A FAIR Approach to Cyber and Technology Risk Measurement

Jack Jones
Chairman
FAIR Institute

Chad Weinman
VP Professional Services,
RiskLens

Jack Freund Ph.D.
Fellow
FAIR Institute

Rachel Slabotsky
Sr. Manager, Professional Services
RiskLens

FAIR INSTITUTE

Join the FAIR Institute

Members of the FAIR Institute take advantage of many benefits. The greatest benefit is access to the exclusive community of information risk officers, cyber security leaders and business executives who share their experience and knowledge on the growing discipline of information risk management.

Members also receive:

- Full access to our ever-growing Resource Library and content generated by the Institute,
- Discounts on events and the annual FAIR Conference,
- Weekly blog updates,
- Much more!

FAIR Institute Breakfast

When: February 26, 2020,
7:30 - 10:30 AM PST

Where: Parc 55 San Francisco,
Embarcadero Room (Level Three)
55 Cyril Magnin Street,
San Francisco, CA 94102

Building an Effective Cyber Risk Management Program that Actually Works

FAIR Institute Breakfast Meeting during RSAC2020

2020 FAIR Conference (FAIRCON2020)

October 6 & 7, 2020
Marriott Wardman Park
Washington, DC

FAIRCON20 brings leaders in information and operational risk management together to explore best FAIR practices that produce greater value and enable business-aligned communication.

Factor Analysis of Information Risk (FAIR) has emerged as the standard Value at Risk (VaR) framework for understanding, measuring and analyzing information risk, and ultimately, for enabling well-informed decision making.

The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk with FAIR.

- Explore best risk management practices that align with business goals
- Discover new FAIR-based products and services to help your program
- Expand your industry wide network

Reserve your Seat Today: http://www.fairinstitute.org/faircon20

FAIR Training Courses Discount

FAIR ANALYSIS
FUNDAMENTALS
RiskLens Academy

RSAC20FAIRTR

- **35% off** FAIR Analysis Fundamentals and/or FAIR Analyst Learning Path
- No minimum purchase requirement, available to everyone with the code.
- Limited to one discounted transaction per customer.
- Active through March 31.

FAIR INSTITUTE

Current Cyber Risk Measurement Practices and Why They’re Evolving

Jack Jones

Chairman

FAIR Institute

Which should we fix first?

Unreliable Access
Privilege Management

Weak
Intrusion Detection

Both were rated **“High Risk”**

What’s the **ROI** for a Cybersecurity Investment?

How much do they really understand?

CISO

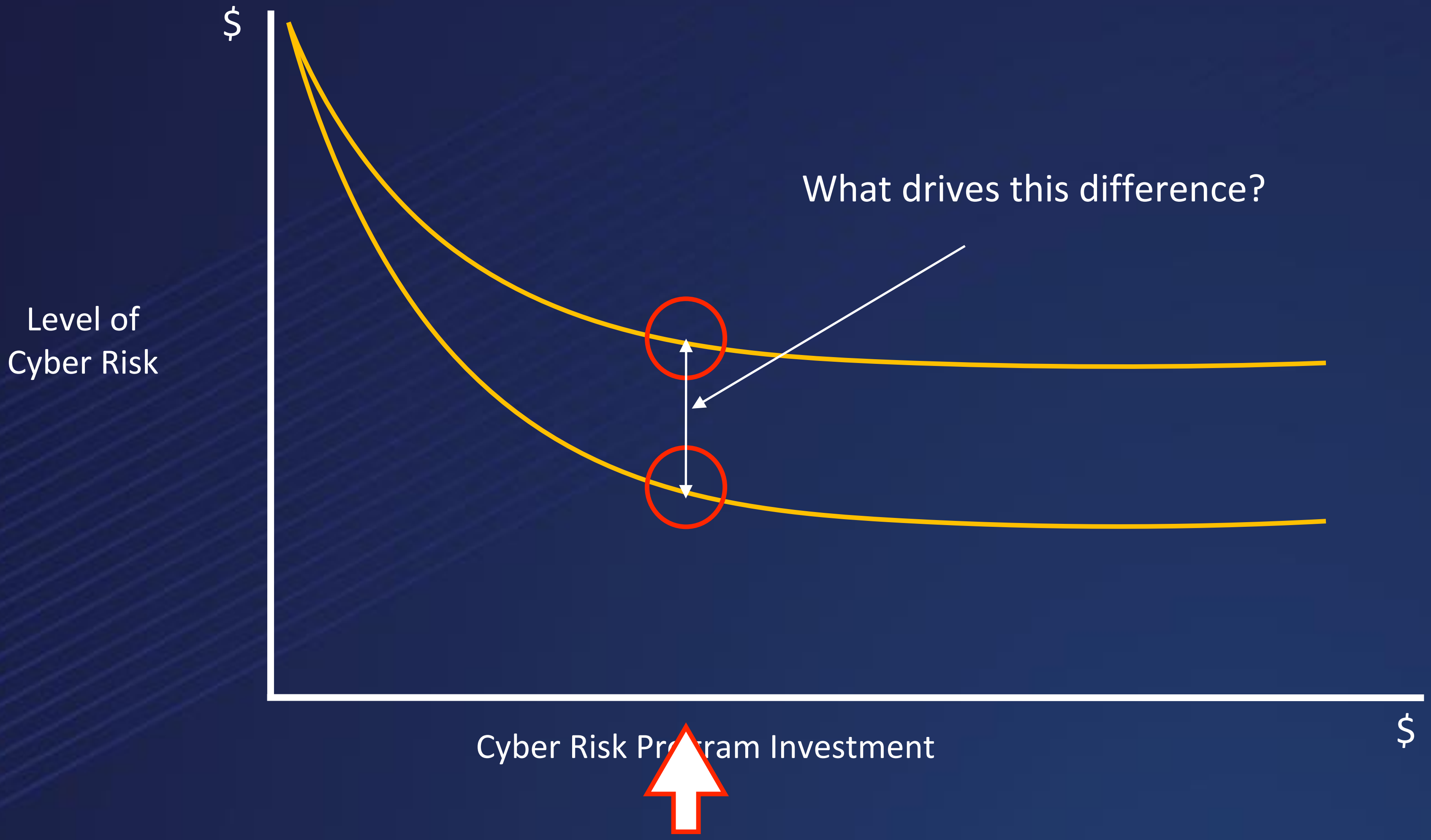
Δεν γνωρίζουμε πόσο μεγάλο είναι ο κίνδυνος που έχουμε.

The risk landscape in a nutshell…

Complex

Dynamic

Limited Resources



What drives this difference?

Decisions

Prioritization and solution choices.

What’s wrong with what we’ve been doing?

Weak password

Missing patch

Cyber criminals

Which of the "Highs" is highest?

Outdated policy

No monitoring

Weak encryption

Inappropriate access privilege

Highest "Medium" vs. lowest "High"?

Limited logging

Flat architecture

How much risk is there in total?

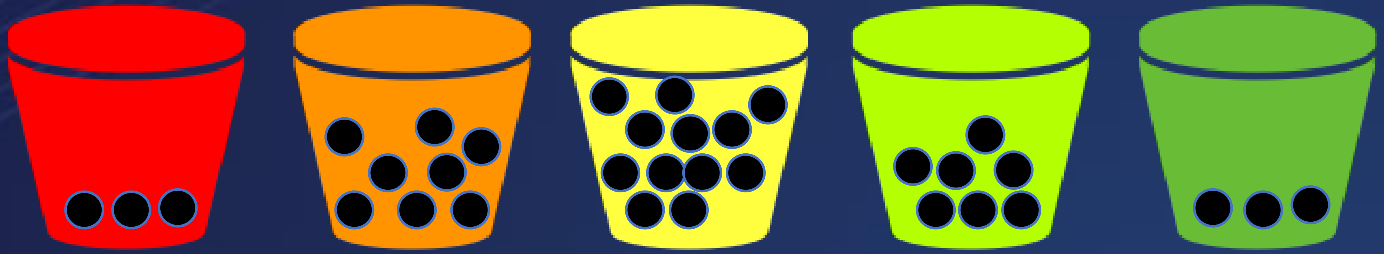
No backups

Disgruntled insiders

Unencrypted PII/PHI

Local admin privileges

Where are lines drawn, and why?



How fast are they going?

Qualitatively

Quantitatively

Measuring speed

Requires three elements:

1. The scope of what’s being measured

   Which car(s)?

   Which part of the track?

   Which lap(s)?

2. An analytic model

   What data? (time, distance)

   How the data are used (speed = distance/time)

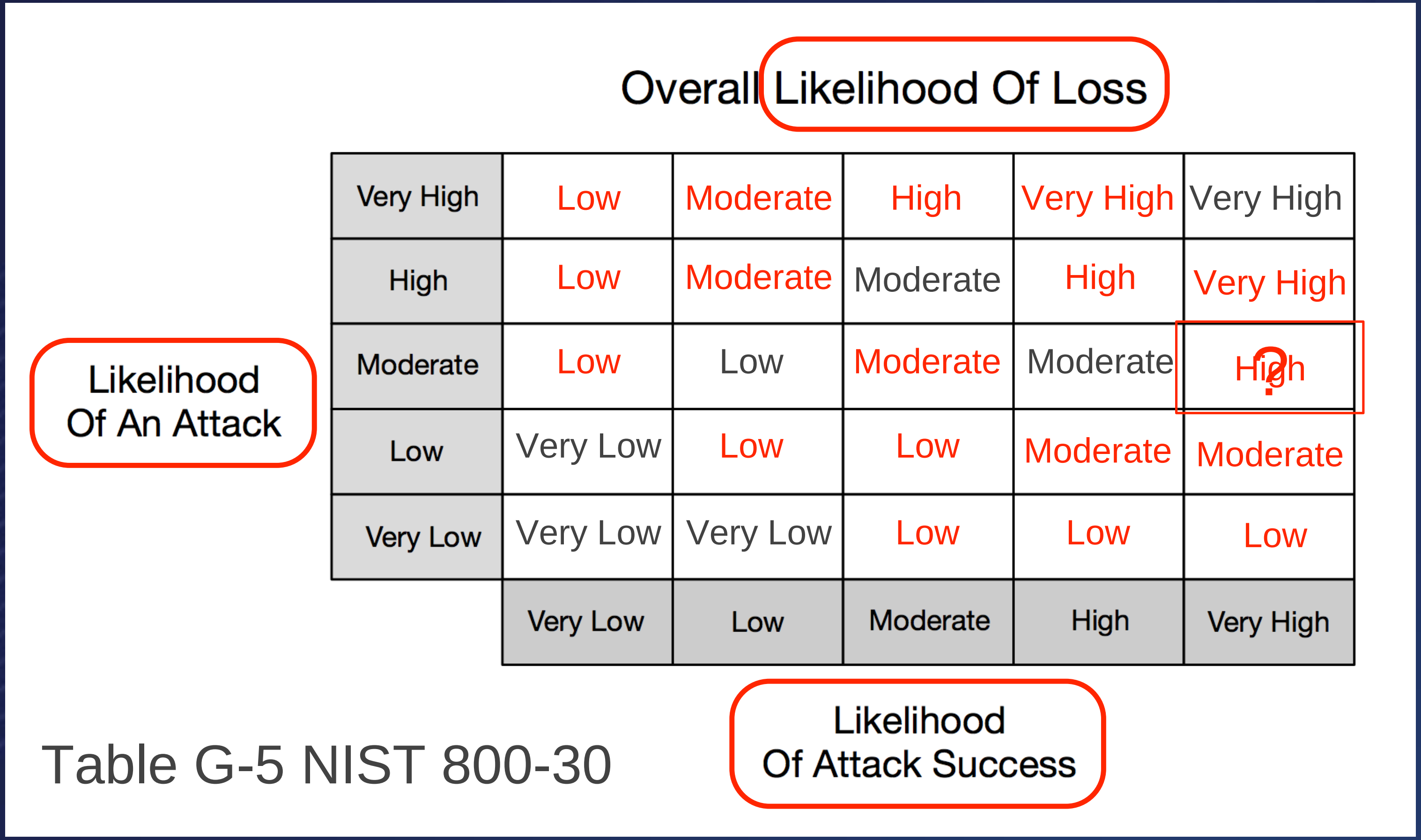
3. Data

Measuring risk

Requires three elements:

1. The scope of what's being measured
   - What asset?
   - What threat?
   - Which vector?
   - What type of event (e.g., C, I, A)?
2. An analytic model (e.g., FAIR)
   - What data?
   - How the data are used
3. Data

Inaccurate model (example)



Overall Likelihood Of Loss

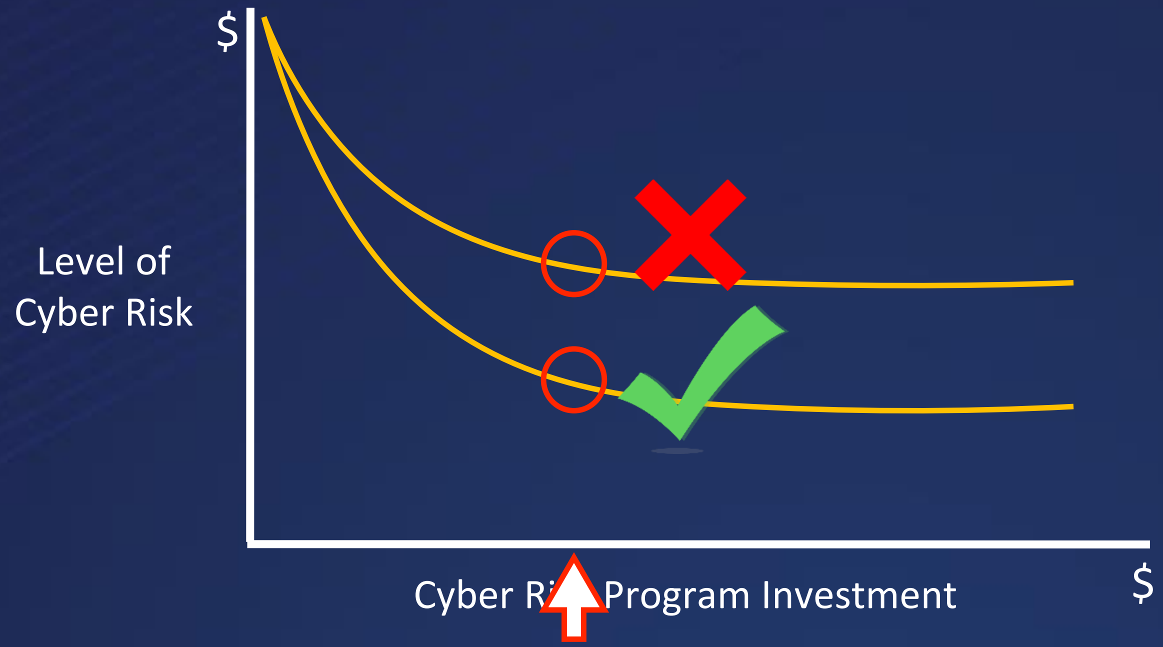
Likelihood Of An Attack

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
	Very Low	Low	Moderate	High	Very High

Likelihood Of Attack Success

Table G-5 NIST 800-30

Why does this matter?



Contributing to every breach…

Poor prioritization, wasted resources and ineffective communication

From now on, ask yourself…

- Which risk management curve are we on, and why?
- What needs to change?

FAIR INSTITUTE

An Introduction to FAIR

Jack Freund, Ph.D.

Director, Risk Science, RiskLens

FAIR Institute Fellow

Applying CRQ Using FAIR

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

Applying CRQ Using FAIR

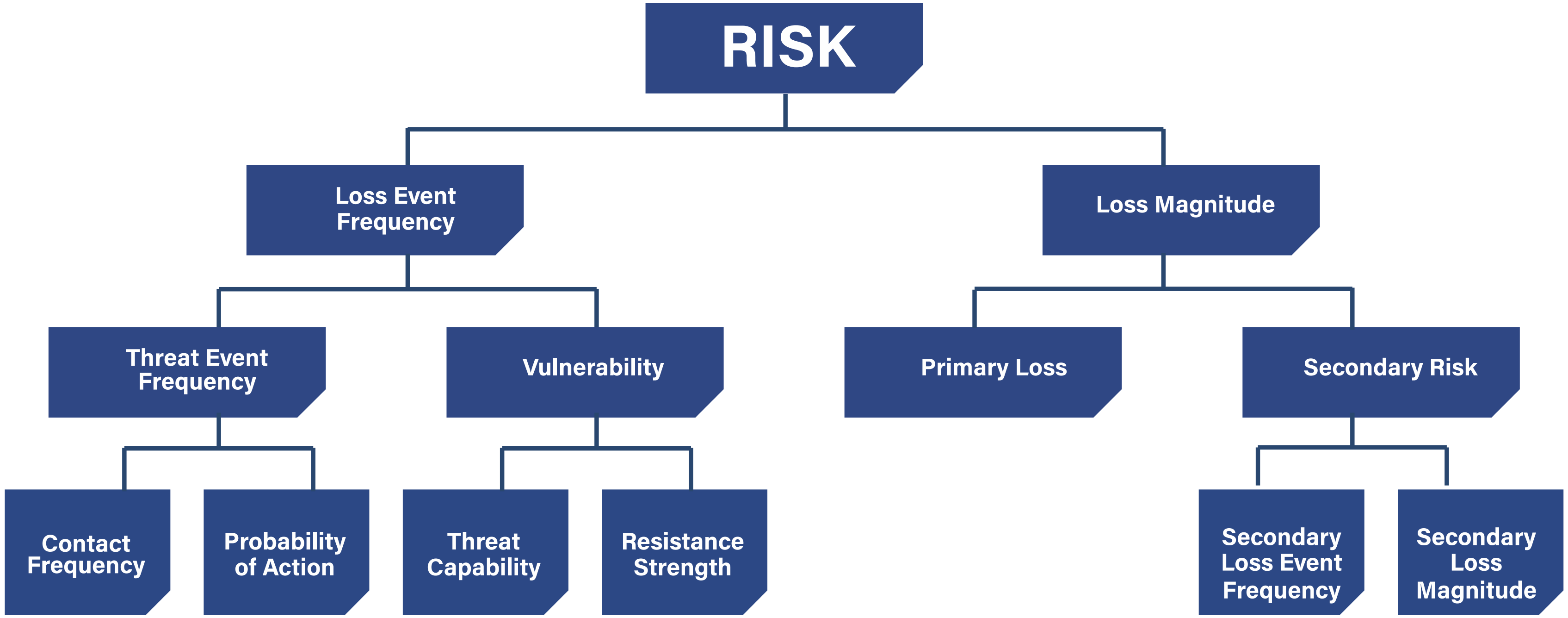
An audit discovered that privileges are not consistently being updated for user accounts with access to a customer service application containing credit card numbers.

- Who? Privileged Insiders
- What? Permissions
- What impact (loss)? CC Exfil

Loss Narrative:

Privileged Insiders utilizing legitimately granted permissions they no longer need exfiltrate payment card data for monetization.

Factor Analysis of Information Risk (FAIR)



- RISK
  - Loss Event Frequency
    - Threat Event Frequency
      - Contact Frequency
      - Probability of Action
    - Vulnerability
      - Threat Capability
      - Resistance Strength
  - Loss Magnitude
    - Primary Loss
    - Secondary Risk
      - Secondary Loss Event Frequency
      - Secondary Loss Magnitude

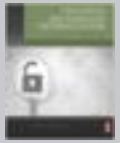
Accredited as an Industry Standard by

Complementary to Risk Frameworks

Supported by a Fast Growing Community

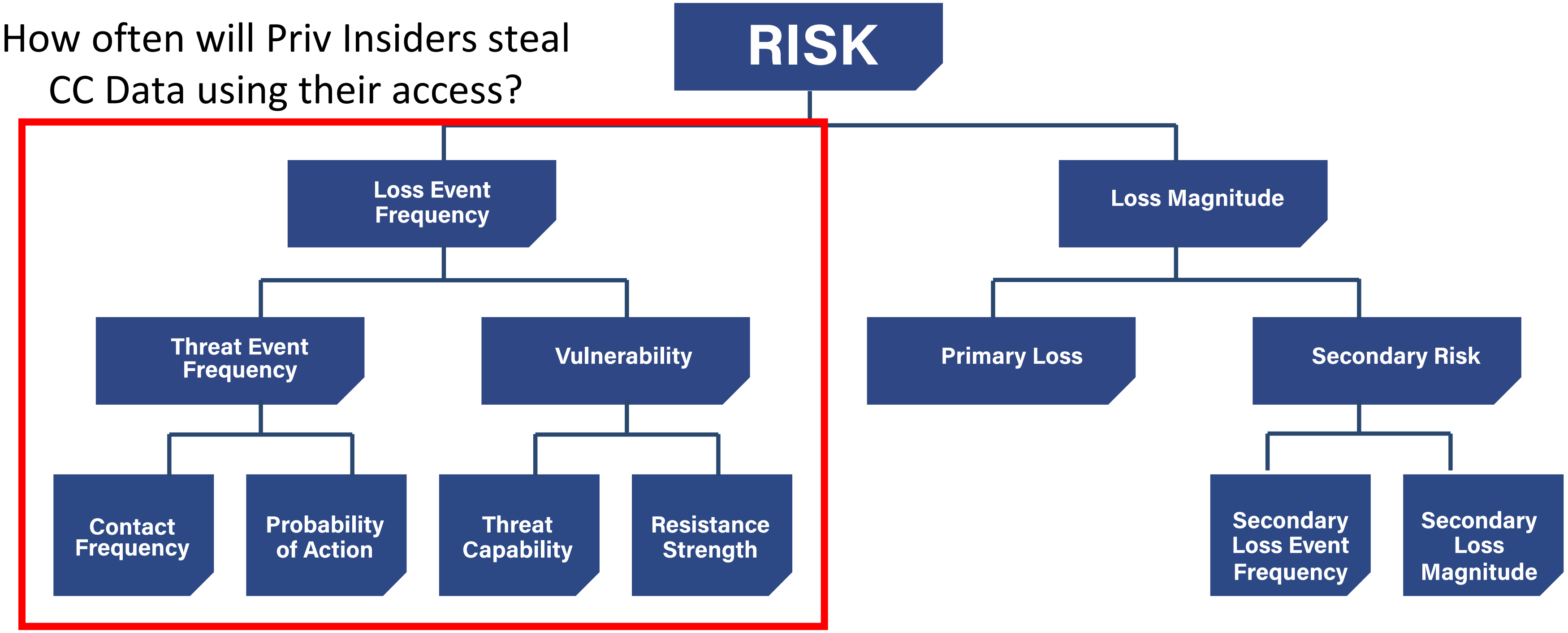
Wide Industry Adoption 30% Fortune 1000

FAIR Book Inducted in Cybersecurity Canon



Decomposing a Loss Scenario

How often will Priv Insiders steal CC Data using their access?



