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Step 2: Likelihood of Threat Event Resulting in Adverse Impacts

In FAIR this is referred to as “Vulnerability”

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Step 3: Overall Likelihood

In FAIR this is referred to as “Loss Event Frequency”

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Step 4: Estimating impact

Very High	Multiple severe or catastrophic adverse effects on the organization's assets or individuals
High	A severe or catastrophic adverse effect on the organization's assets or individuals
Moderate	Serious adverse effect on the organization's assets or individuals
Low	Limited adverse effect on the organization's assets or individuals
Very Low	Negligible adverse effect on the organization's assets or individuals

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

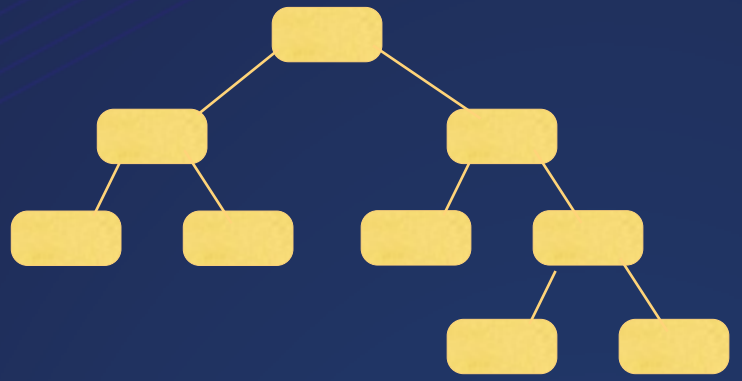
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Step 5: Estimating risk

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Using FAIR



Threat Event Frequency

- Definition

  The probable frequency, within a given timeframe, that a threat will act in a manner that may result in loss

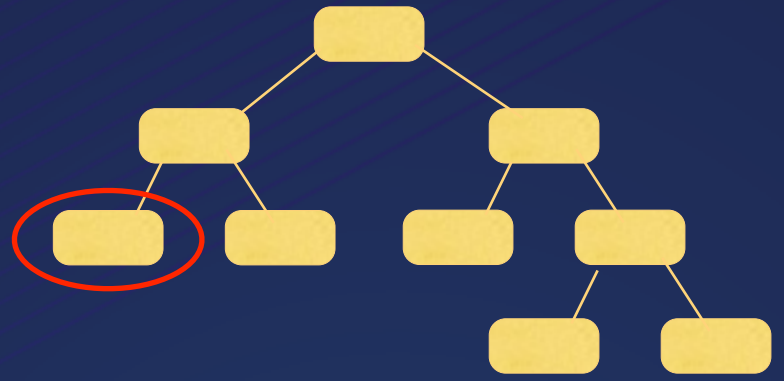
- Estimates

  Qualitative: Low

  Min: .05 yr (1 in 20 yr)

  Max: 5 yr (Logging!)

  ML: .1 yr (1 in 10 yr)

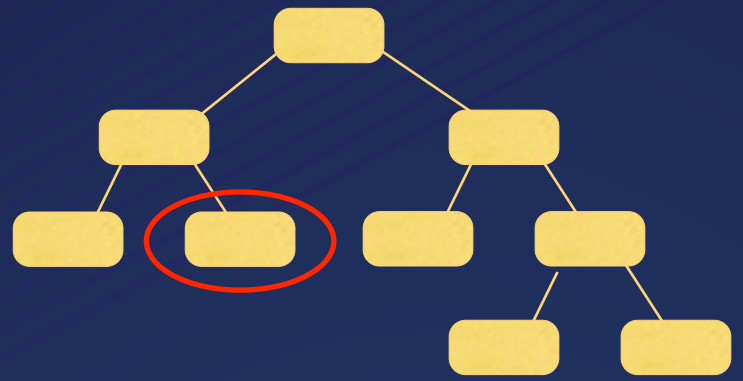


- Data/Rationale
  - 30 user accounts (out of 200) with inappropriate access levels (15%)
  - HR records show 2 events of misuse in the past 3 yrs (“snooping”)
  - Snooping was performed by personnel with appropriate access
  - No history of malicious misuse