- RISK
  - Loss Event Frequency
    - Threat Event Frequency
      - Contact Frequency
      - Probability of Action
    - Vulnerability
      - Threat Capability
      - Resistance Strength
  - Loss Magnitude
    - Primary Loss
    - Secondary Risk
      - Secondary Loss Event Frequency
      - Secondary Loss Magnitude

Accredited as an Industry Standard by

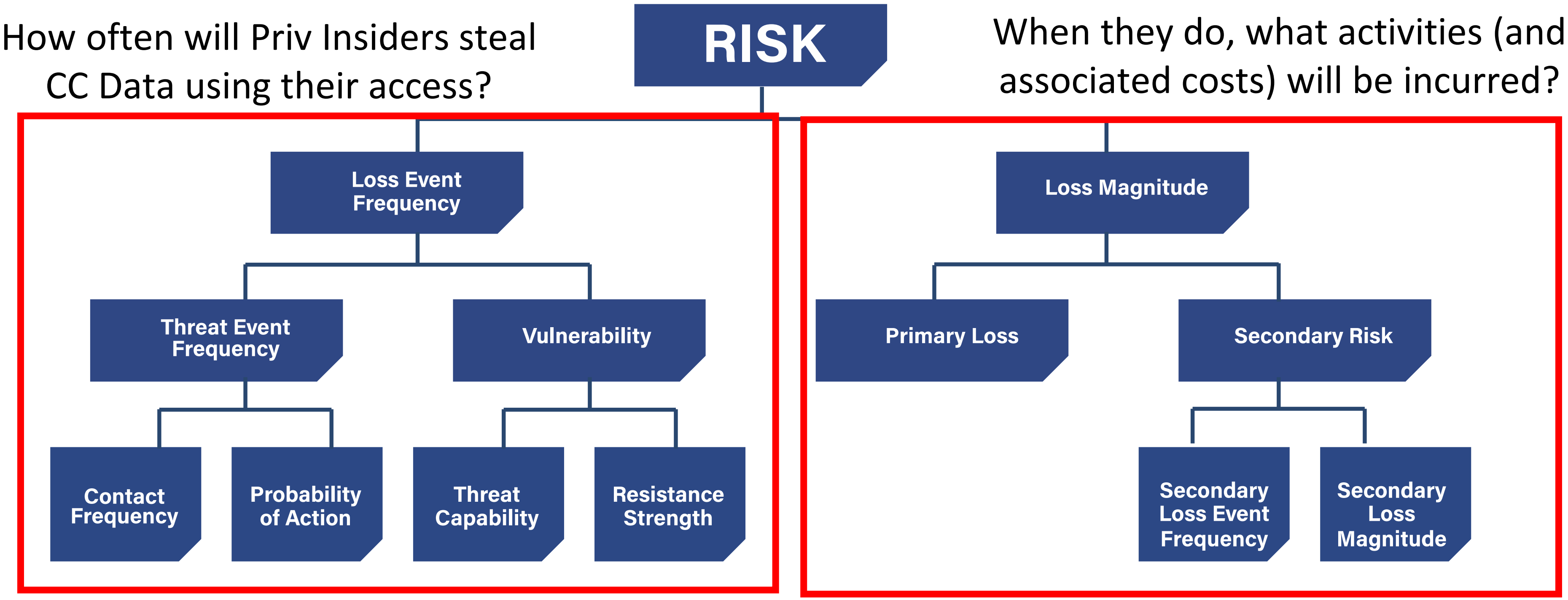
Complementary to Risk Frameworks

Supported by a Fast Growing Community

Wide Industry Adoption 30% Fortune 1000

FAIR Book Inducted in Cybersecurity Canon

Decomposing a Loss Scenario


How often will Priv Insiders steal CC Data using their access?

When they do, what activities (and associated costs) will be incurred?

Accredited as an Industry Standard by

THE Open GROUP

Complementary to Risk Frameworks

Information Security Management ISO 27001 Certified

NIST

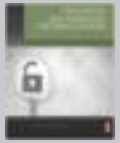
Supported by a Fast Growing Community

FAIR INSTITUTE

Wide Industry Adoption 30% Fortune 1000

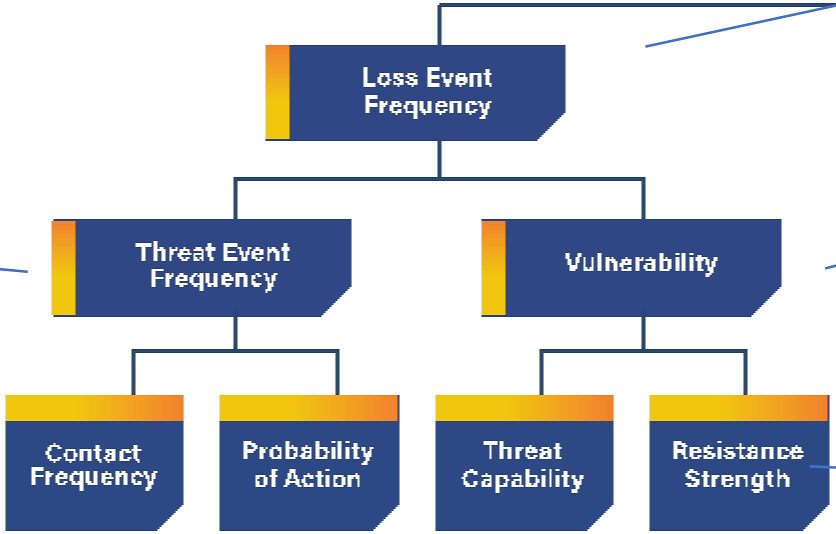
FORTUNE 1000

FAIR Book Inducted in Cybersecurity Canon



Decomposing a Loss Scenario -Frequency

How often will Priv Insiders steal CC Data using their access?



How often will it happen and we lose data?

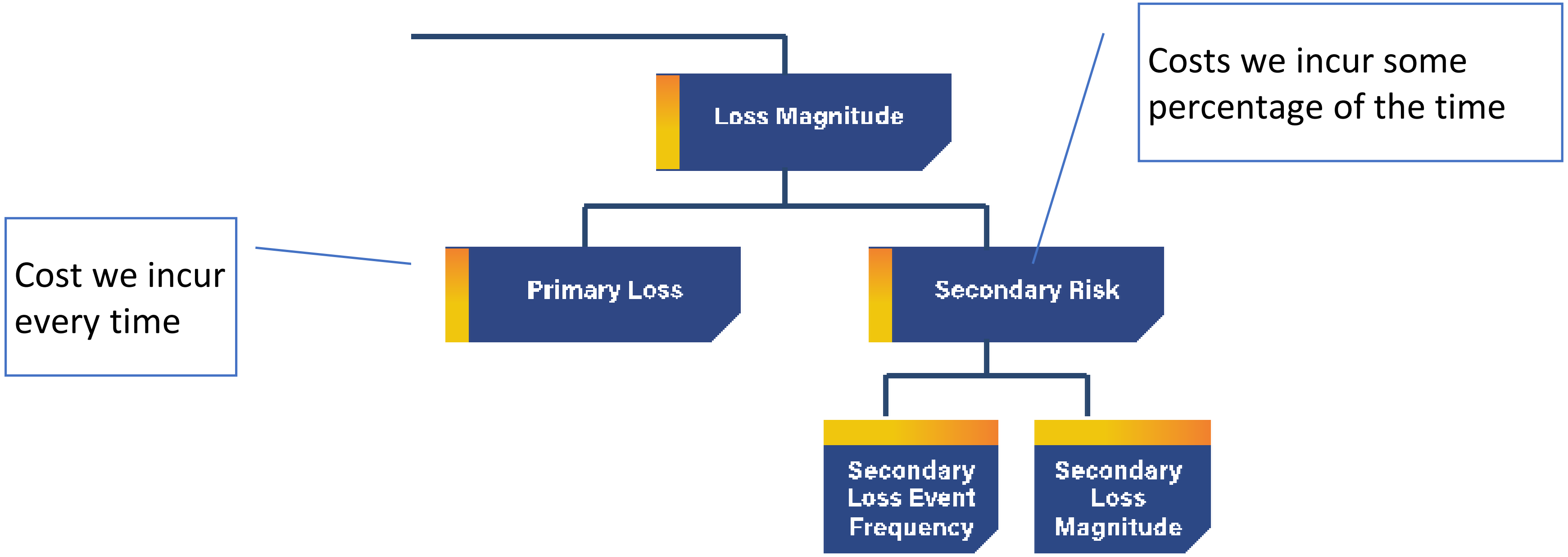
How often will they try to do it?

How vulnerable/susceptible are we to attacks of this type?

How to compute the win/loss ratio? (Preventative controls vs. Priv Insider capability)

Decomposing a Loss Scenario - Loss

When they do, what activities (and associated costs) will be incurred?



Cost we incur every time

Costs we incur some percentage of the time

FORMS OF LOSS:

PRODUCTIVITY LOSS: Loss that results from an operational inability to deliver products or services

RESPONSE COSTS: Loss associated with the costs of managing an event

REPLACEMENT COSTS: Loss that results from an organization having to replace capital assets

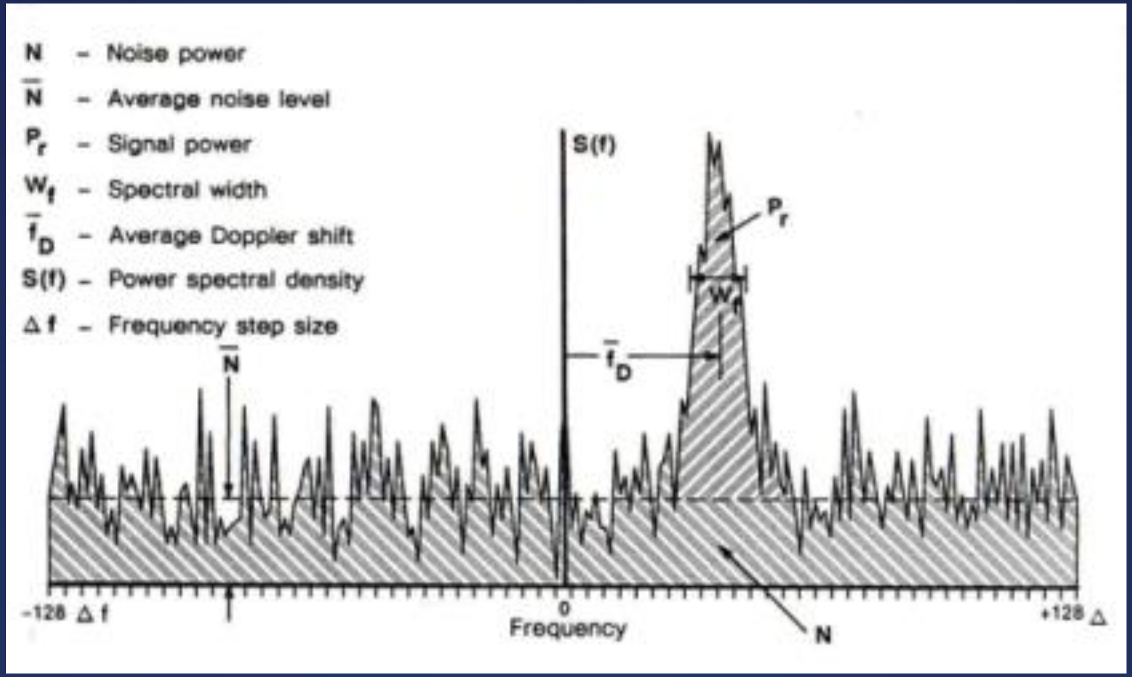
COMPETITIVE ADVANTAGE LOSS: Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

FINES AND JUDGMENTS: Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE: Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

What is measurement?

- A quantitatively expressed **reduction of uncertainty** based on one or more observations
  - Douglas Hubbard
- Signal to Noise Ratio – uncertainty reduction in a signal
  - Shannon-Hartley Theorem



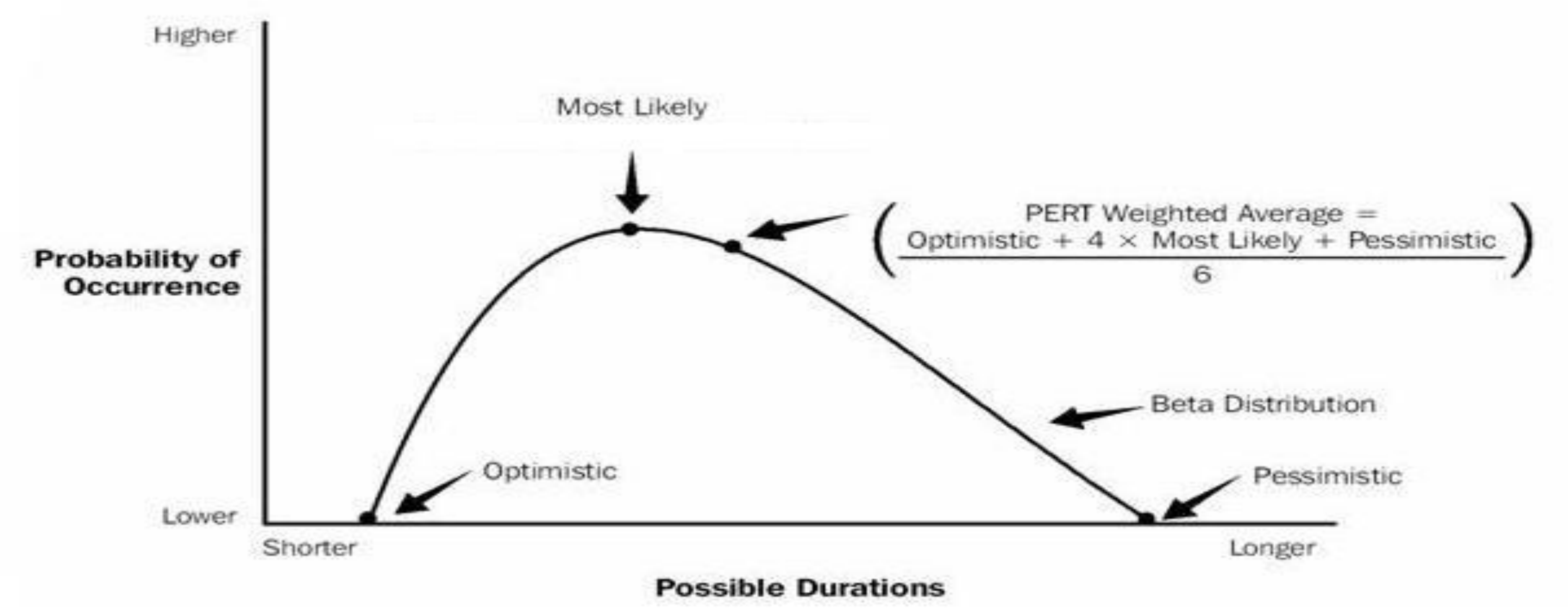
Getting over Measurement as "Precision"

- "The winning general is the one who can best act on imperfect information and half-formed theories"
  - Napoléon Bonaparte

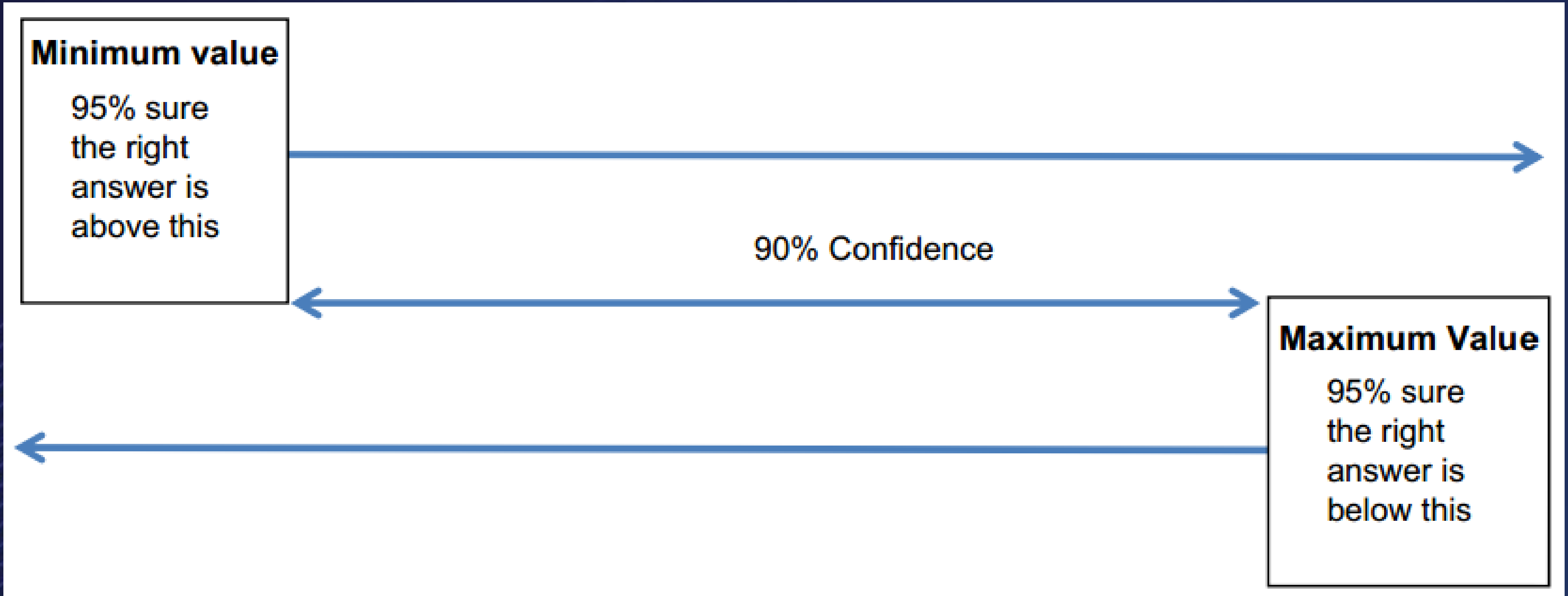
© Getty Images/The Bridgeman Art Library

Using PERT + Calibration to Overcome Bias

- People are more comfortable expressing values using ranges
- Since risk is necessarily a forward-looking discipline, there is inherent uncertainty (no prediction, think forecasting)



Estimating things you don’t know, with 90% confidence



Minimum value

95% sure the right answer is above this

90% Confidence

Maximum Value

95% sure the right answer is below this

The insurance industry doesn’t have data either (sometimes)

- **Cancellation Insurance**
  - 1916 Summer Olympics—to be held in Berlin, Germany. Canceled due to the outbreak of World War I
  - 1940 Summer Olympics—to be held in Tokyo, Japan. Canceled due to the outbreak of World War II
  - 1940 Winter Olympics—to be held in Sapporo, Japan. Canceled due to the outbreak of World War II
  - 1944 Summer Olympics—to be held in London, United Kingdom. Canceled due to the outbreak of World War II
  - 1944 Winter Olympics—to be held in Cortina d’Ampezzo, Italy. Canceled due to…you guessed it: World War II
- **Coupon Insurance**
- **Special Construction Projects**
  - The Channel Tunnel (*le tunnel sous la Manche*; aka “Chunnel”)
- **Cyber Insurance…**
- **Many others…**
- **You are not a beautiful and unique snowflake**

Estimating

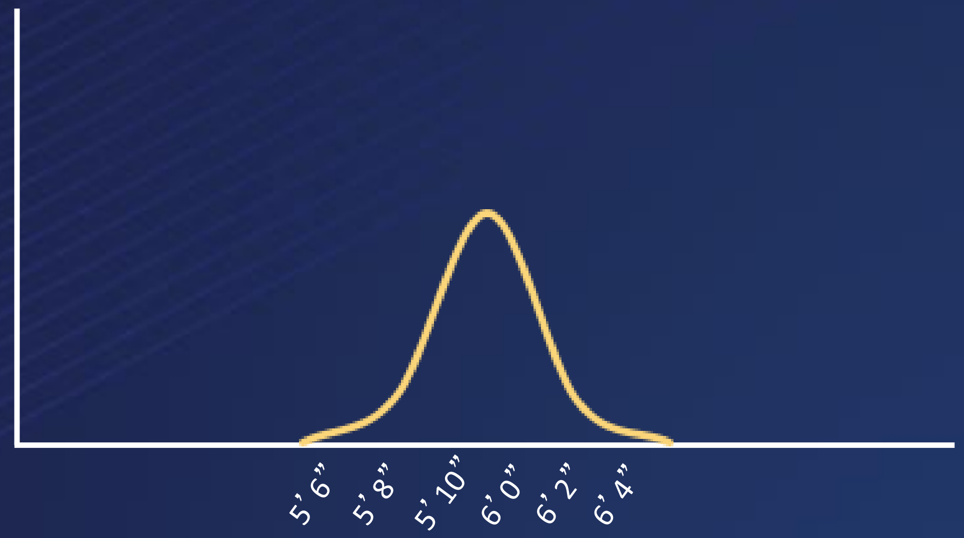
- How tall am I?
  - 5’8”
  - 5’9”
  - 5’10”
  - 5’11”
  - 6’0”
  - 6’1”
  - 6’2”
  - 6’3”
  - 6’4”

Estimating using ranges

- How tall am I?
  - < 5’8”
  - 5’8” - 6’2”
  - 6’2” - 6’6”
  - > 6’6”

Estimating using distributions

- How tall am I?



FAIR INSTITUTE

Cost Benefit Analysis + Prioritization

Chad Weinman

VP Professional Services,

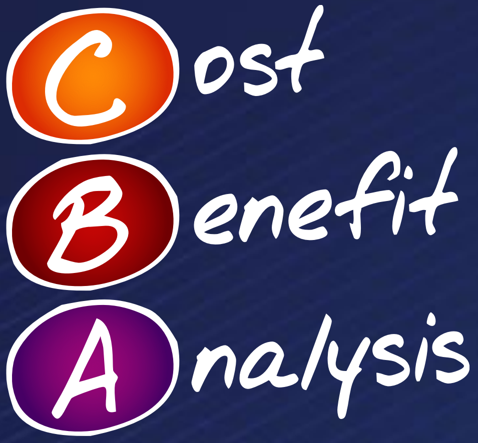
RiskLens

Rachel Slabotsky

Sr. Manager, Professional Services

RiskLens

Session Topics

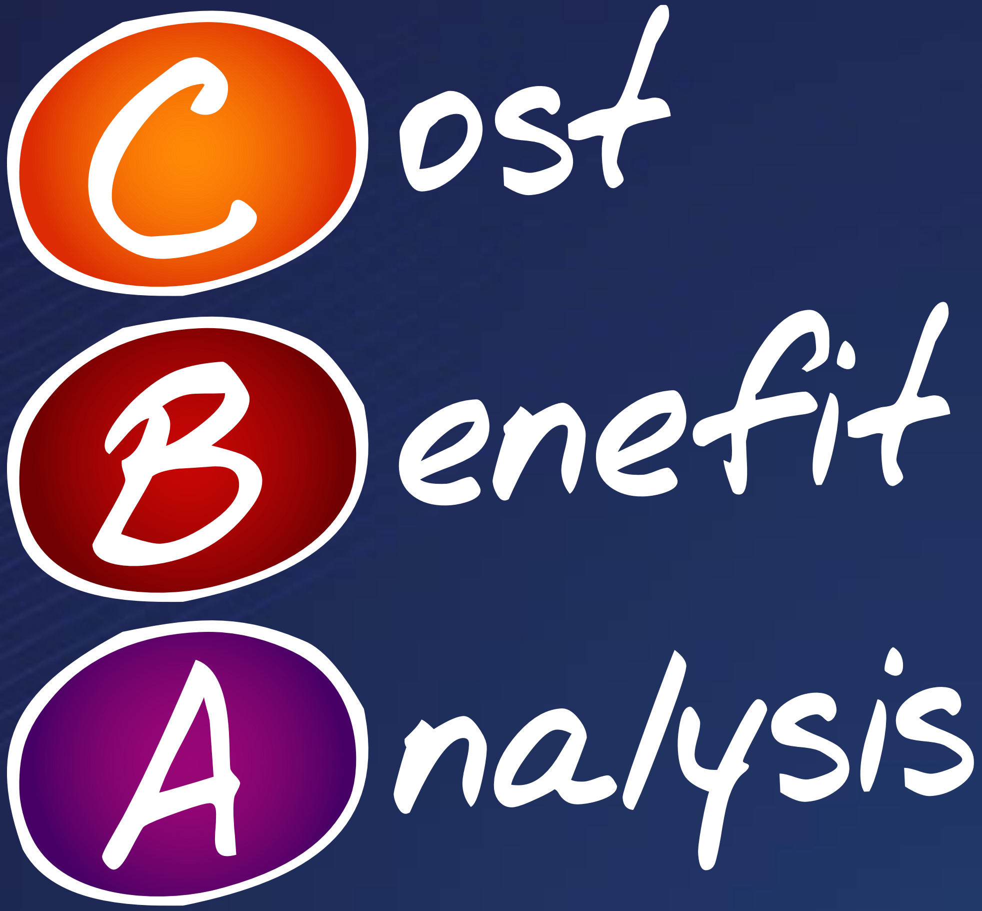


Introduction to Problem Space

Example Case Studies

Key Takeaways

Questions



Cost

Benefit

Analysis

Not only do traditional methods have logical flaws, they prevent us from answering some important risk-based questions.

“Should we invest in this new control?”

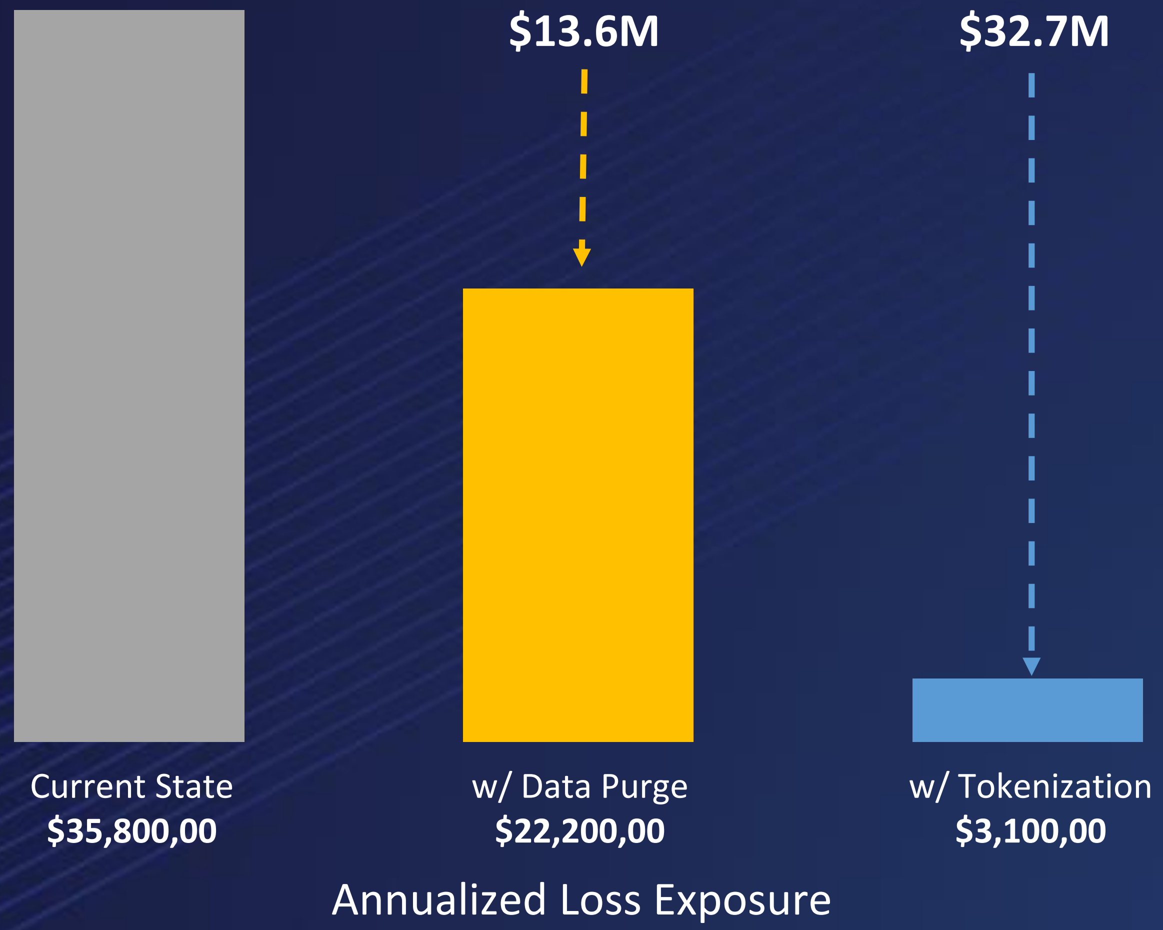
“Is the risk reduction worth the cost?”

Case Study ***#1***

Which security investment provides the greatest reduction in risk: **Data Purge** or **Tokenization**?

VS.

Data Purge vs. Tokenization



Key Drivers – Data Purge

Reduction of potential PII records stolen

- ➢ Maximum of 6M (4M reduction) for database cluster

Key Drivers – Tokenization

Reduction in likelihood of secondary fall-out

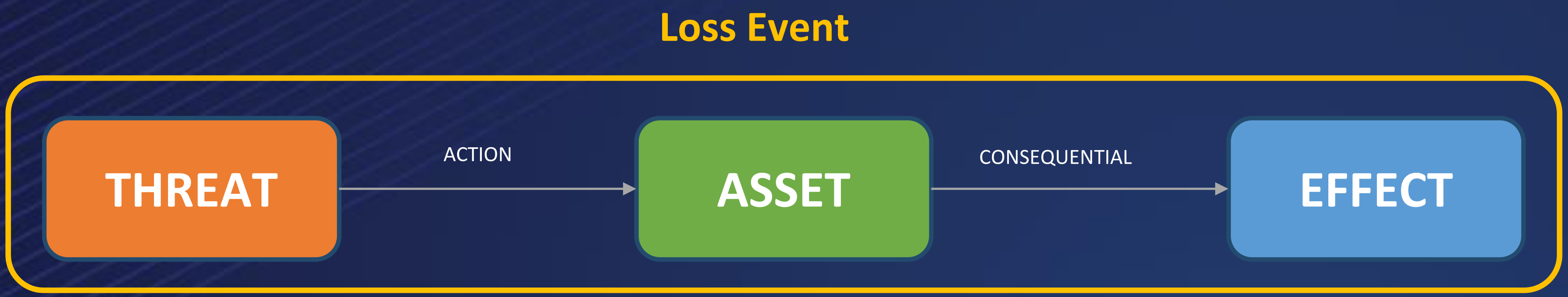
- ➢ Sensitive records would not be viewable to public with tokenization

Steps to Perform a FAIR-Based Cost-Benefit Analysis

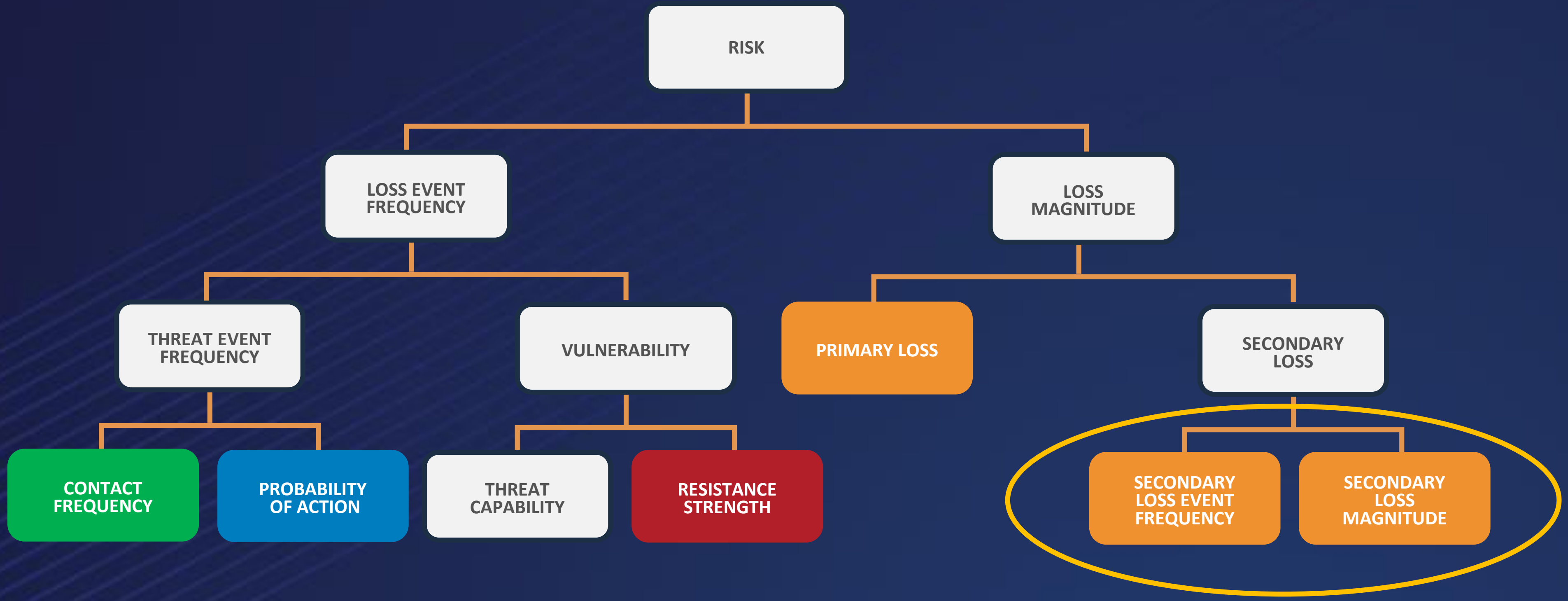
1. Identify and analyze baseline loss event(s)
2. Determine which factor(s) of the FAIR model are impacted
3. Update baseline analysis for FAIR Model factor(s) impacted
4. Compare analysis deltas to annualized investment cost

Step 1: Identify and analyze baseline loss event(s)

The risk associated with an external **malicious actor** breaching **PII from a database cluster** supporting the customer order system, resulting in a **loss of confidentiality**.



Step 2: Determine which factor(s) of the FAIR model are impacted



Avoidance

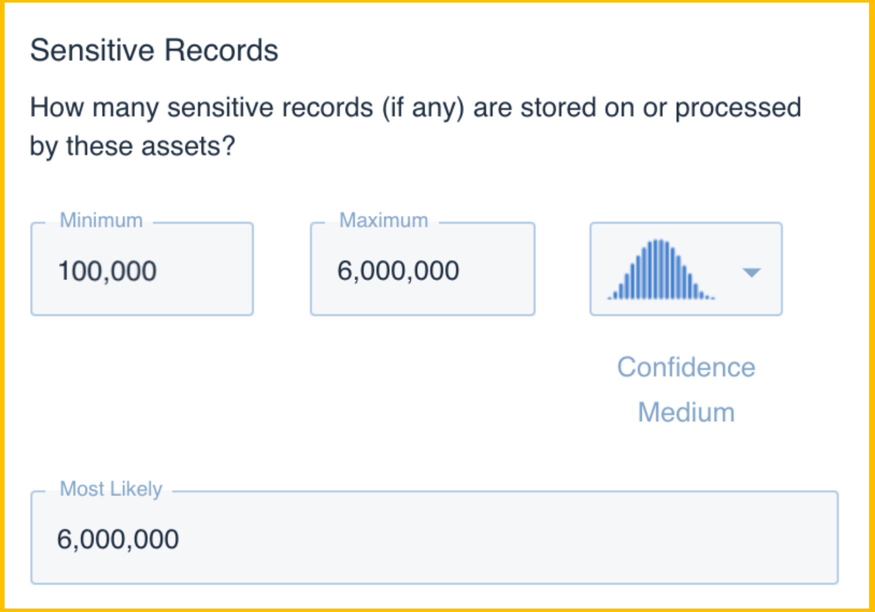
Deterrence

Resistance / Vulnerability

Detective / Responsive

Step 3: Update baseline analysis for FAIR Model factor(s) impacted

Data Purge



Sensitive Records

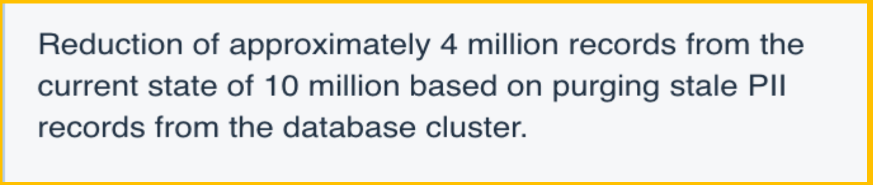
How many sensitive records (if any) are stored on or processed by these assets?

Minimum: 100,000

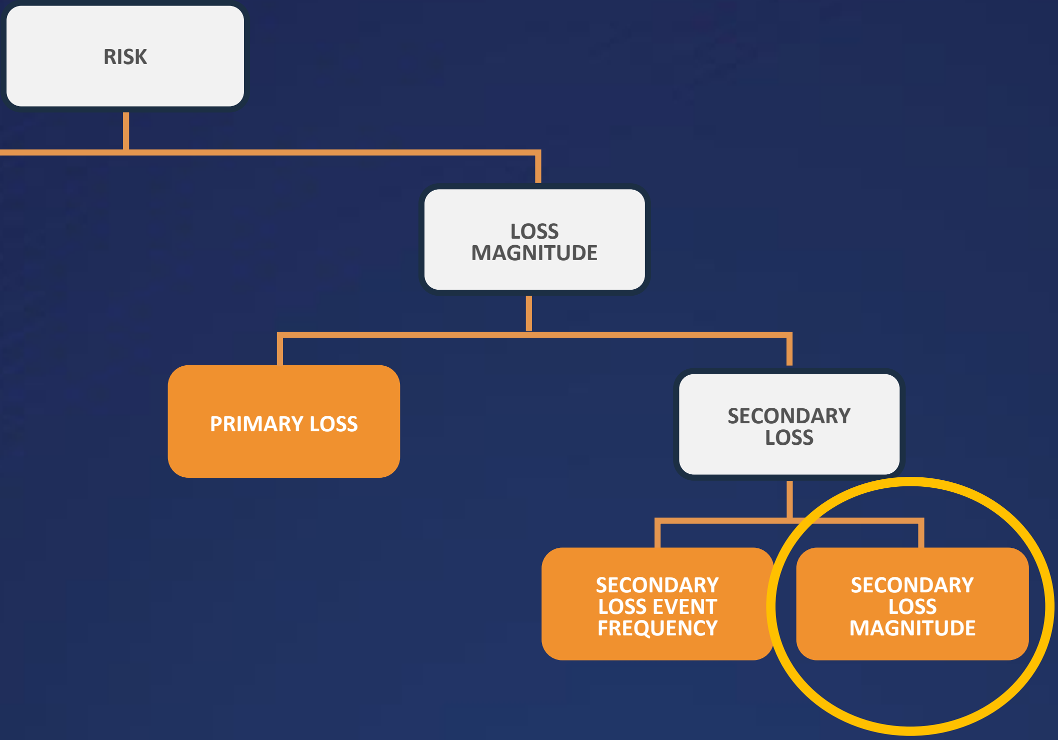
Maximum: 6,000,000

Confidence: Medium

Most Likely: 6,000,000



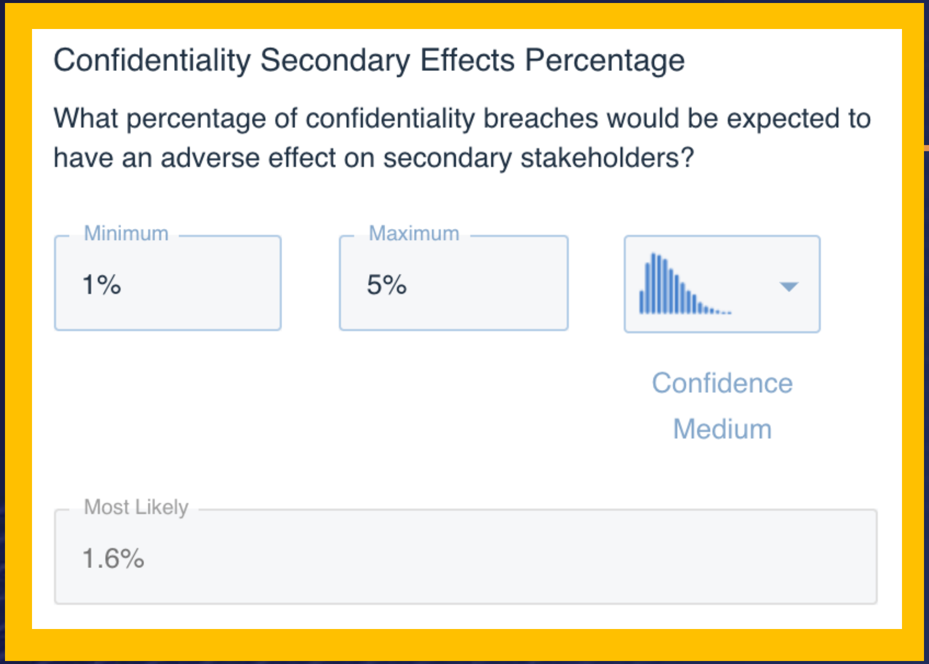
Reduction of approximately 4 million records from the current state of 10 million based on purging stale PII records from the database cluster.