Vulnerability

- Definition

  The probability that a threat event will become a loss event



- Estimates

  Qualitative: Very High

  100%

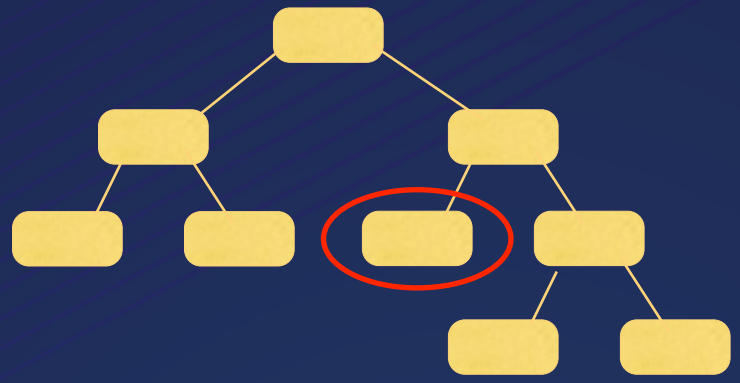
- Data/Rationale

  These are privileged insiders who don't have to overcome controls in order to execute the illicit action

Primary Loss Magnitude

- Definition

  Loss that occurs directly as a result of the threat act against the asset.



- Estimates

  Qualitative: Moderate

  Min: $ 25k

  Max: $ 150k

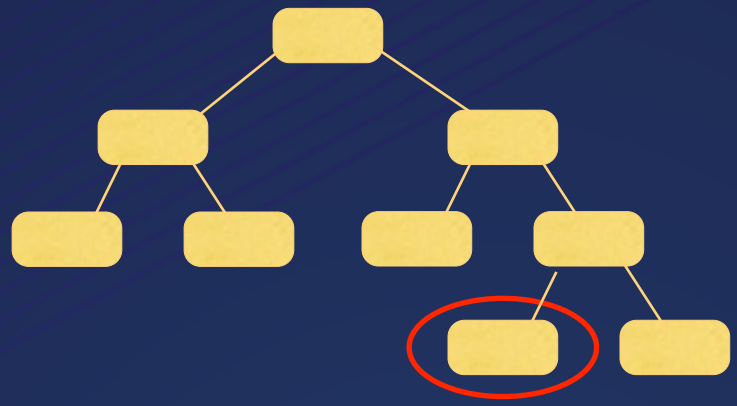
  ML: $ 40k

- Data/Rationale
  - Forensic/investigative costs
  - Costs associated with replacing the malicious employee

Secondary Loss Event Frequency

- **Definition**

  The probability of secondary loss (fallout)



- **Estimates**

  Qualitative: Very High

  100%

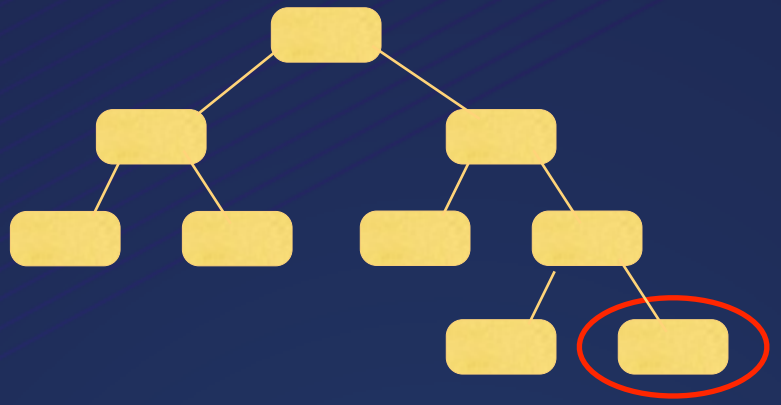
- **Data/Rationale**

  Assumes that any compromise of customer information would require notification and other secondary costs

Secondary Loss Magnitude

- Definition

  The probable loss magnitude resulting from fallout



- Estimates

  Qualitative: Moderate

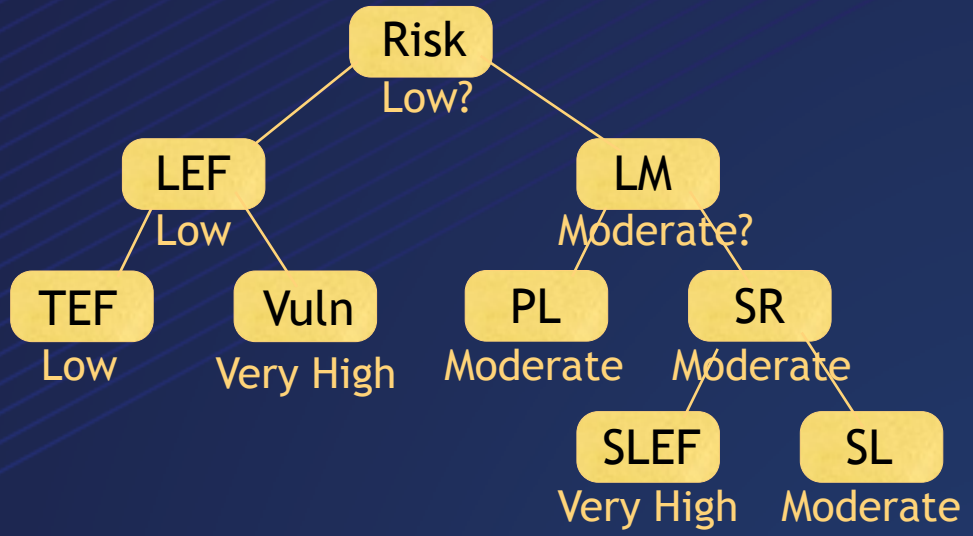
  Min: $ 100

  Max: $ 500k

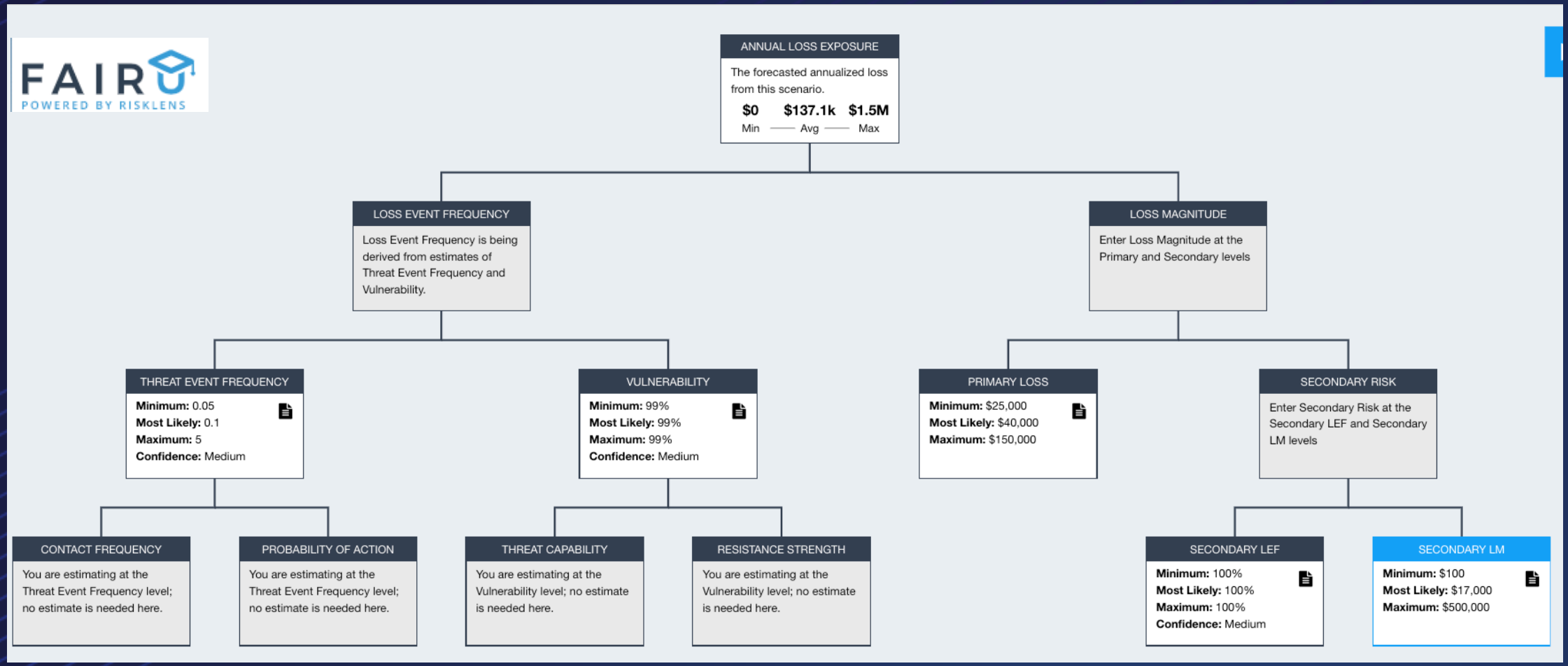
  ML: $ 17k

- Data/Rationale
  - Minimum of 1 customer record
  - Most Likely 20 customer records
  - Max 100 records (only accessible one at a time)
  - Includes notification costs, credit monitoring, legal defense, and customer churn