Reduction of potential number of PII records stolen

Step 3: Update baseline analysis for FAIR Model factor(s) impacted

Tokenization



Confidentiality Secondary Effects Percentage

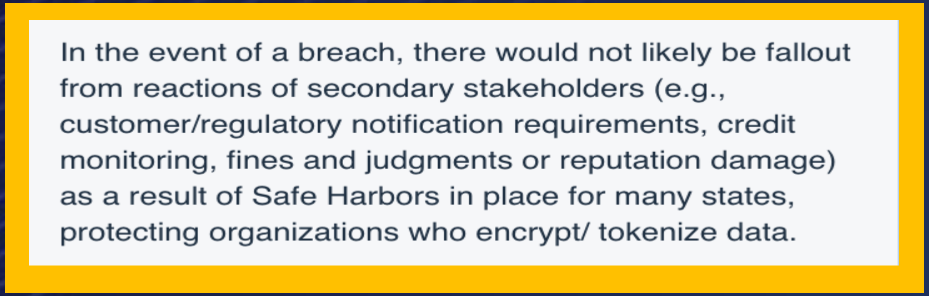
What percentage of confidentiality breaches would be expected to have an adverse effect on secondary stakeholders?

Minimum: 1%

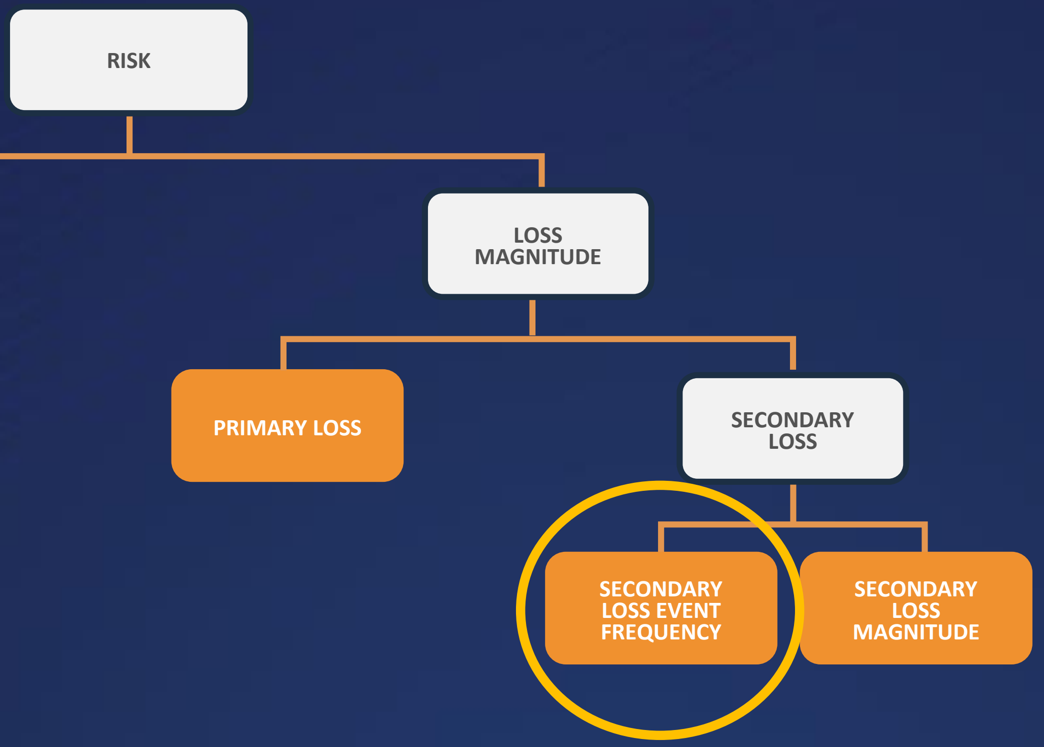
Maximum: 5%

Confidence: Medium

Most Likely: 1.6%

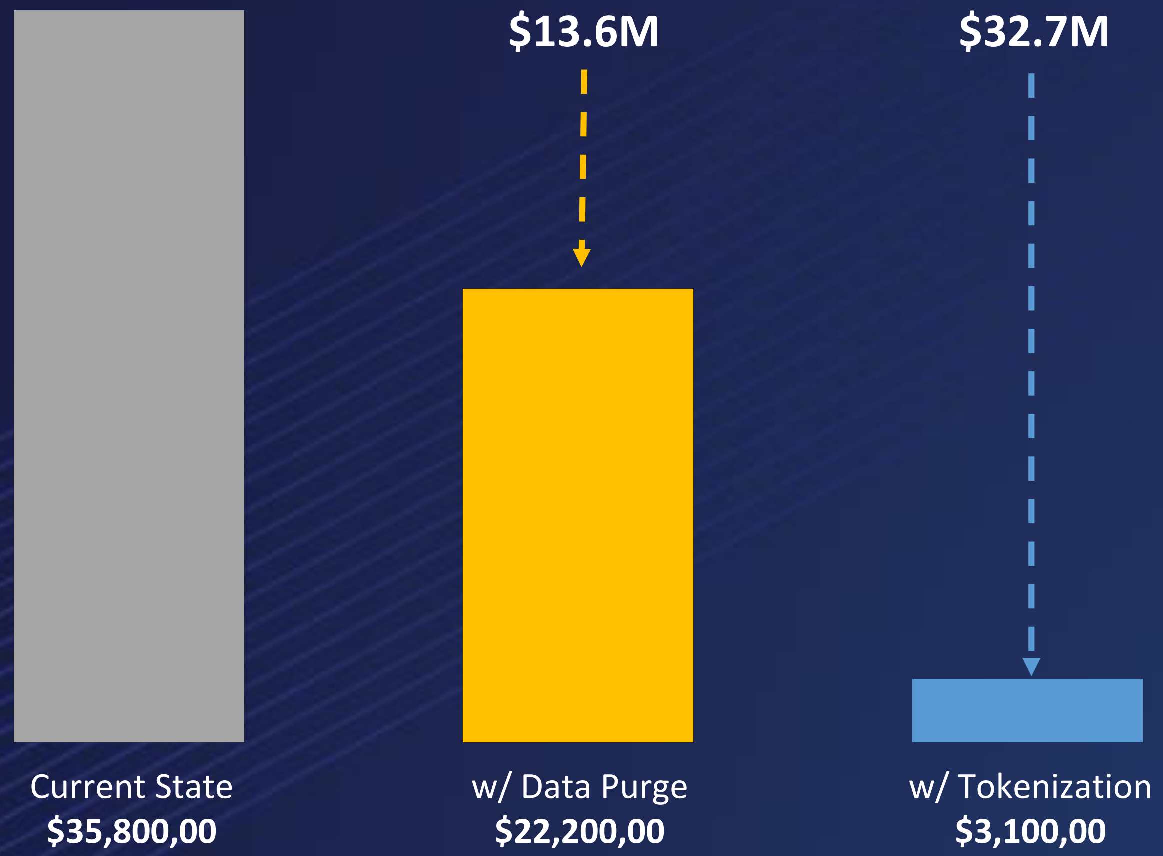


In the event of a breach, there would not likely be fallout from reactions of secondary stakeholders (e.g., customer/regulatory notification requirements, credit monitoring, fines and judgments or reputation damage) as a result of Safe Harbors in place for many states, protecting organizations who encrypt/ tokenize data.



Reduction in the likelihood of fallout from secondary stakeholders

Step 4: Compare analysis deltas to annualized investment cost



Annualized Loss Exposure

Data Purge

$13.6M

RISK REDUCTION

VS.

$XX

INVESTMENT

Tokenization

$32.7M

RISK REDUCTION

VS.

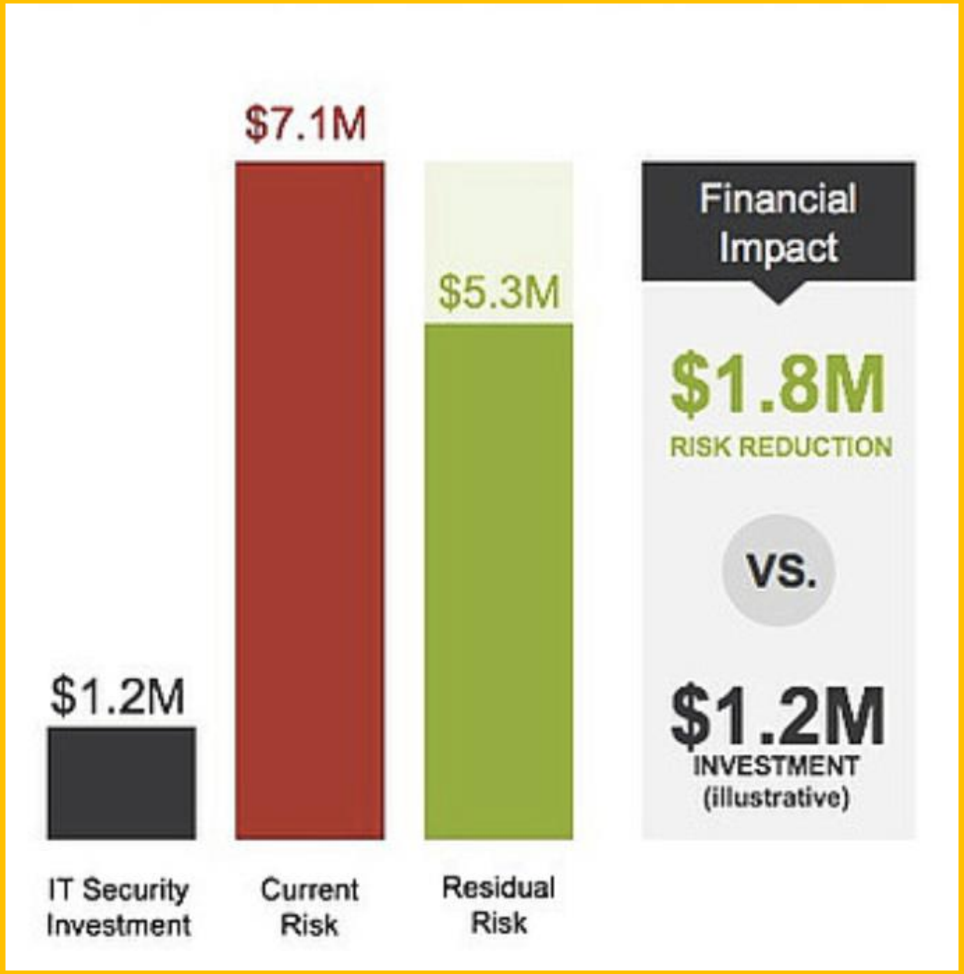
$XX

INVESTMENT

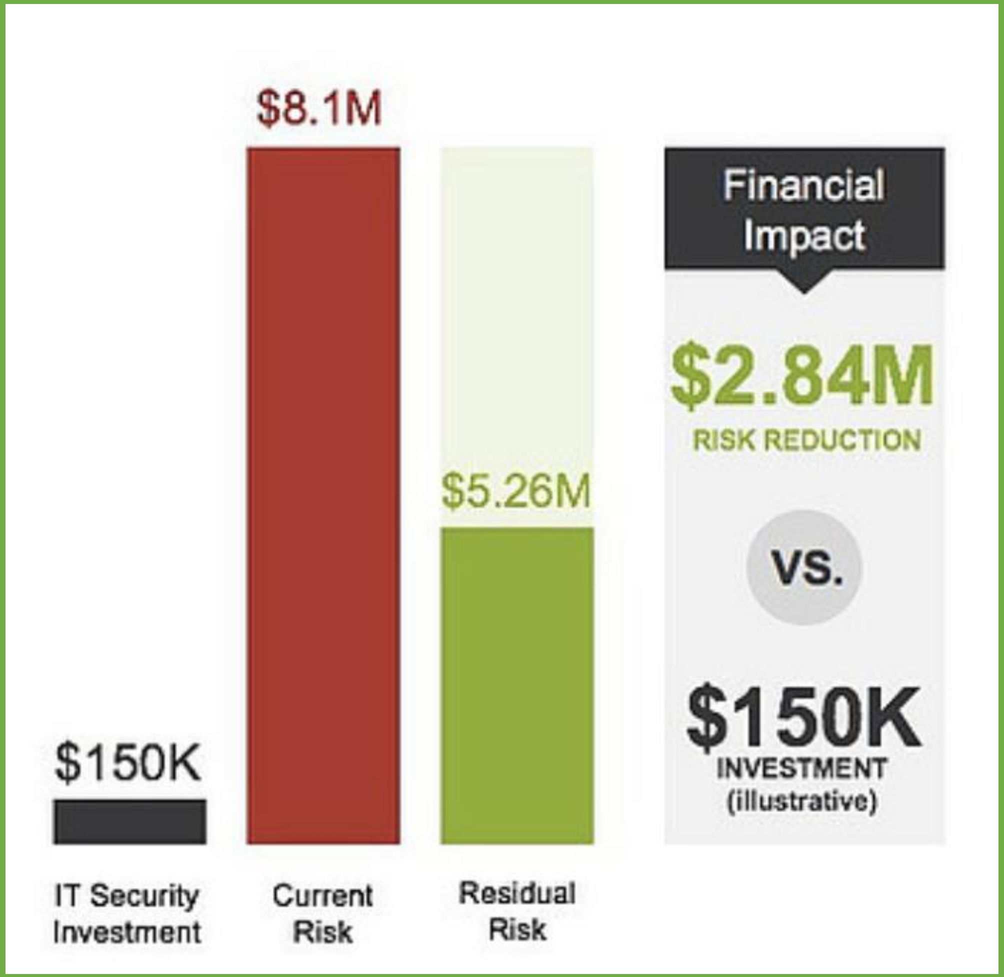
Case Study ***#2***

What’s the **ROI** for a Cybersecurity Investment?

Endpoint Module for Zero Day Threats



Proxy Anywhere Solution

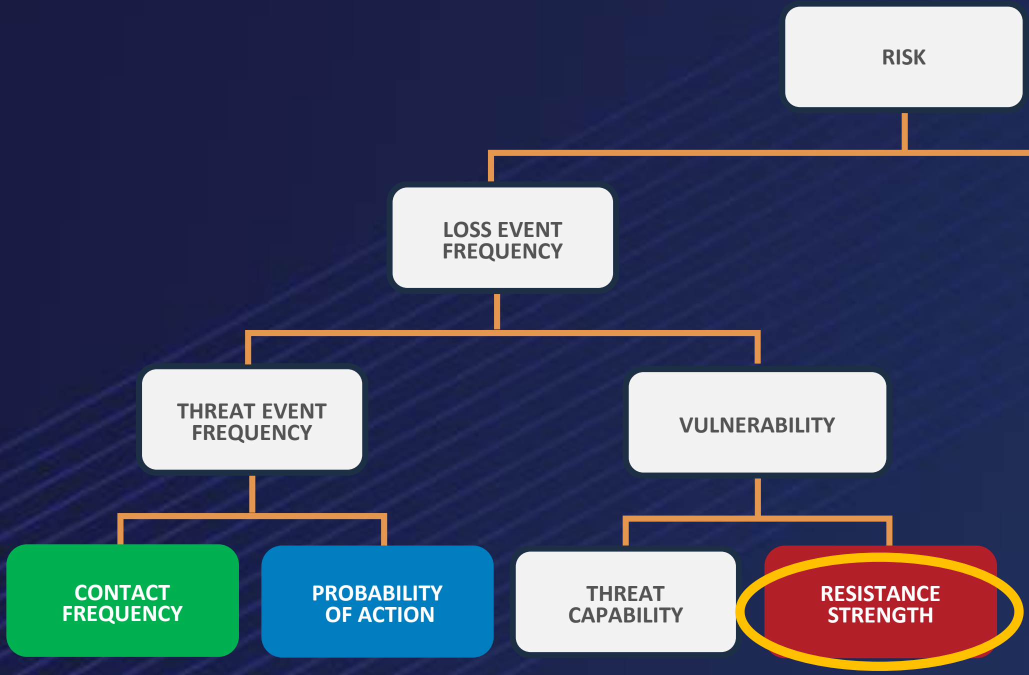


Case Study ***#3***

Using FAIR to Evaluate a High-Risk Audit Finding

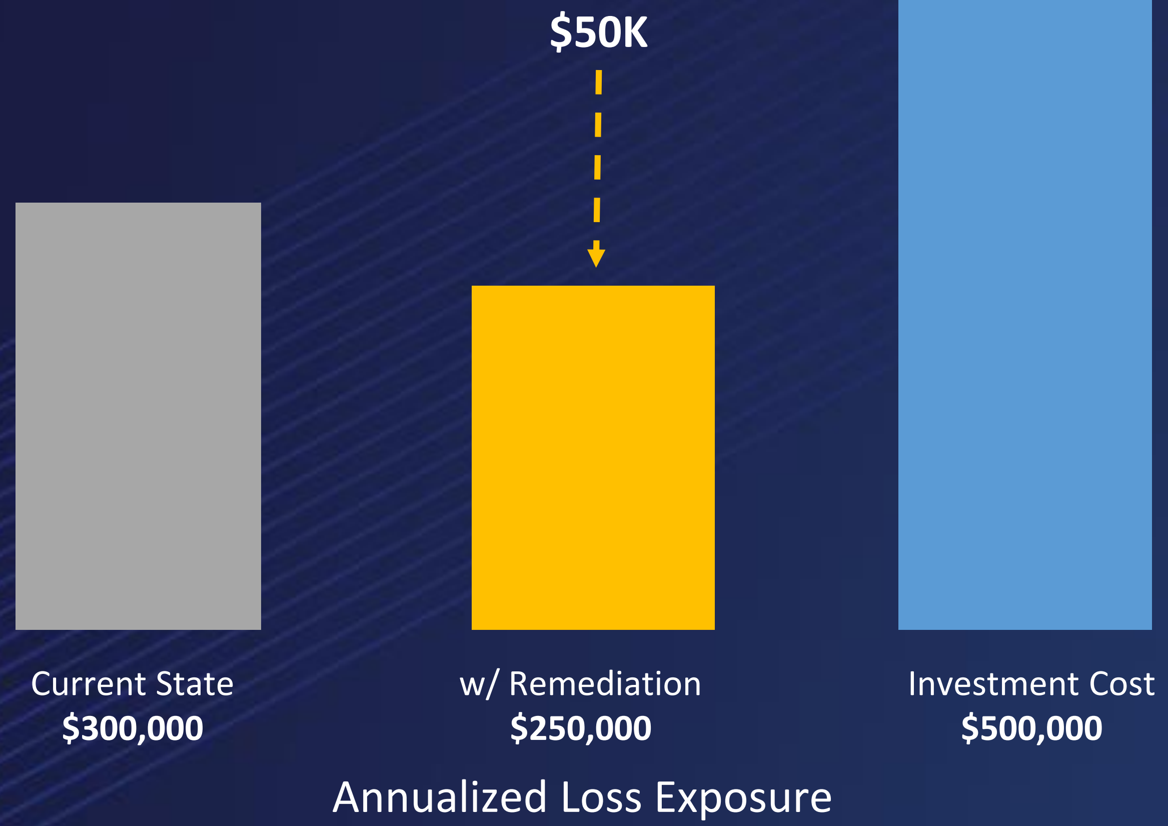
"The patching process for the Enterprise Resource Planning (ERP) platform was not meeting policy expectations"

Audit Finding



Recommendation from Audit
Execute upgrades ahead of schedule and optimize patch management efforts to ensure compliance with patch management policies

Cost-Benefit of Remediating “High” Risk Audit Finding



Key Takeaways

Audit finding should not be classified as “high” based on materiality

Alternative investments should be considered to justify the remediation

In Summary

Instead of this…

“We need this new software/control

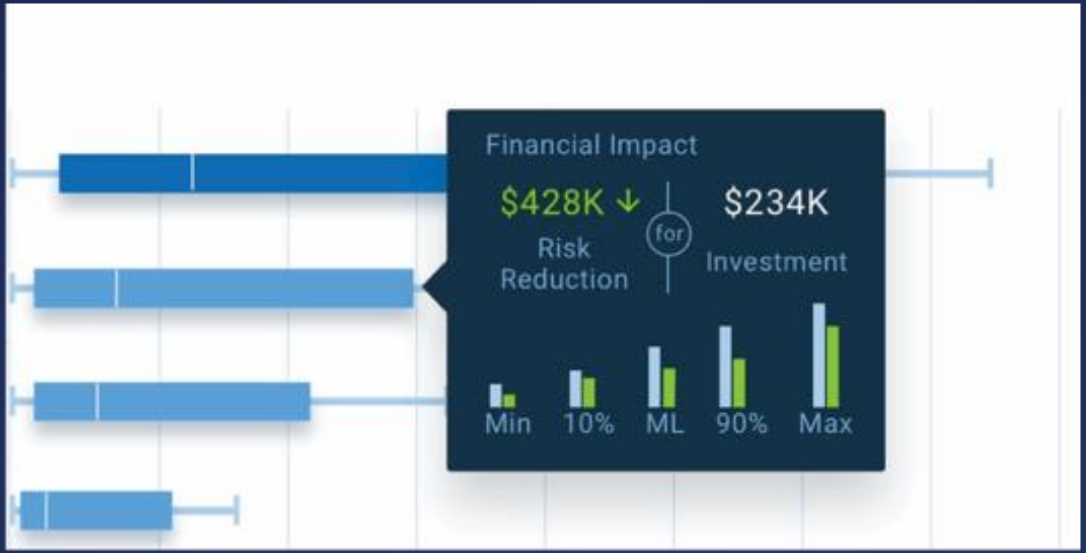
because we’re currently at high risk of experiencing

a data breach.

The likelihood is **medium** and the impact is high,

meaning it’s a high risk.”

You could have this:



Reduction in forecasted loss: $428K
Cost of control: $234K

Priorities

1 ________________________________

2 ________________________________

3 ________________________________

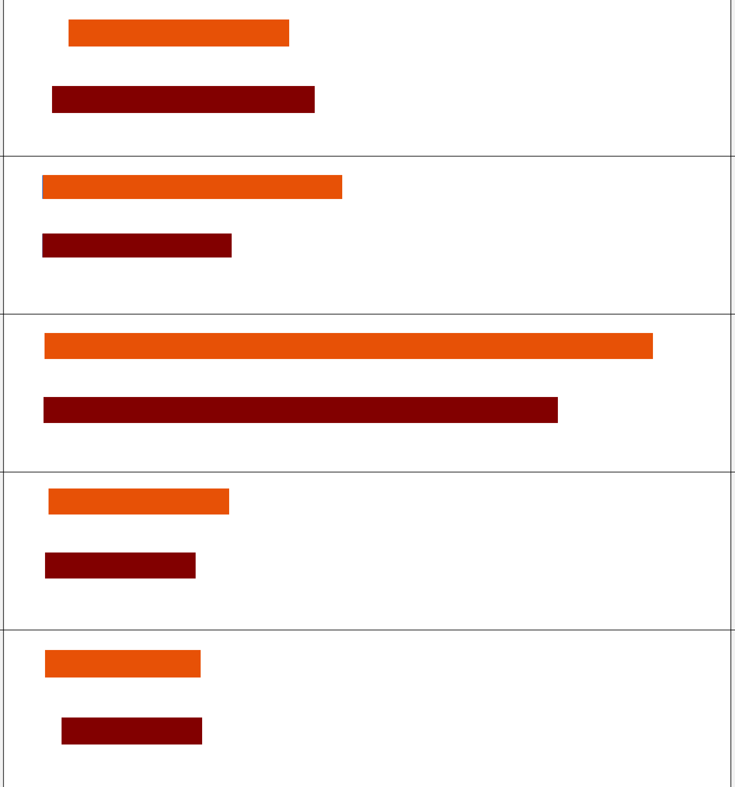
Every organization has limited resources: People, Time, Budget

Prioritization is a requirement for your your risk management program

“Which risk should we mitigate?”

“How do I know what I should tackle next?”

Strategy #1 Focus on the areas where exposure is the greatest



Risk Theme	Org	Range of Exposure (10th-90th)
Systems Failure Outage of key systems (DDOS, Ransomware)	BU1 BU2	$500K – $4M $250K – $5M
Identity Management Confidentiality loss by stolen or shared credentials	BU1 BU2	$20K – $6M $15K – $3.5M
Patch Management Confidentiality loss by exploited application system	BU1 BU2	$45K – $11.5M $10K – $10M
Endpoint Malware Confidentiality loss due to malware / malicious code on endpoint	BU1 BU2	$150K – $3.5M $75K – $3M
Human Error Confidentiality loss due to mis-handling / mis-deliver of Customer data	BU1 BU2	$75K – $3M $400K – $3M

Key Takeaway

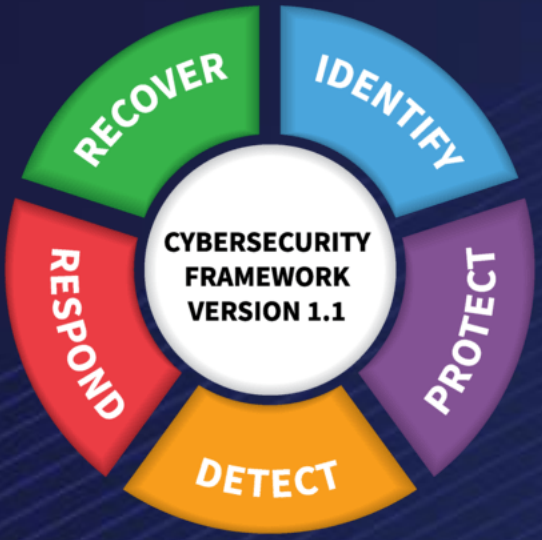
We should prioritize our resources in mitigating risk related to Patch Mgt.

Steps to develop a cyber risk dashboard

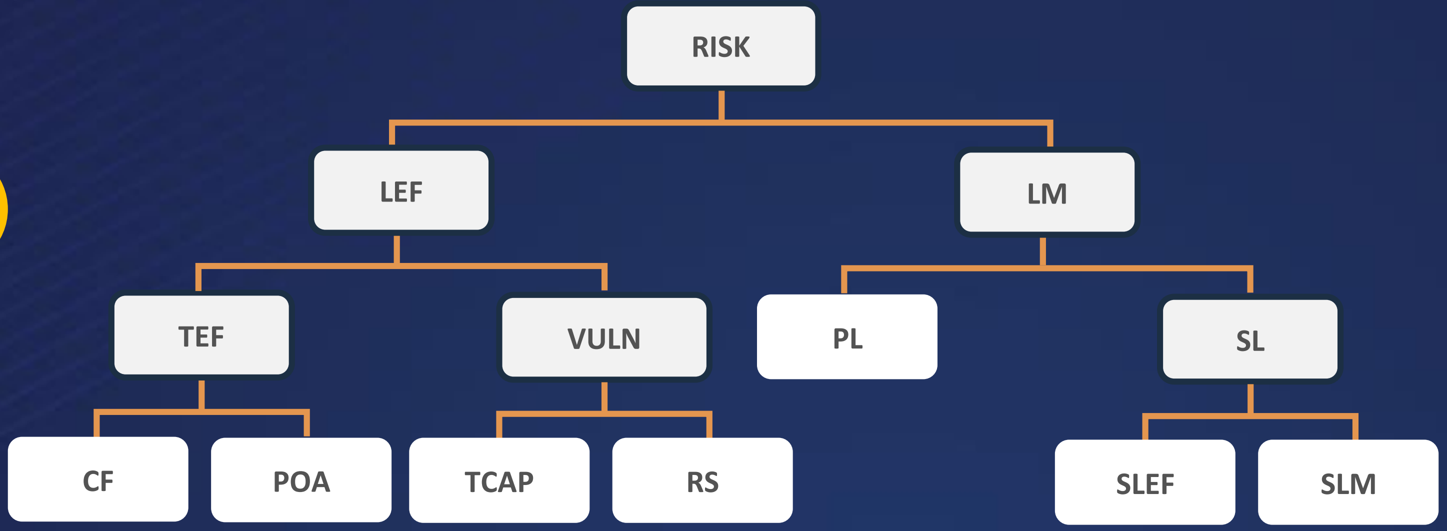
1. Identify and define risk themes
2. Analyze quantitatively the exposure of each theme
3. Show uncertainty (Don’t hide it!)
4. Compare risk themes to each other

Strategy #2

Bring an economic component to existing approaches, like NIST CSF



+



Key Takeaway

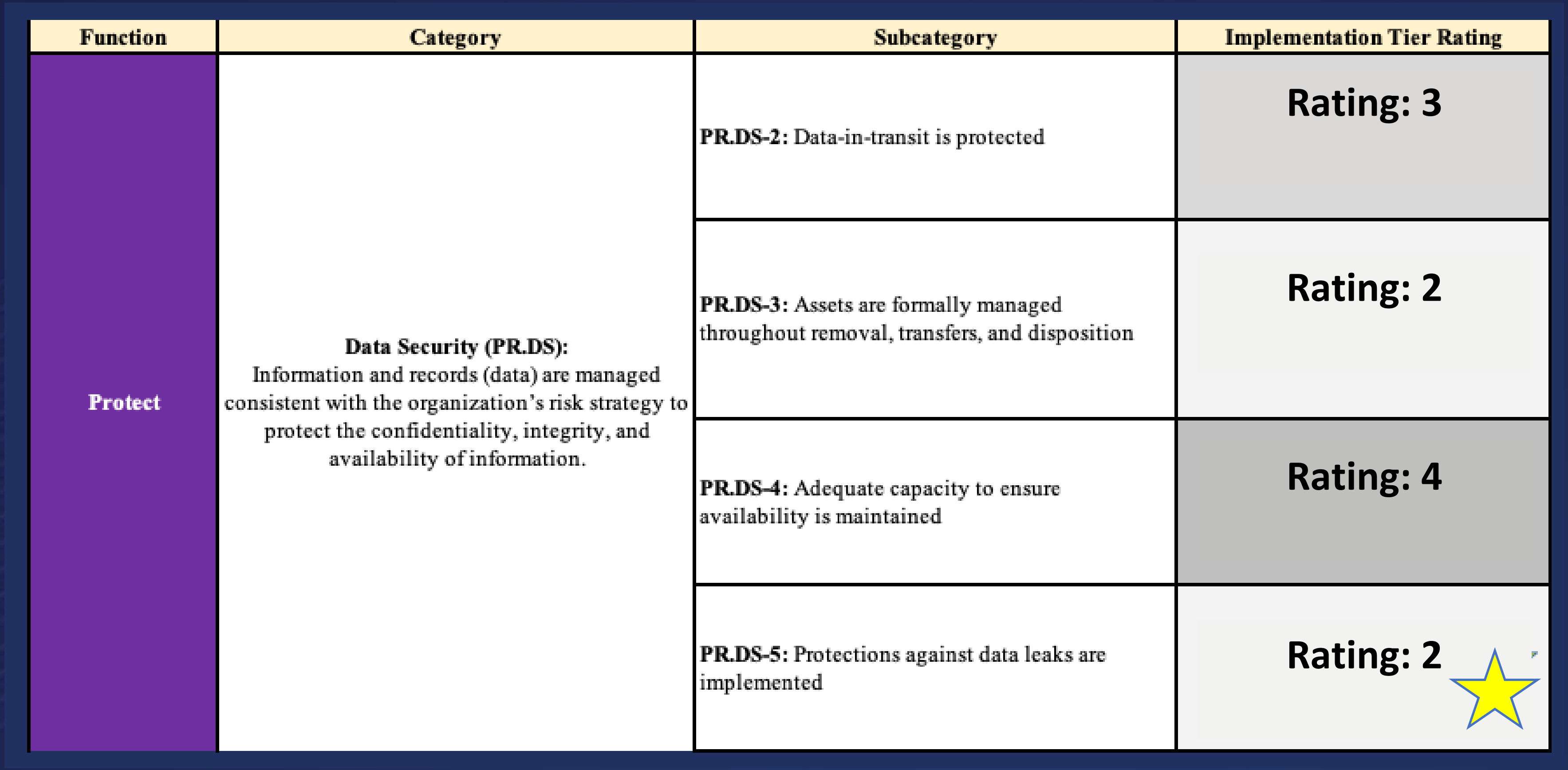
FAIR is often a compliment to existing security frameworks

Common Today:

Key Questions?

How do we prioritize where to focus when there are multiple areas that are lower than our targets?

Is spending $2M a good business case to move from a 2 -> 4?



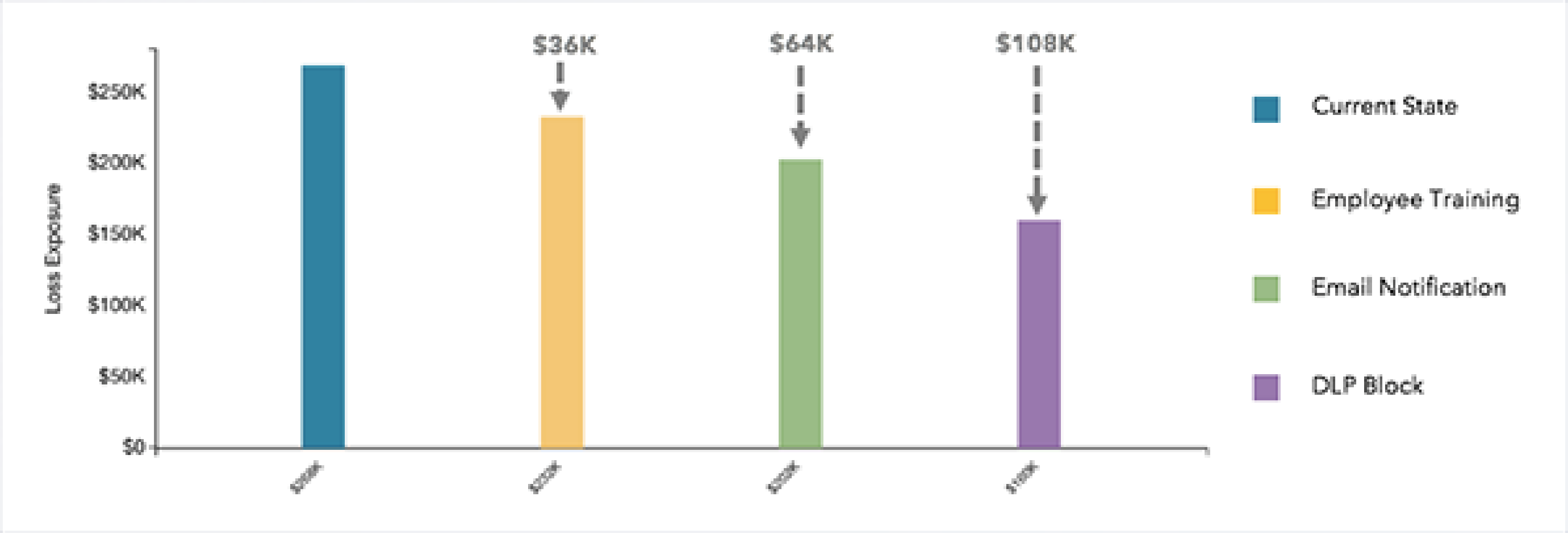
Function	Category	Subcategory	Implementation Tier Rating
Protect	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected	Rating: 3
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Rating: 2
		PR.DS-4: Adequate capacity to ensure availability is maintained	Rating: 4
		PR.DS-5: Protections against data leaks are implemented	Rating: 2 ☆

"We should spend $2M within the next year on enhancing DLP because we have a maturity score of 2 and we feel we should be a 4."

Future State:

One example as part of a larger business case:

We observed that accidental incidents account for majority of data leakage. Per a FAIR analysis, we showed implementing a DLP Block would only reduce our exposure by an estimated $108K per year. Clearly not justifying a large DLP investment.



Steps to apply within NIST CST

1. Identify CSF subcategory where current state is lower than desired target state (Gap exists)

2. Define risk scenarios associated with that subcategory

3. Perform cost benefit analysis work
   (What Rachel discussed)

4. Communicate the business case associated with NIST CSF ratings to improve prioritization

Step 1: Identify CSF subcategory where current state is lower than the desired target state (Gap exists)

Protect (PR)

Category:	Data Security (PR.DS):
Subcategory:	PR.DS-1: Data-at-rest is protected

Current Rating:
Tier 2: Risk Informed

Target Rating:
Tier 3: Repeatable

Step 2: Define risk scenarios associated with that subcategory

Protect (PR)

Category: Data Security (PR.DS):

Subcategory: PR.DS-1: Data-at-rest is protected

Current Rating:
Tier 2: Risk Informed

Target Rating:
Tier 3: Repeatable

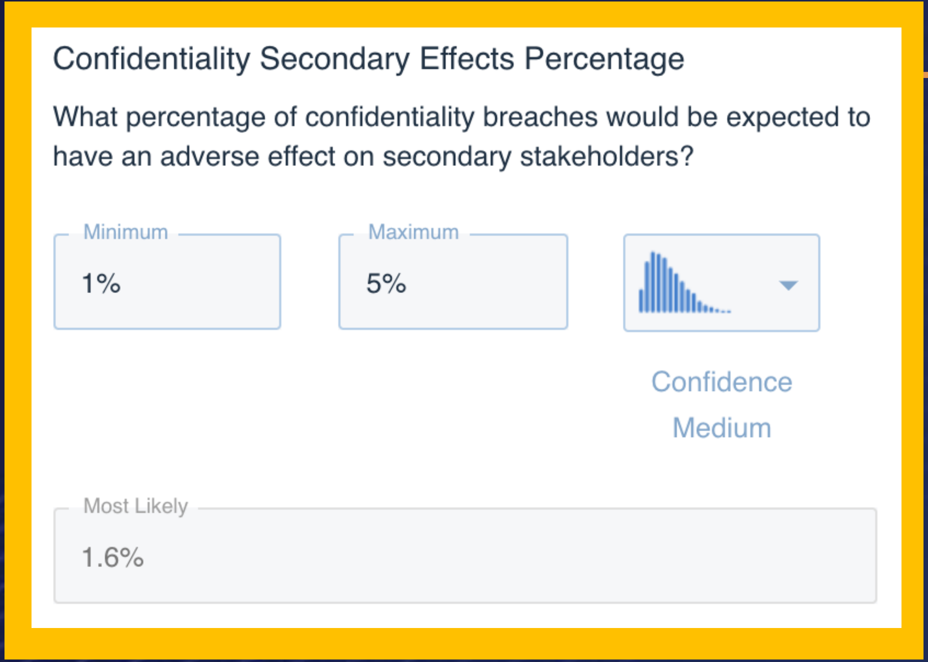
Breach of sensitive customer data by malicious insider from Shared Drive environment

+

Breach of sensitive customer data by Cybercriminal from unencrypted crown jewel database

Step 3: Perform cost benefit analysis work

Tokenization



Confidentiality Secondary Effects Percentage

What percentage of confidentiality breaches would be expected to have an adverse effect on secondary stakeholders?

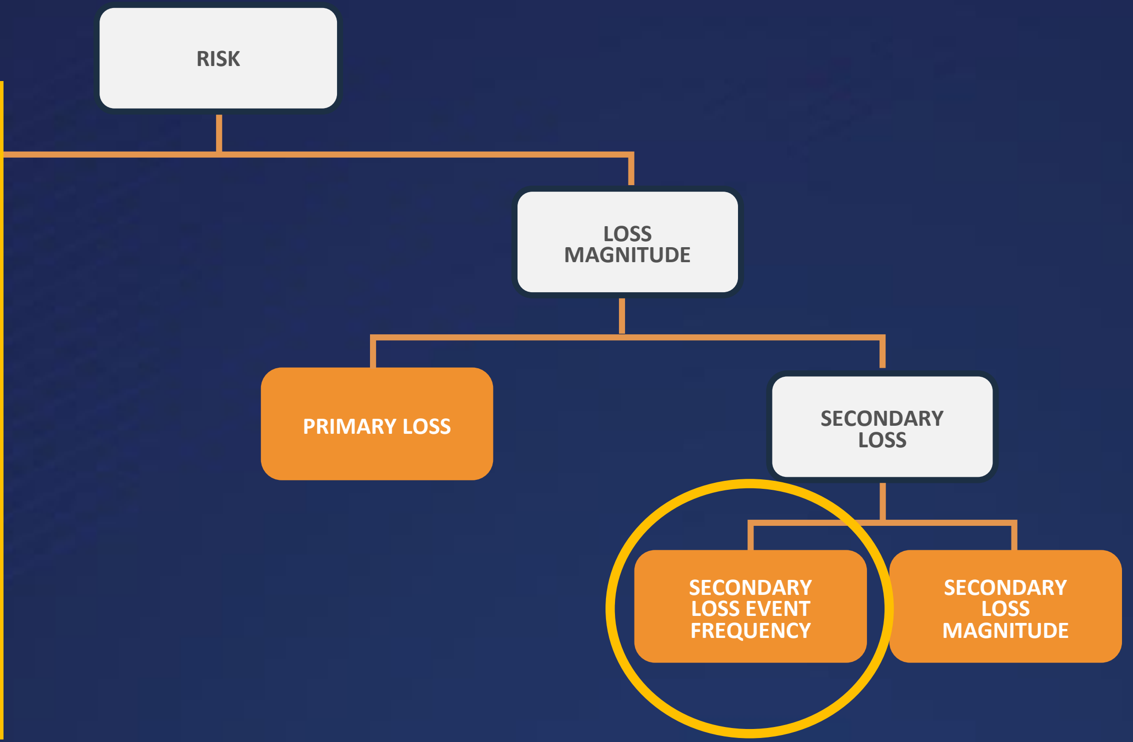
Minimum: 1%

Maximum: 5%

Confidence: Medium

Most Likely: 1.6%

In the event of a breach, there would not likely be fallout from reactions of secondary stakeholders (e.g., customer/regulatory notification requirements, credit monitoring, fines and judgments or reputation damage) as a result of Safe Harbors in place for many states, protecting organizations who encrypt/ tokenize data.