Deriving risk

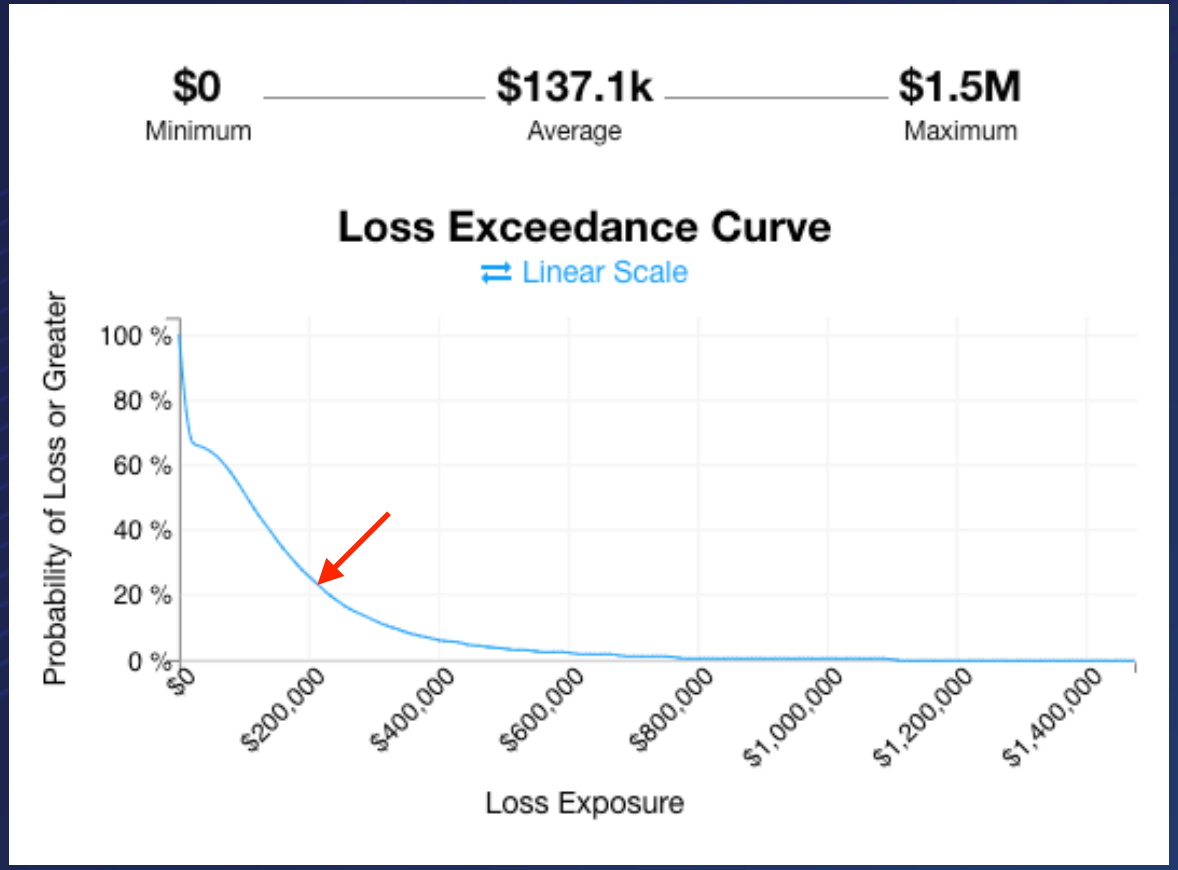


Deriving risk



https://app.fairu.net

Deriving risk



https://app.fairu.net

Weak Intrusion Detection

Scoping this analysis…

- What is the asset at risk? Customer information
- Who/what is the threat actor(s)? Cyber criminals
- What type of action Malicious
- What type of event is it (C, I, or A)? Confidentiality
- What is the loss event scenario? The confidentiality of customer data is maliciously compromised by cyber criminals who are able to breach the perimeter.