Reduction in the likelihood of fallout from secondary stakeholders

Step 4: Communicate the business case associated with NIST CSF ratings to improve prioritization

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Protect (PR)

Category: Data Security (PR.DS):

Subcategory: PR.DS-1: Data-at-rest is protected

Current Rating:
Tier 2: Risk Informed

Target Rating:
Tier 3: Repeatable

Completing 2 identified projects will increase our CSF implementation tier and are estimated to reduce **$800K - $4M** of annualized risk

In Summary

We all have this…

Limited:

People,

Time,

Budget

We need to prioritize…

To ensure we make informed decisions and take action to manage risk effectively

Questions

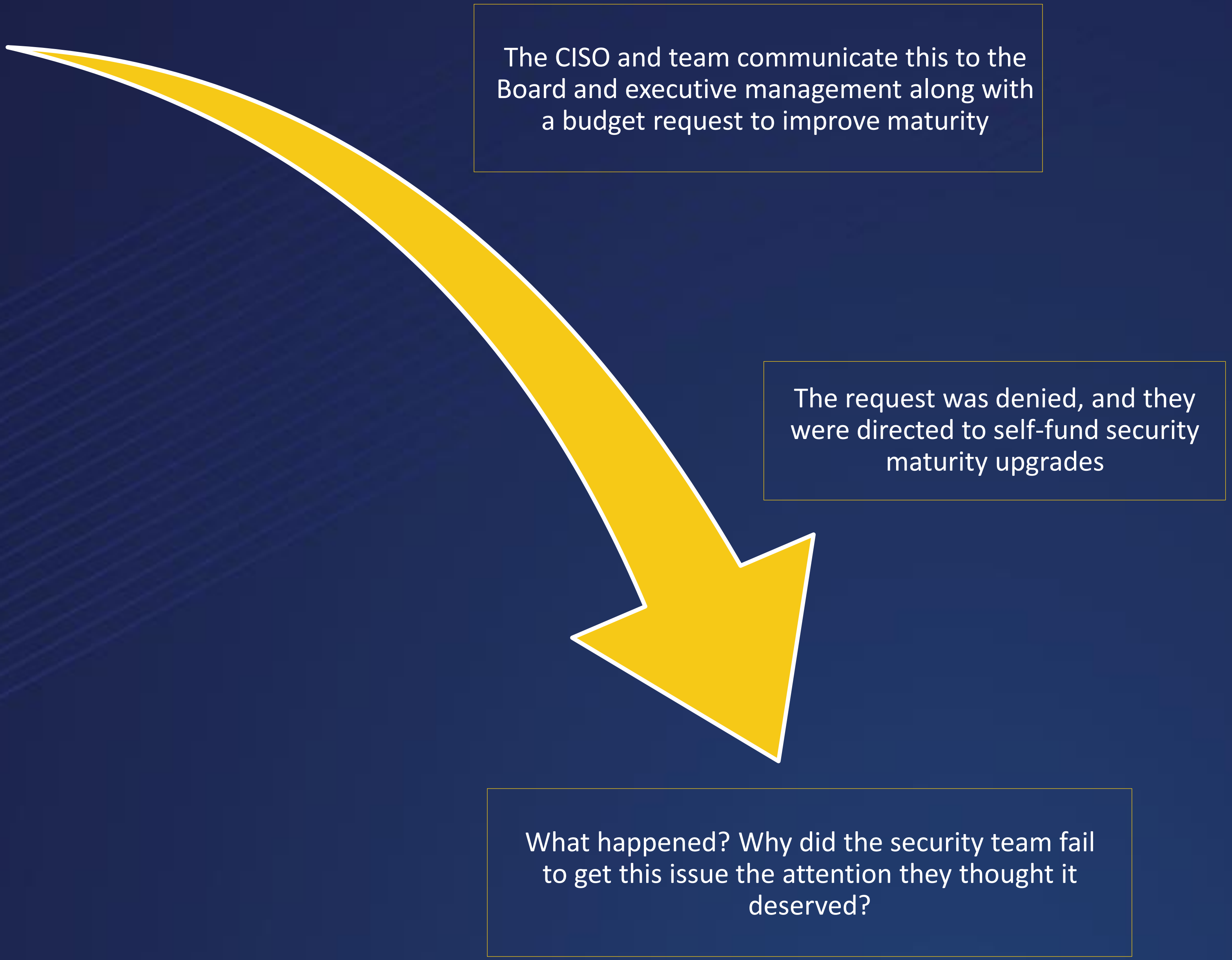
Risk Communication and Reporting

Jack Freund, Ph.D.

Director, Risk Science, RiskLens

FAIR Institute Fellow

A security maturity assessment reveals that an organization has several areas where they need improvement.

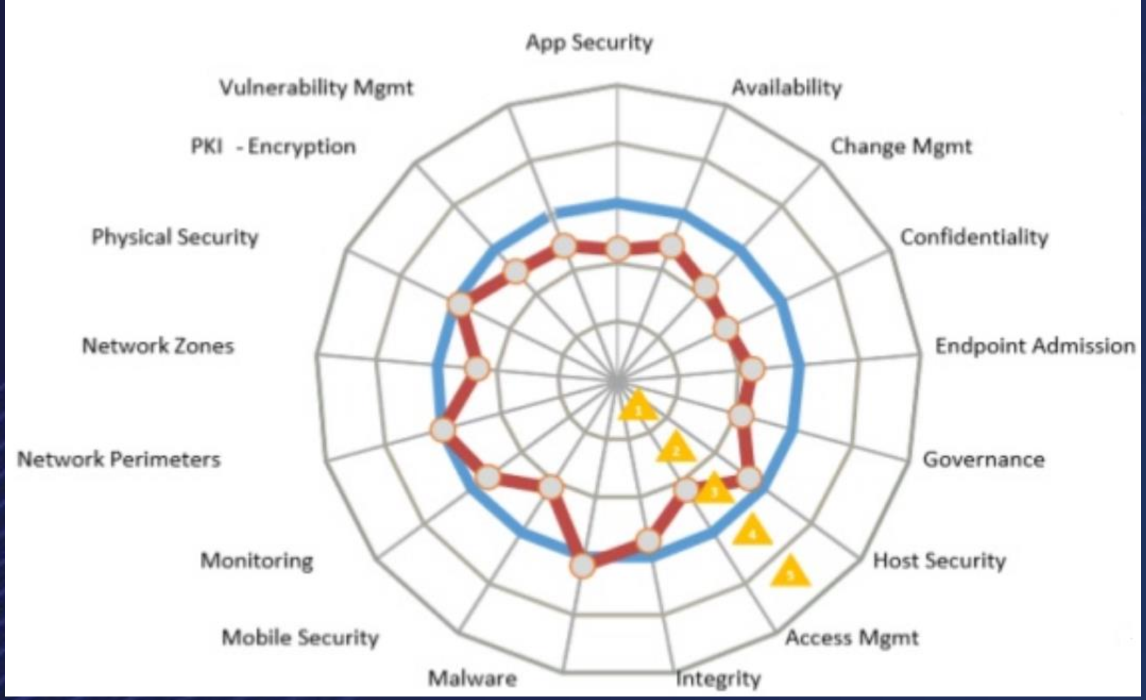


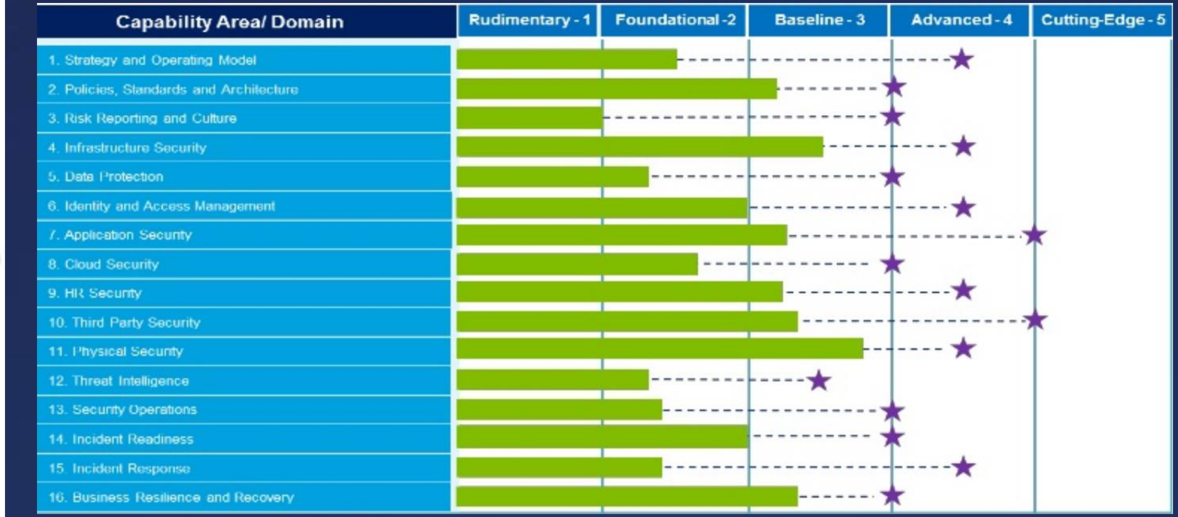
The CISO and team communicate this to the Board and executive management along with a budget request to improve maturity

The request was denied, and they were directed to self-fund security maturity upgrades

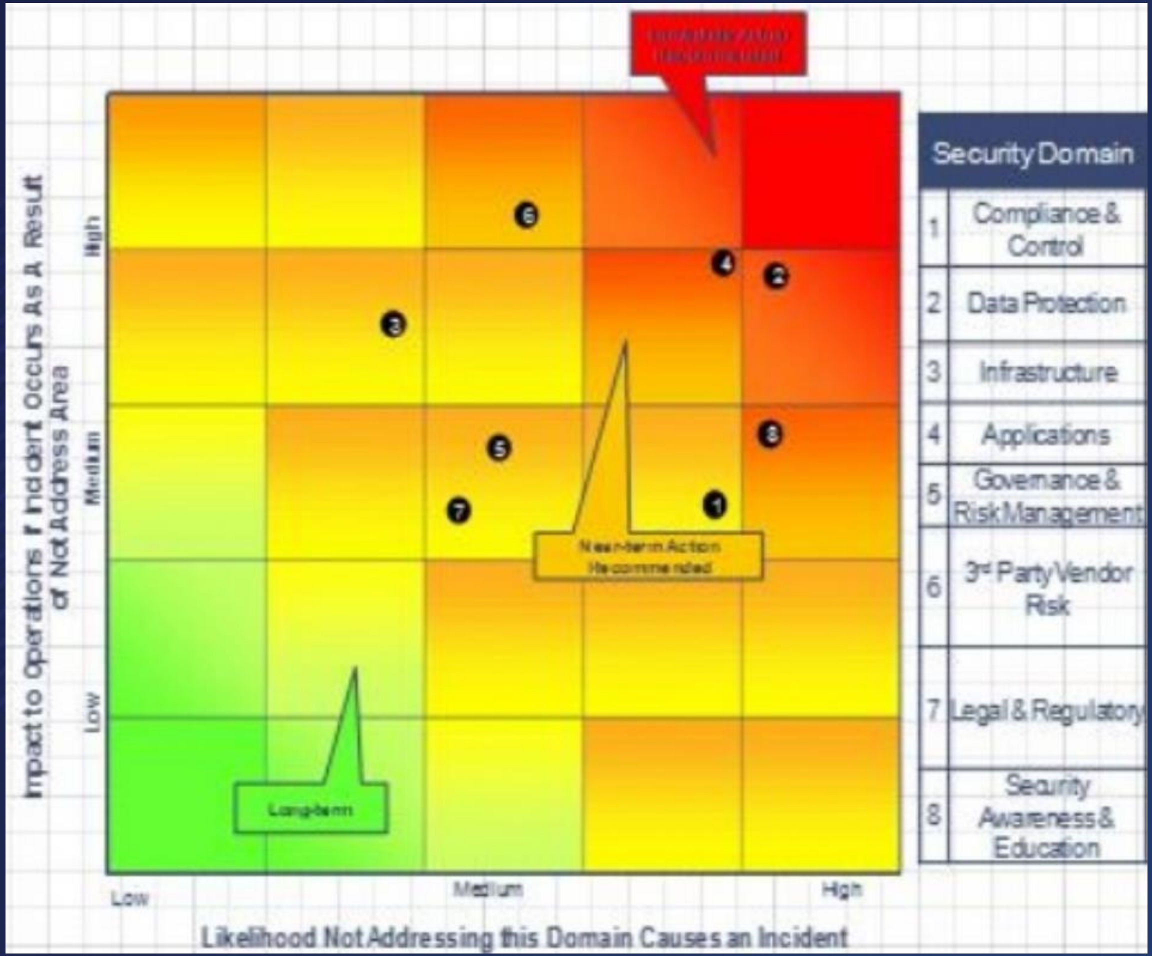
What happened? Why did the security team fail to get this issue the attention they thought it deserved?

Security Maturity Reports



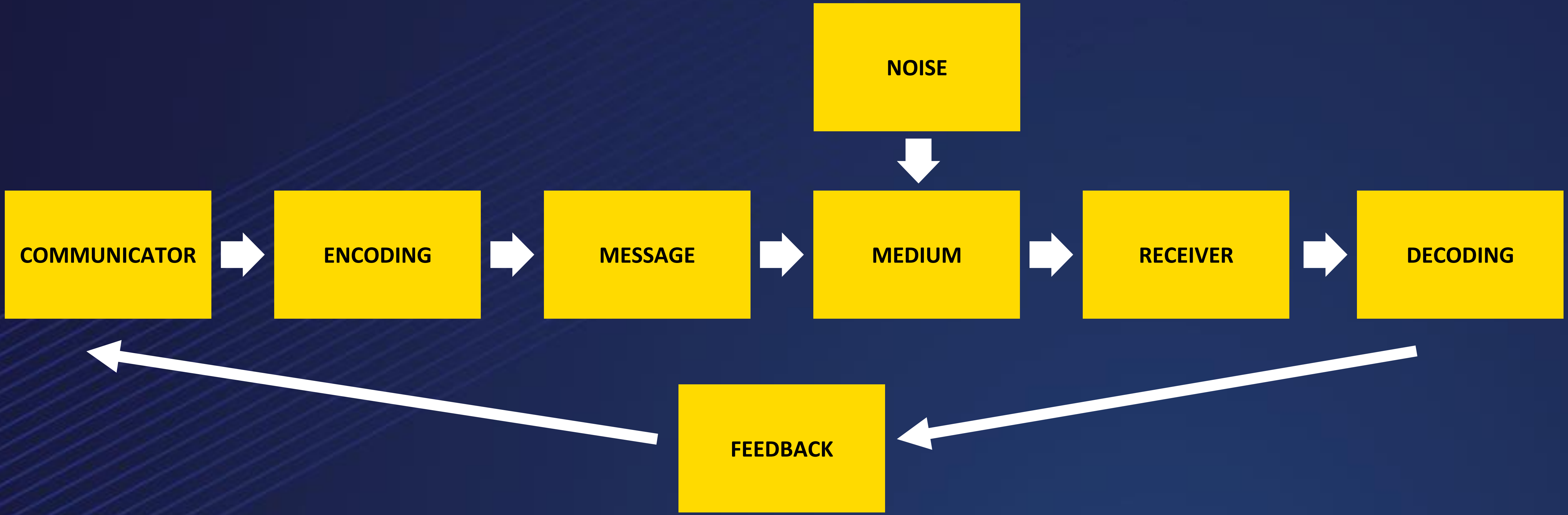


Security Maturity “Risk” Heatmap



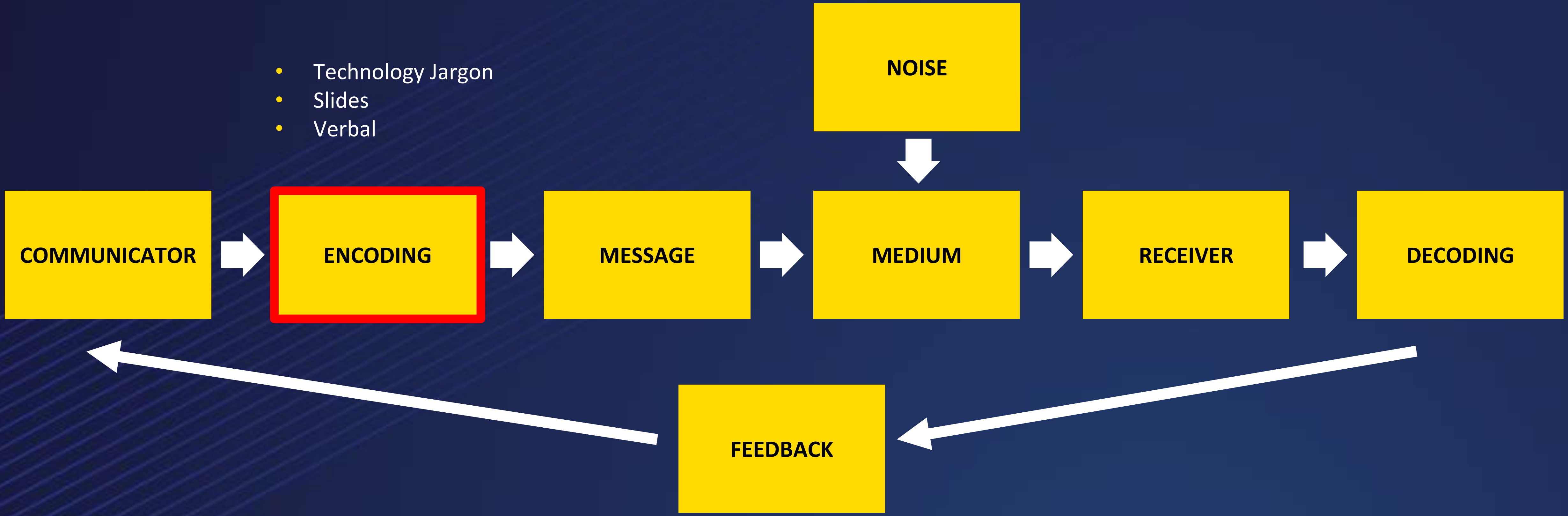
Security Domain	
1	Compliance & Control
2	Data Protection
3	Infrastructure
4	Applications
5	Governance & Risk Management
6	3rd Party Vendor Risk
7	Legal & Regulatory
8	Security Awareness & Education

Contemporary Communication Model



Contemporary Communication Model

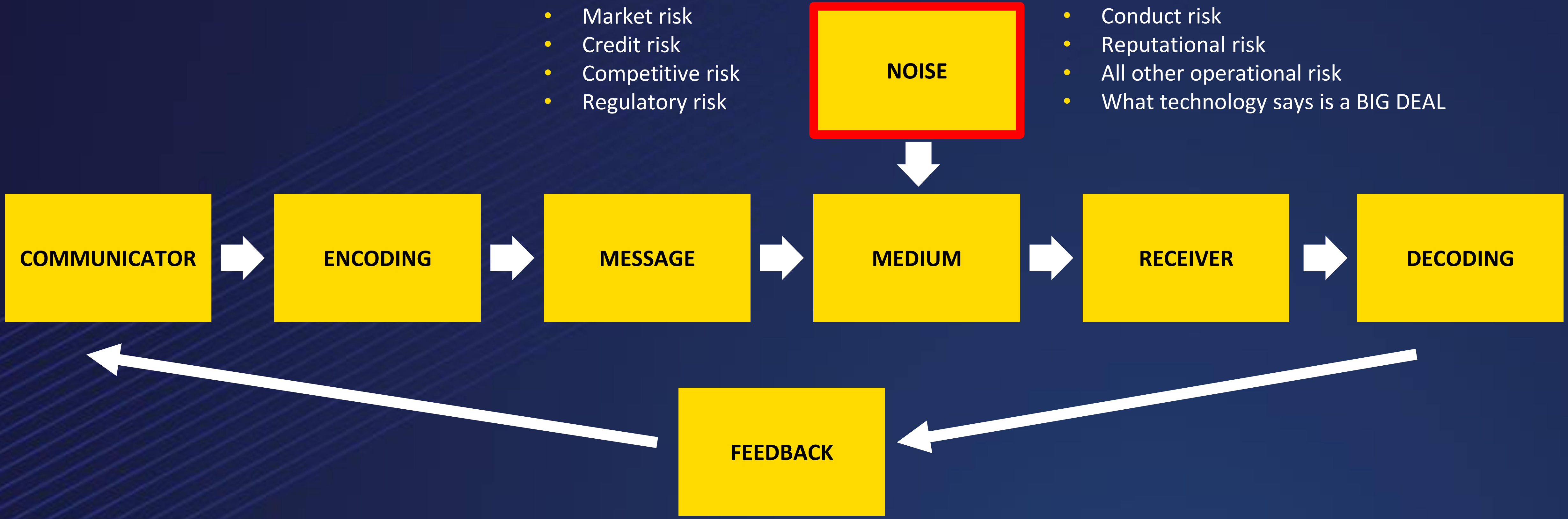
- Technology Jargon
- Slides
- Verbal



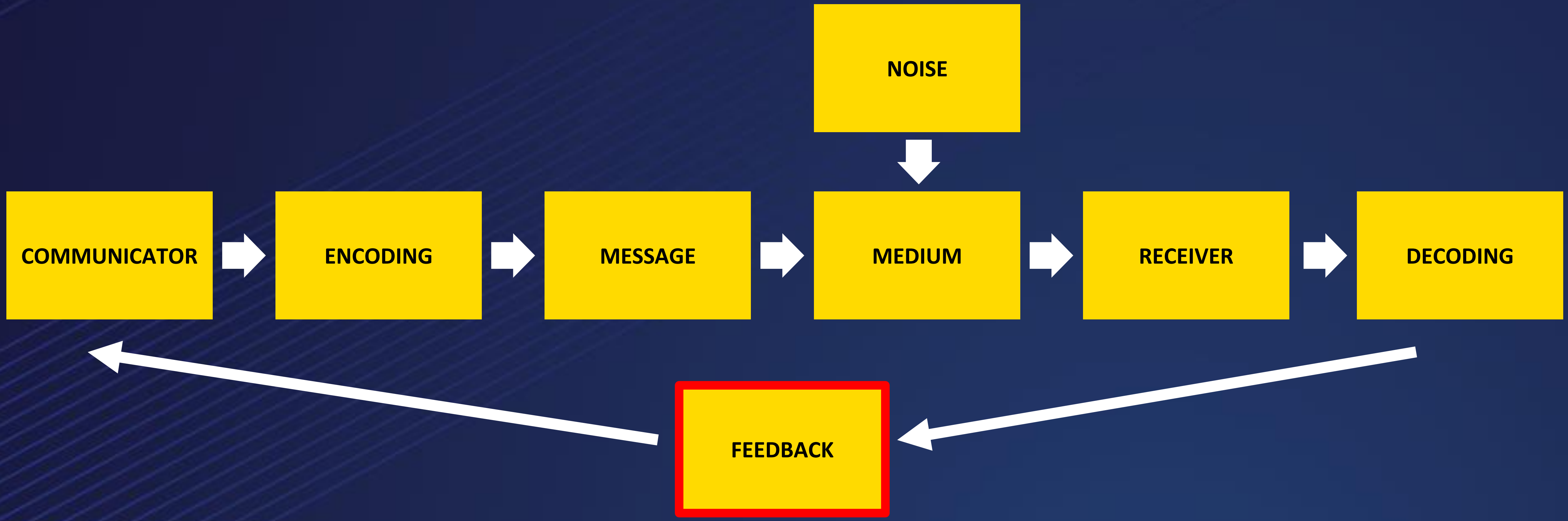
Models of Communication (Modern)

- Market risk
- Credit risk
- Competitive risk
- Regulatory risk

- Conduct risk
- Reputational risk
- All other operational risk
- What technology says is a BIG DEAL



Models of Communication (Modern)



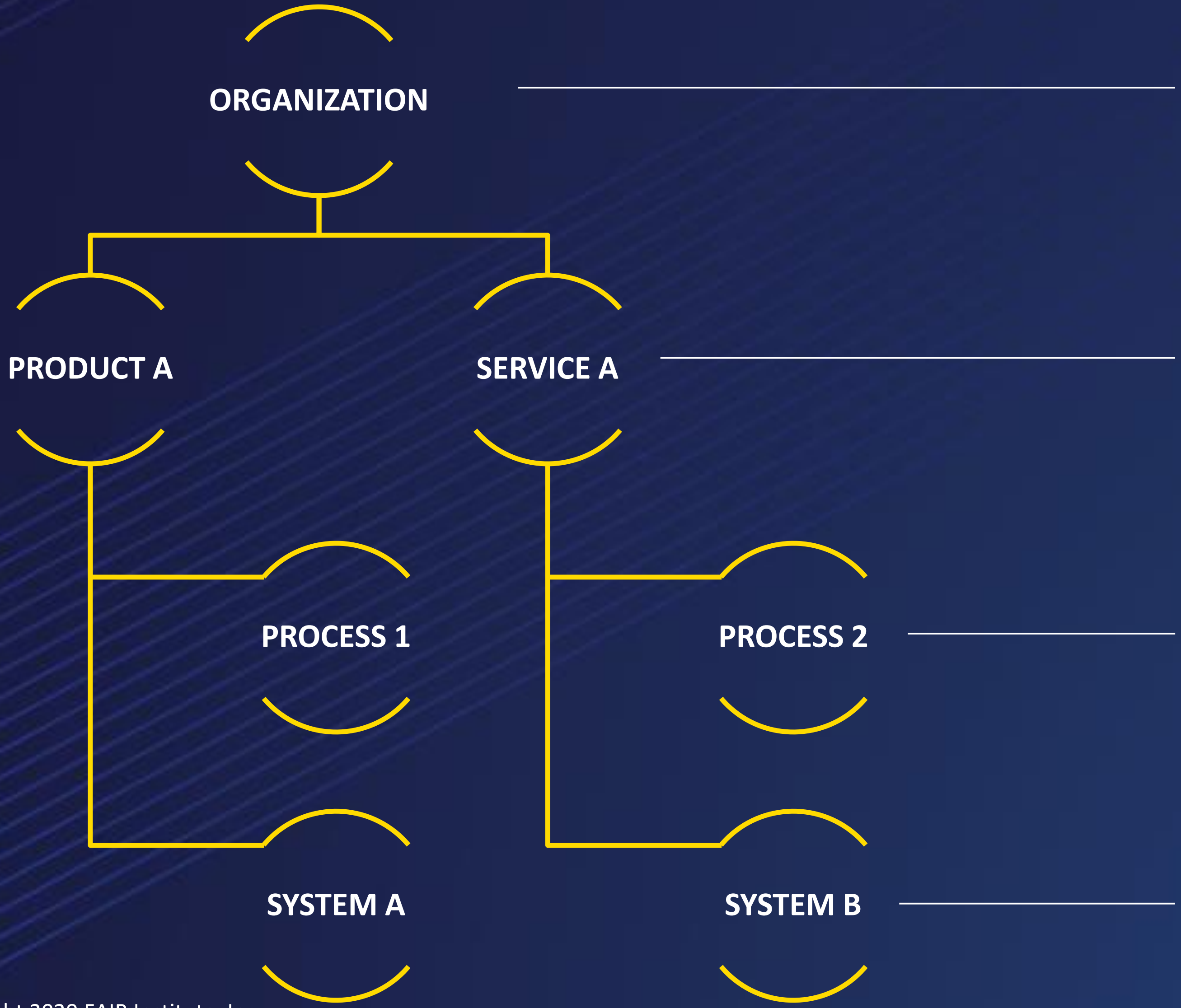
- “Once again, the business didn’t do the things I wanted. I don’t know what’s up with them.”
- “I’ll send them articles about how this vulnerability is a BIG DEAL”
- “They’ll see, once there’s a hack I’ll get the budget I need!”

Loss Event Scenarios

You can only assess the risk associated with a loss event scenario

- Without a loss event, there is **NO** risk
- All risk is about forecasting a **FUTURE** event that may or may not come to pass.

How Organizations Work



ORGANIZATION

PRODUCT A

SERVICE A

PROCESS 1

PROCESS 2

SYSTEM A

SYSTEM B

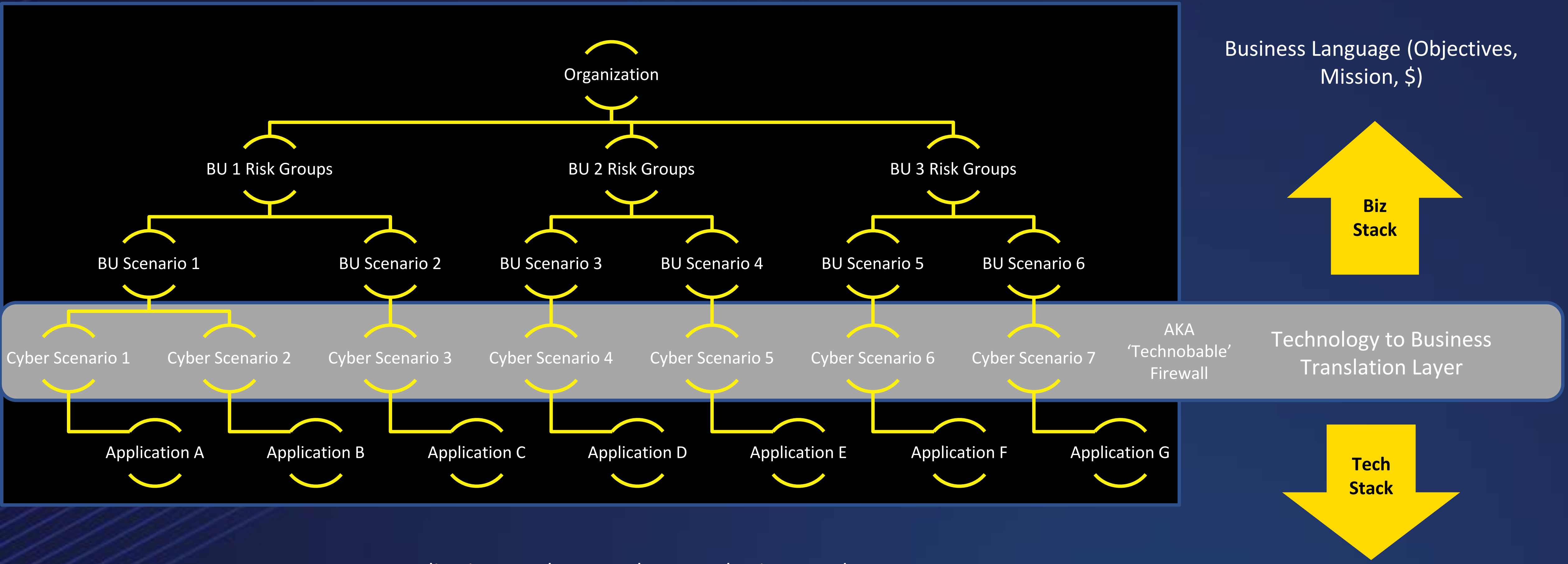
Summary Risks
Big categories that group loss for executives and boards

Business Unit Risks
Tied to things that can go wrong in delivering products and services

Risks to Processes/Technology
Illustrates specific ways that systems can fail/be compromised

All Other Tech
Misconfiguration, patches, upgrades, legacy systems, exploits, etc.

Linking Technology Risk to the Business

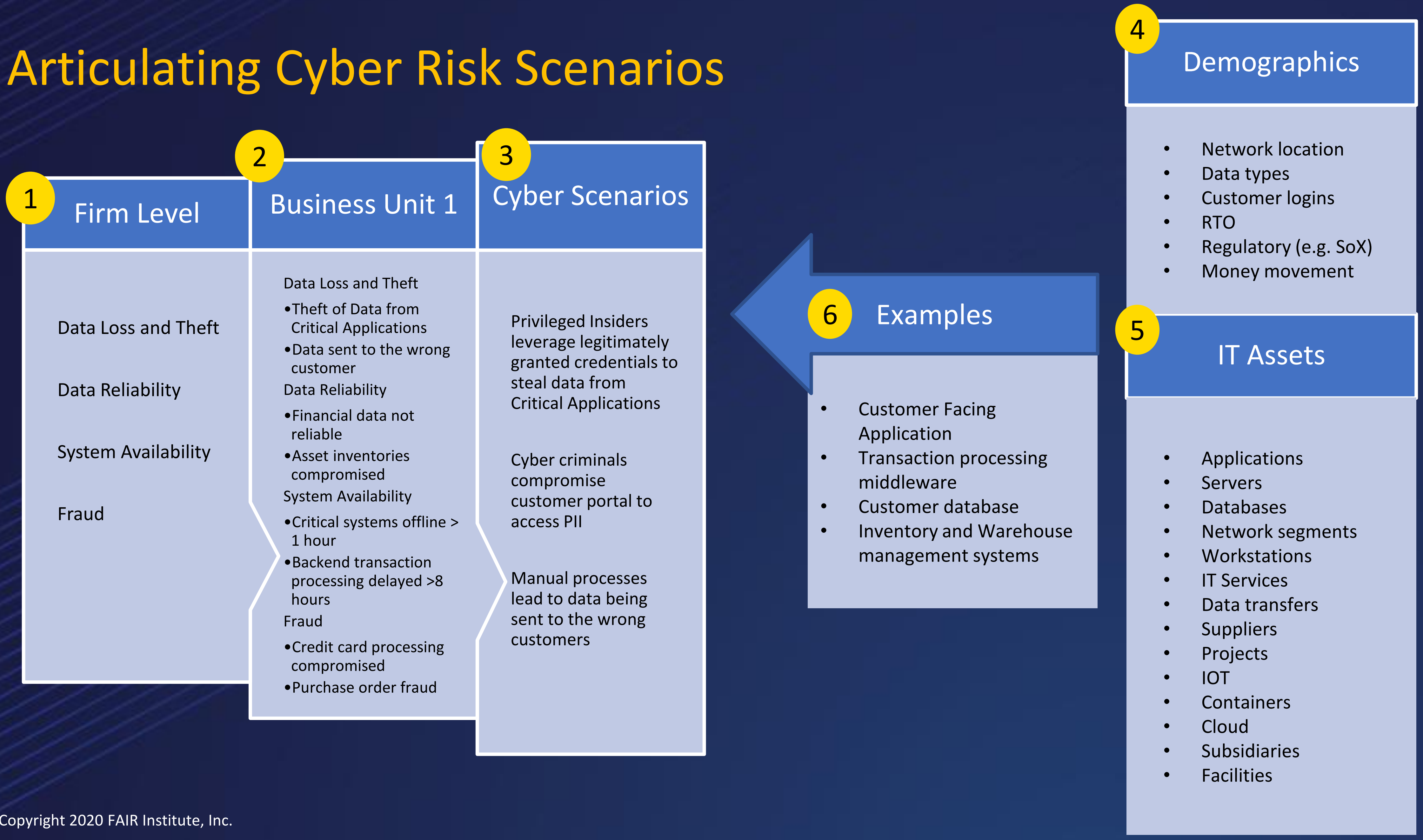


Business Language (Objectives, Mission, $)

Technology Language (Threats, Vulns, Controls)

Application are the nexus between business and technology

Articulating Cyber Risk Scenarios



1 Firm Level

Data Loss and Theft

Data Reliability

System Availability

Fraud

2 Business Unit 1

Data Loss and Theft

- Theft of Data from Critical Applications
- Data sent to the wrong customer

Data Reliability

- Financial data not reliable
- Asset inventories compromised

System Availability

- Critical systems offline > 1 hour
- Backend transaction processing delayed >8 hours

Fraud

- Credit card processing compromised
- Purchase order fraud

3 Cyber Scenarios

Privileged Insiders leverage legitimately granted credentials to steal data from Critical Applications

Cyber criminals compromise customer portal to access PII

Manual processes lead to data being sent to the wrong customers

6 Examples

- Customer Facing Application
- Transaction processing middleware
- Customer database
- Inventory and Warehouse management systems

4 Demographics

- Network location
- Data types
- Customer logins
- RTO
- Regulatory (e.g. SoX)
- Money movement

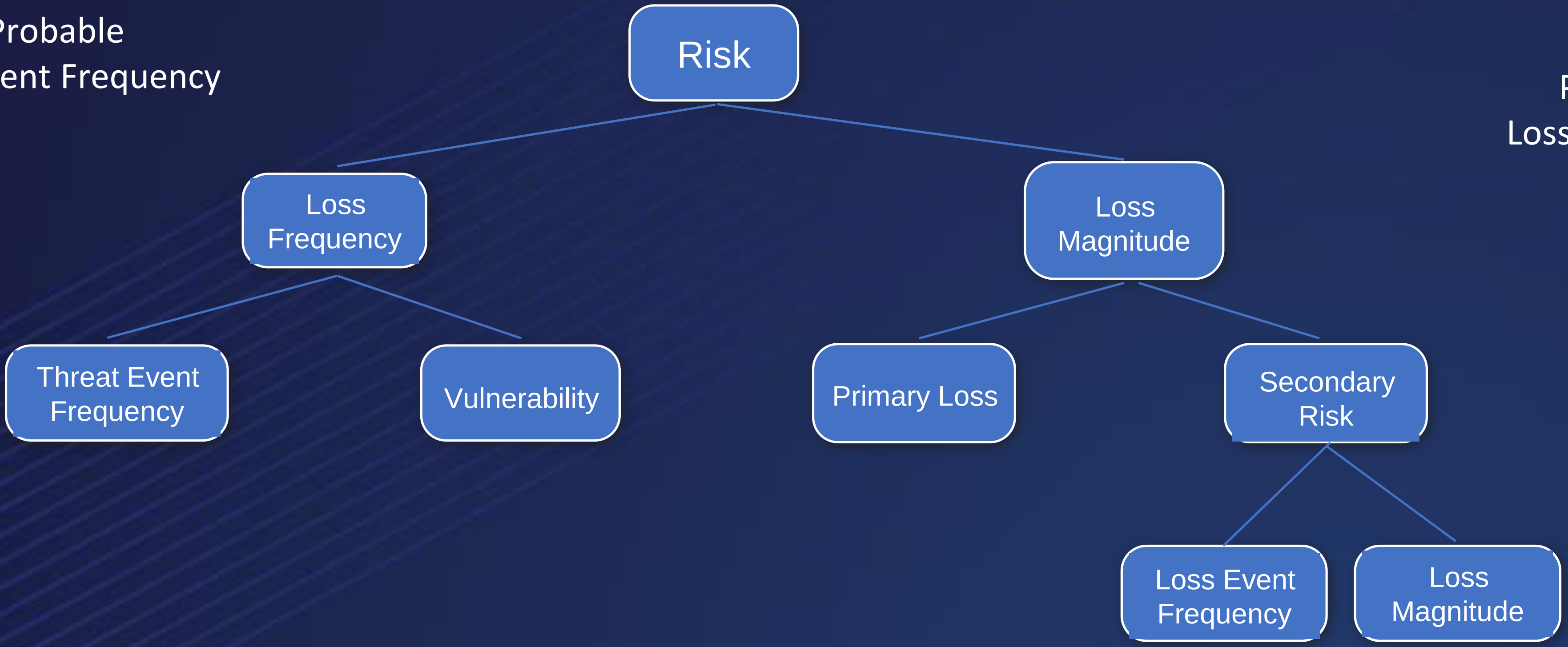
5 IT Assets

- Applications
- Servers
- Databases
- Network segments
- Workstations
- IT Services
- Data transfers
- Suppliers
- Projects
- IOT
- Containers
- Cloud
- Subsidiaries
- Facilities

FAIR (Factor Analysis for Information Risk)

Probable
Loss Event Frequency

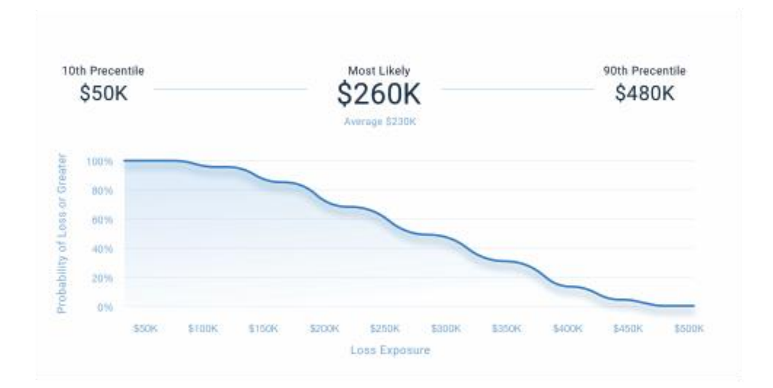
Probable
Loss Magnitude



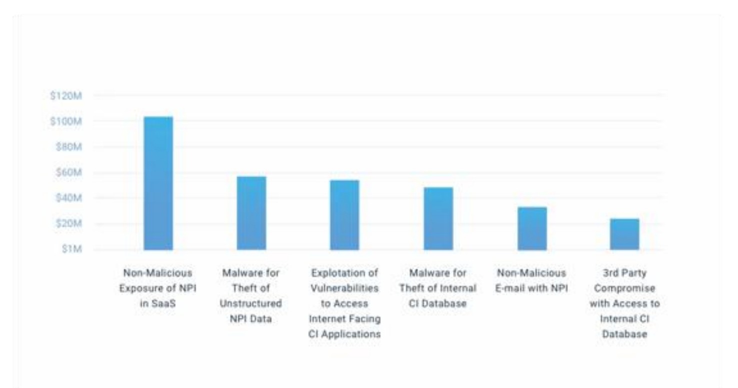
How often bad things happen, and how bad they're likely to be.

Examples of Quantitative Risk Communication

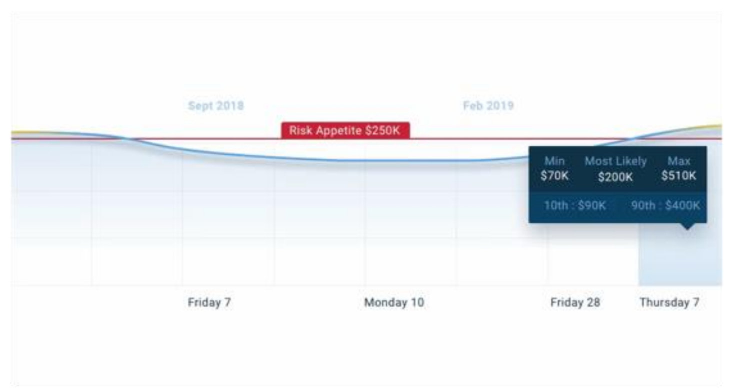
“HOW MUCH RISK DO WE HAVE?”