Threat Event Frequency

- Definition

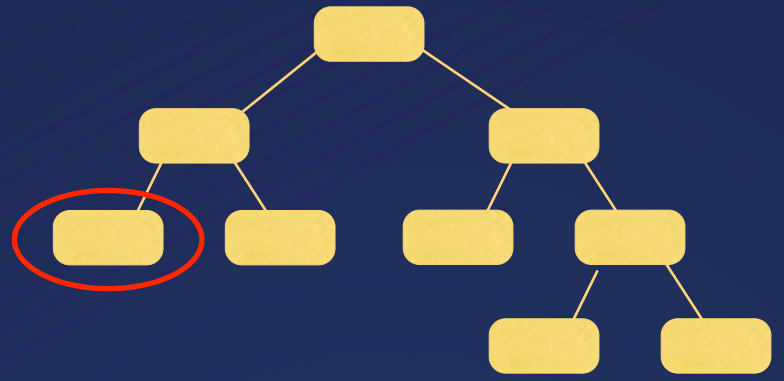
  The probable frequency, within a given timeframe, that a threat will act in a manner that may result in loss

- Estimates

  Min: .1 yr (1 in 10 yr)

  Max: 5 yr

  ML: .2 yr (every other year)



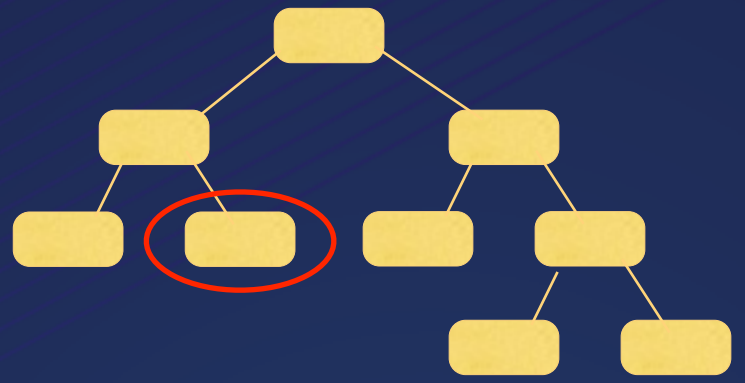
- Data/Rationale

  Based on SME estimates as well as on data from compromised systems at the perimeter that have evidence of attempts to move deeper and laterally within the network.

Vulnerability

- Definition

  The probability that a threat event will become a loss event



- Estimates

  Min: 75%

  Max: 99%

  ML: 95%

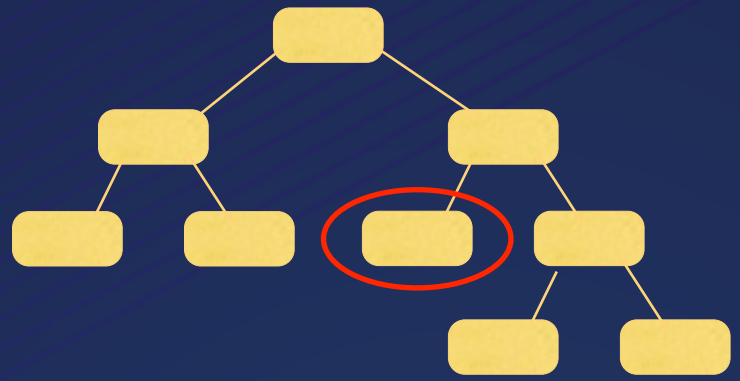
- Data/Rationale

  Breaching the perimeter typically involves gaining (or positions the threat actor to gain) access to legitimate accounts, which makes it much more likely that internal resistive controls will be ineffective.

Primary Loss Magnitude

- Definition

  Loss that occurs directly as a result of the threat act against the asset.



- Estimates

  Min: $ 50k

  Max: $ 500k

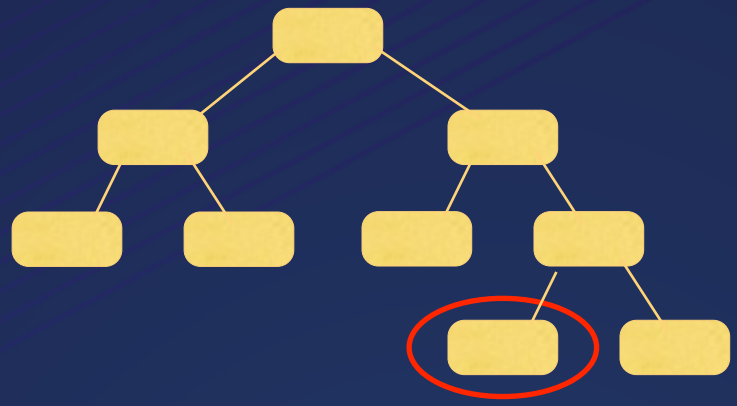
  ML: $ 100k

- Data/Rationale
  - Internal personnel response efforts
  - Outsourced forensic/investigative costs

Secondary Loss Event Frequency

- Definition

  The probability of secondary loss (fallout)



- Estimates

  100%

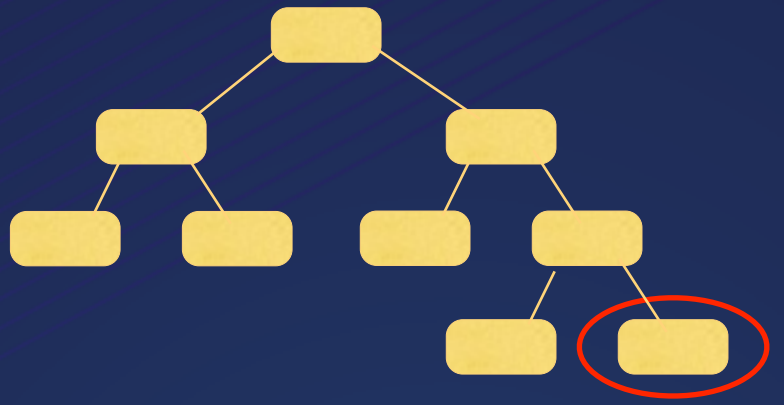
- Data/Rationale

  Assumes that without early detection the threat actor will eventually compromise some amount of customer information, which would require notification and other secondary costs.

Secondary Loss Magnitude

- Definition

  The probable loss magnitude resulting from fallout



- Estimates

  Min: $ 5k

  Max: $ 100M

  ML: $ 1M

- Data/Rationale
  - Minimum of 1 customer record
  - Most Likely 1M customer records
  - Max all customer records
  - Includes notification costs, credit monitoring, legal defense, and customer churn

Results

Inappropriate Access Privileges

Weak Intrusion Detection

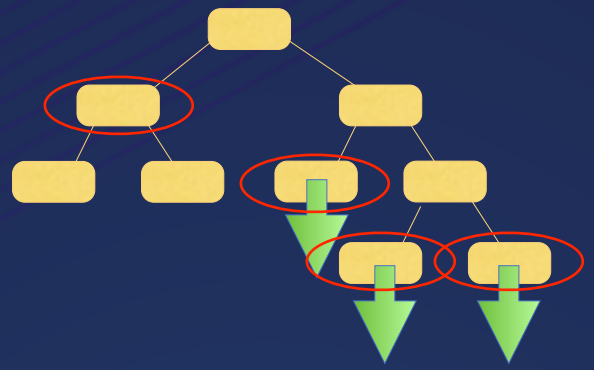
How much less risk will we have if…?

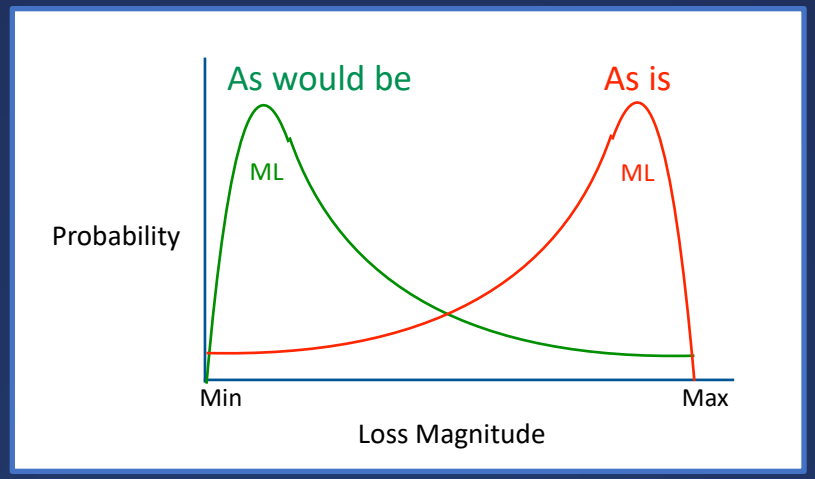
The solutions required for improving this situation were expected to cost approximately $750k in year one, and an additional $300k to $500k annually thereafter.

Is the investment worth it?

What changes with strong detection?

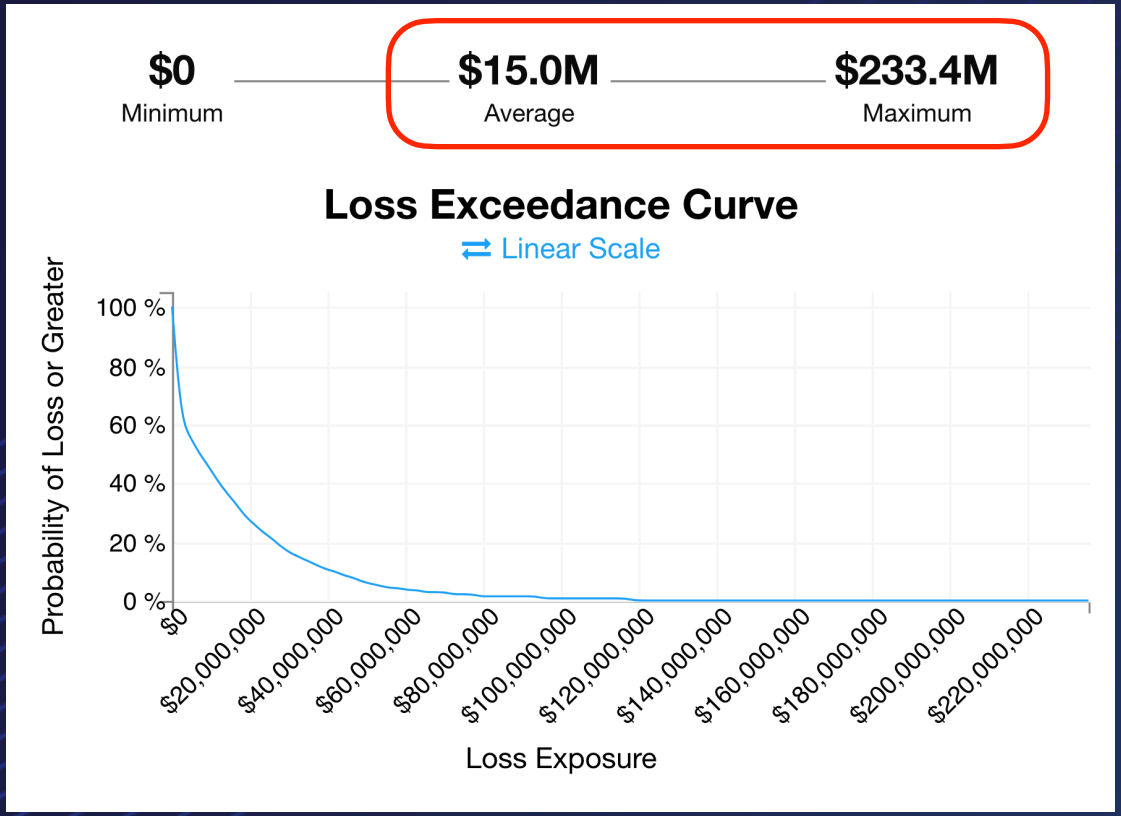
- Loss Event Frequency doesn't change
- Loss Magnitude changes:
  - Primary loss goes down because of earlier detection and simpler forensics.
  - Secondary LEF goes down because there are better odds of intervening before customer data is compromised.
  - Secondary LM goes down because the threat actor is less likely to have time to find the mother load.
- Only the Most Likely (ML) values change (not Min or Max)!





Cost-benefit analysis results

Before



After

Wrapping up

Making better cyber and technology risk decisions

- Decisions are always based on priorities.
- Prioritization is always based on comparisons, which are based on measurements.
- Three fundamental requirements for reliable risk measurements:
  - Clarity: You can't reliably measure what you haven't clearly defined
  - An accurate model: All models are imperfect — but some are fundamentally broken
  - Data: Data will always have uncertainty. The key is to faithfully account for and communicate uncertainty.
- How effectively we apply our limited risk management resources boils down to how well we're able to measure risk.
- FAIR enables better risk measurement.