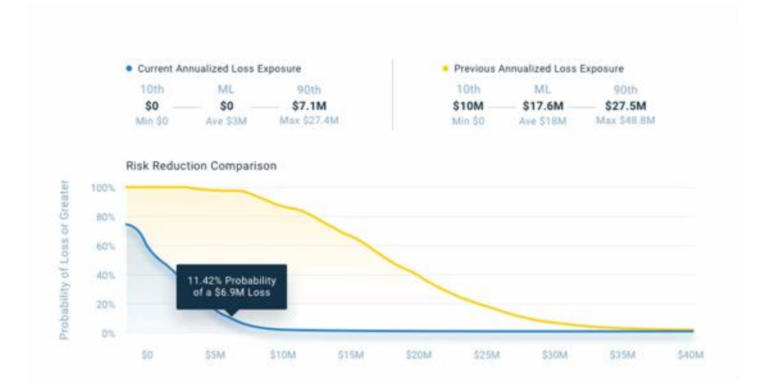
“WHAT ARE OUR TOP RISKS?”



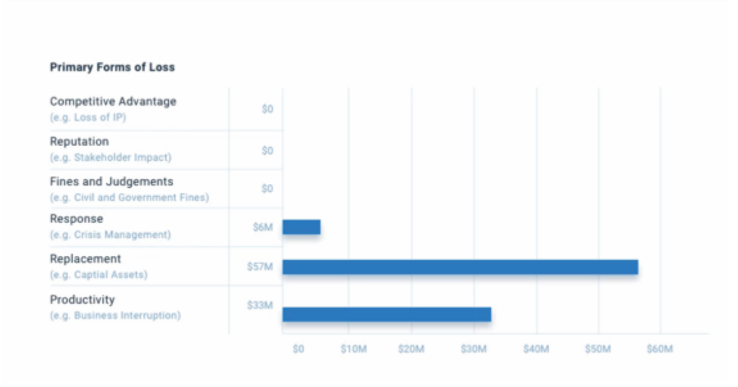
“HOW IS OUR RISK TRENDING VS. APPETITE?”



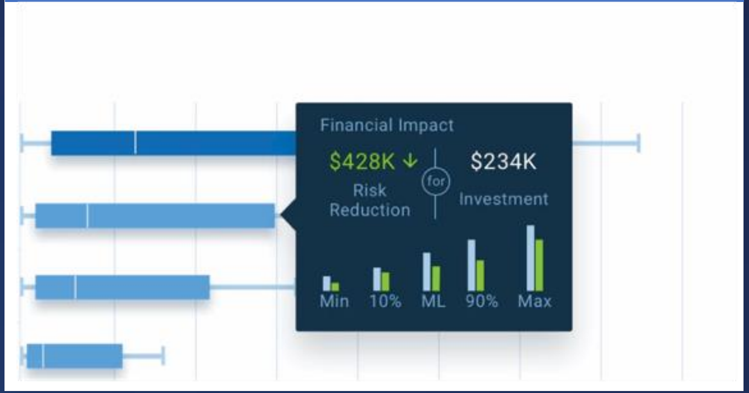
“HAVE WE REDUCED RISK?”



“WHAT TYPE OF LOSS CAN WE EXPECT?”

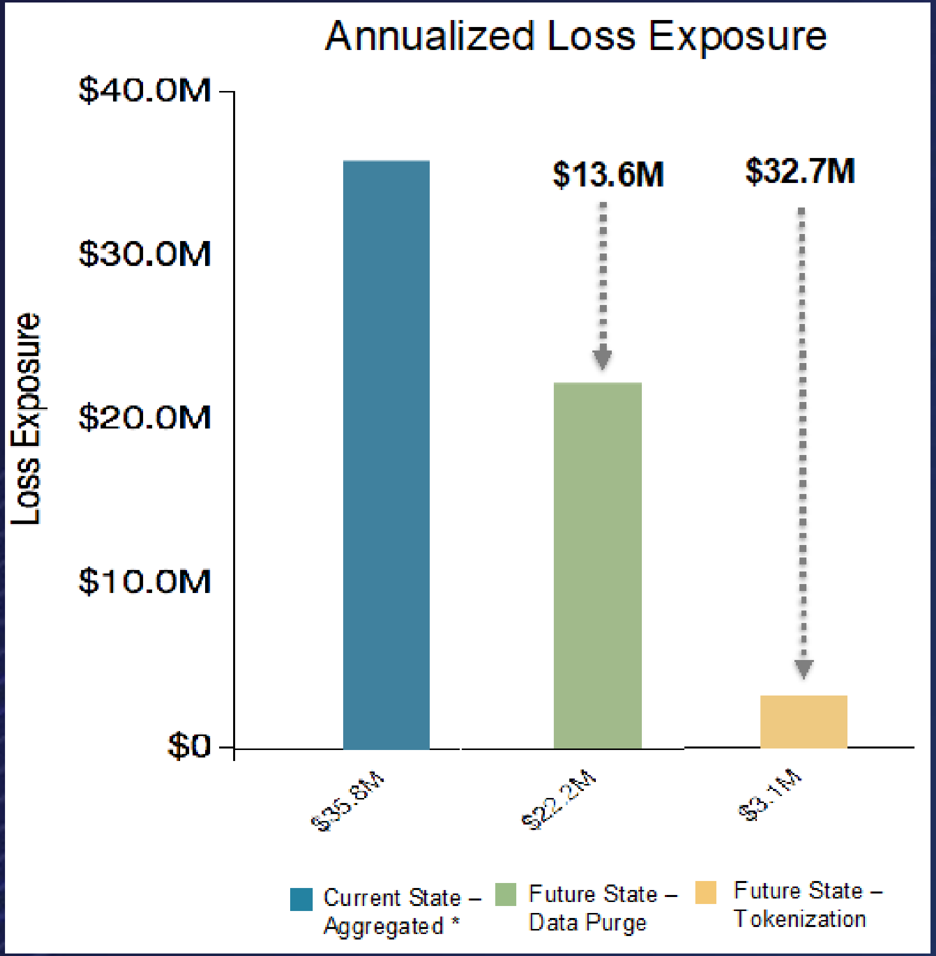


“WHAT IS THE COST/BENEFIT OF THIS PROJECT?”



(Source: RiskLens)

Security Project Analysis



Data Purge

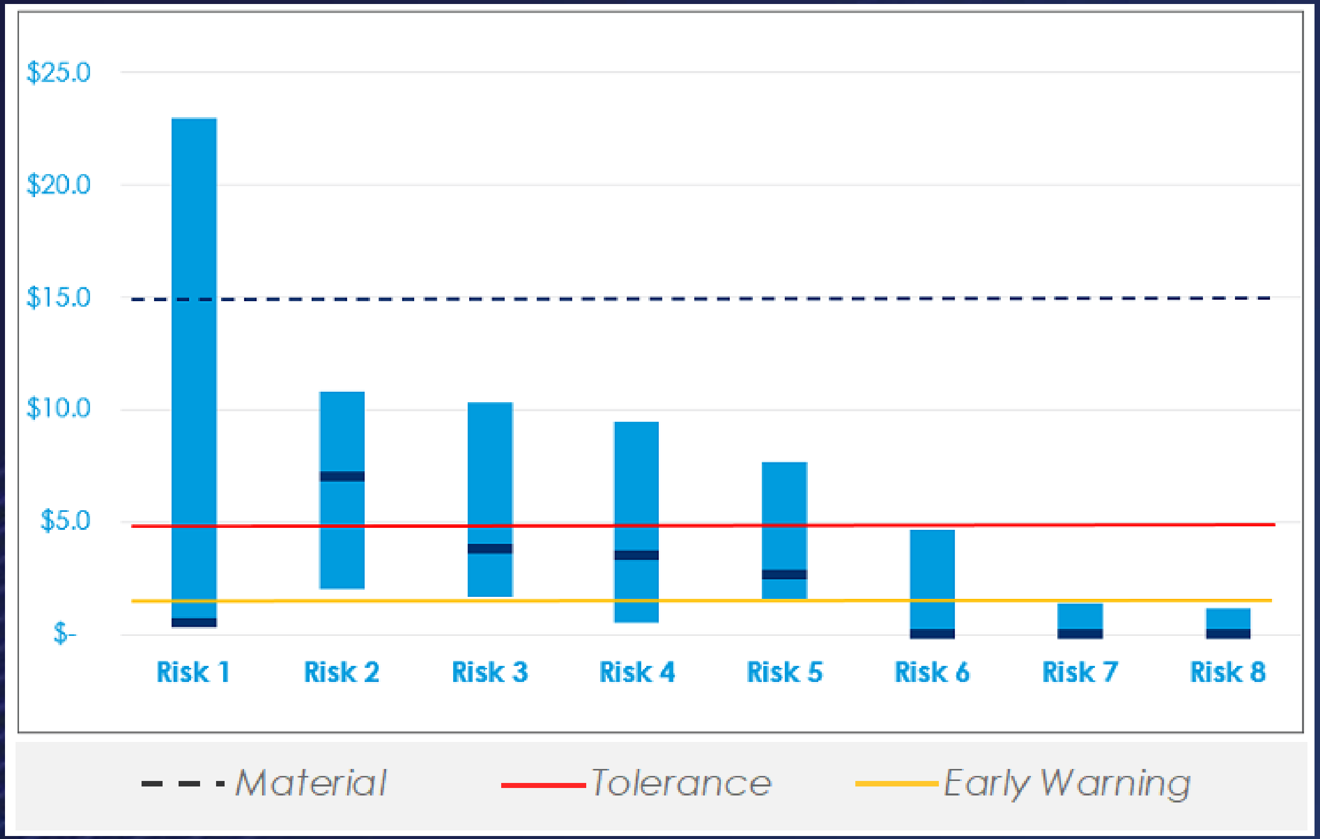
- Reduction of potential PII records stolen
- Maximum of 1.8M (1.2M reduction) for file shares
- Maximum of 6M (4M reduction) for database cluster

Tokenization

- Reduction in likelihood of secondary fallout
- Reduction in secondary loss event frequency as the remaining data would be “phone book” data

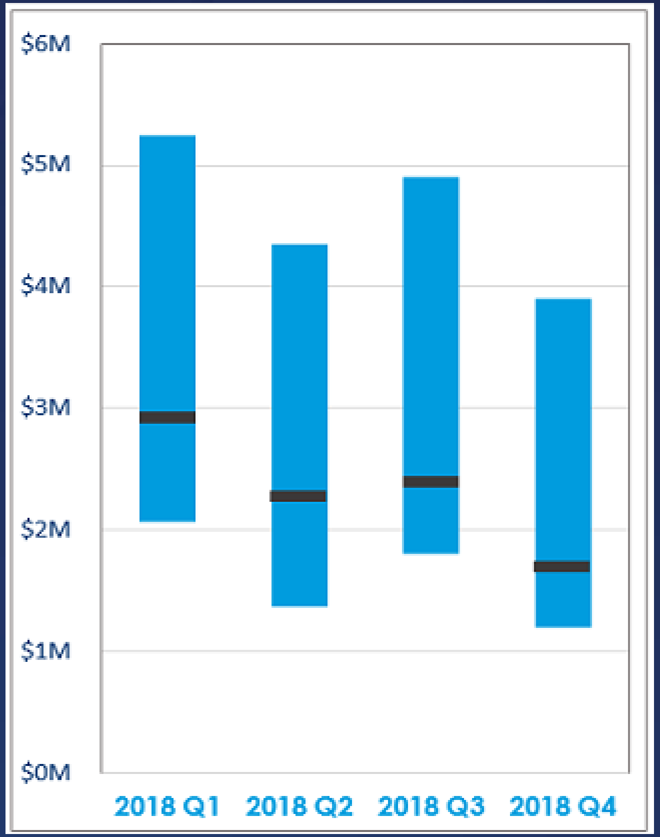
Top Risk Report, Risk Appetite, and Risk Trending

Organizational Top Risk v. Risk Appetite



*Dark bar in center of box represents most likely loss. Threshold breach determined by most likely value.

Overall Loss Exposure Trend



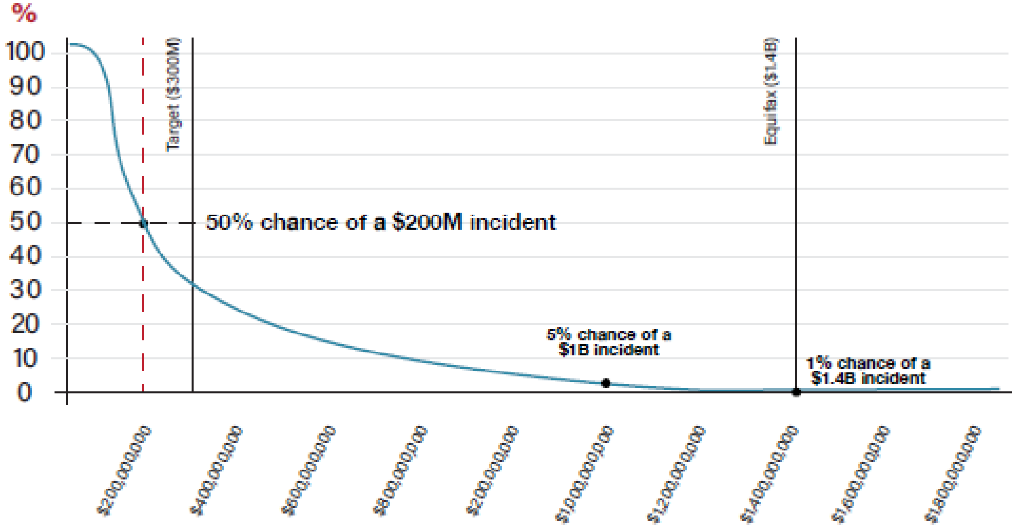
*Aggregated scenarios above early warning threshold

White Labeled Sample Board Report

Overall Risk

Cyber Value at Risk (VAR)

50% chance of exceeding risk appetite ($200M) in the next 3 years



- Aggregate cyber losses to the firm are represented to the left in the loss exceedance chart. This shows a 50% chance of having a $200M incident (and exceeding appetite), a 5% chance of having a $1B incident, and a 1% chance of a $1.4B incident.
- A cyber insurance purchase has been postponed and could safeguard against some of the impact of a cyber incident of this magnitude.
- These aggregate values are comprised of the top 4 risk scenarios outlined below of which, three are in yellow status and one is in green. Action plans have maintained or reduced loss exposure in the three yellow risks.
- The last business continuity test reflected the improvements in system recovery capabilities, thus the likelihood of a system outage over 8 hrs has decreased into yellow status.
- Data breach probability continues to be in Yellow status and this is attributed to a rise in both the number and sophistication of phishing attacks, resulting in more compromises despite improvements in anti-phishing training. Other forms of attacks appear to be declining. A proposed solution to mitigate this exposure is covered in the Pending Decision section of this report (page 5).
- Regulatory non-compliance remains low since closing existing MRAs. This should drop lower after our next review meeting with the regulator.
- Financial misstatement risk remains low due to strong change control processes.

Top Risk Scenarios with KRIs

TOP RISKS

		PROBABILITIY OF OCCURING IN THE NEXT 12 MONTHS				
RISK	R/Y/G THRESHOLDS	4Q 2018	1Q 2019	2Q 2019	3Q 2019	TREND
SYSTEM OUTAGE >8HOURS AFFECTING CRITICAL SYSTEMS	2% < 3% < 5%	7%	7%	5%	3%	⬇
DATA BREACH AFFECTING > 1M PII RECORDS	5% < 7% < 10%	10%	8%	8%	8%	➡
REGULATORY NON-COMPLIANCE RESULTING IN AN MRIA	2% < 3% < 5%	5%	5%	3%	3%	➡
IT-RELATED FINANCIAL MISSTATEMENTS (>$1M)	2% < 3% < 5%	2.5%	2.5%	2.5%	2.5%	➡

Incidents & Near Misses

REALIZED RISK EVENTS

	4Q 2018		1Q 2019		2Q 2019		3Q 2019		
INCIDENT TYPE	#	$	#	$	#	$	#	$	TREND
REGULAR < $100K	1	$50,000	2	$65,000	1	$53,000	1	$45,000	➡
REGULAR > $100K	0	-	0	-	1	$127,000	0	-	⬇
NEAR MISS > $100K	1	$400,000	1	$150,000	0	-	1	$240,000	⬆

Actual incidents under $100K are flat this quarter, and there were no incidents over $100K, thanks to early action by the incident response team. There was one near miss of about $240K related to customer statements that was averted due to a manual process that samples statements for accuracy before sending the batch to the printers.

MAJOR INITIATIVES STATUS

MAJOR INITIATIVES	PHASE	STATUS	PROJECTED COMPLETION	NOTES
INDENTITY AND ACCESS AND MANAGEMENT CENTRALIZATION	4 of 4	🟩	1 - NOV 19	
SECURITY INFORMATION AND EVENT MANAGEMENT	3 of 4	🟩	1 - DEC 19	
NETWORK SEGMENTATION	2 of 6	🟨	1 - JUN 20	RESOURCE CONSTRAINTS WITH DATACENTER COORDINATION
RETAIL CLOUD MIGRATION	1 of 3	🟩	1 - MAR 20	
DATACENTER COORDINATION	1 of 9	🟨	1 - JAN 21	NEED TO ACCELERATE TO MEET BUSINESS DEMANDS

Investment Updates (Control Improvements)

Risk Reduction Proposal: Reducing probability of a data breach of > 1M records

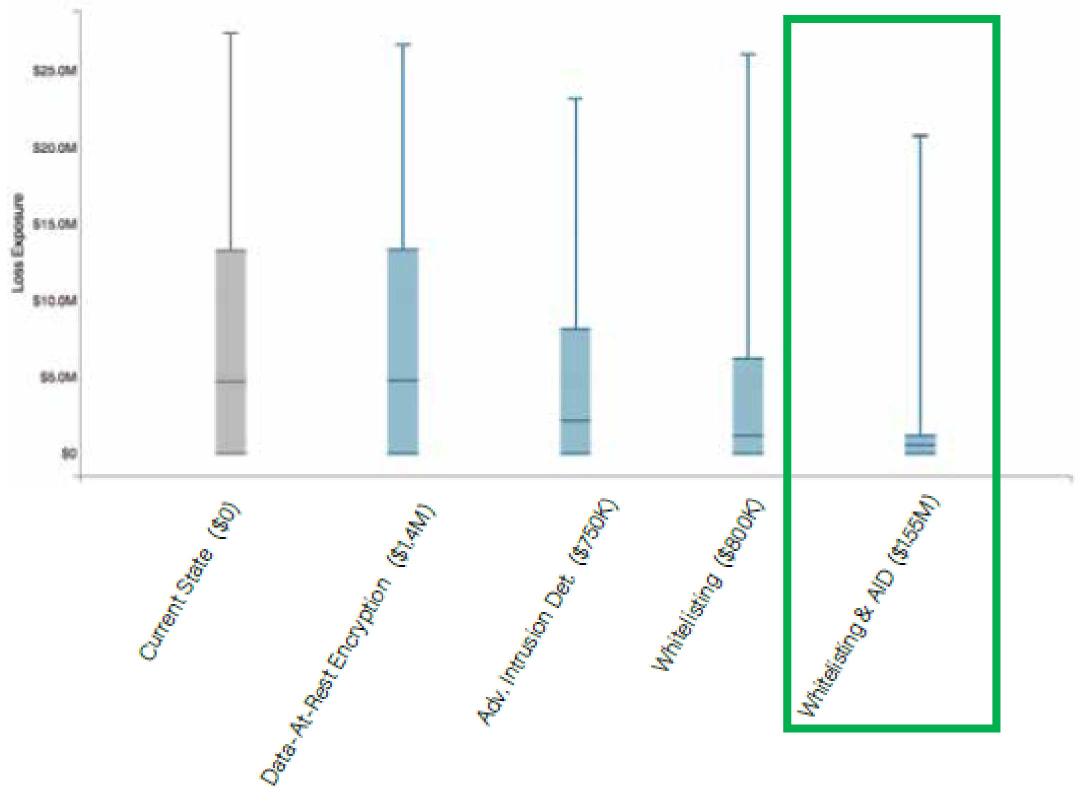
- Option 1 - Do nothing
- Option 2 - Encrypting data at rest
- Option 3 - Advanced intrusion detection (AID)
- Option 4 - Whitelisting
- Option 5 - Both AID and Whitelisting

Conclusions:

- Encrypting data at rest is often considered a "best practice" within the industry, although for mitigating Phishing-related risk it is not cost-effective.

- Advanced Intrusion Detection and Whitelisting are anticipated to have roughly equivalent hard-dollar costs, however the complexity to implement Whitelisting is expected to be significantly higher.

- <u>Recommendation: Leveraging both AID and Whitelisting</u>
  A project to implement AID could be started in 2nd quarter of next year. Due to resource constraints, we recommend postponing a Whitelisting project until 4th quarter of next year or 1st quarter of the year after.



Risk Reduction Proposal (tied to #2 Top Risk)

Strategies For Adopting Cyber Risk Quantification

Jack Jones

Chairman

FAIR Institute

Where do we begin?

Start with “**Why**”?

What pain point are we trying to resolve?

Choose a starting point…

RISK LANDSCAPE CLARITY

Top Risks Identification

Audit Findings Prioritization

Policy Exception Request Reviews

Emerging Threat Analysis

Source: RiskLens FAIR Enterprise Model^{TM}

What Capabilities are Required?

Models

Skills

Data

Tools?

An Example Starting Point

		Risk Landscape Clarity	Operational Decision Support	Strategic Decision Support	Automated decision support
Skills	Dedicated				
	Not dedicated	✓			
Data	Telemetry				
	Reusable libraries				
	Calibrated SME estimates	✓			
Tools	Commercial CRQ apps				
	Home-grown CRQ apps				
	Spreadsheets				

Evolving to…

		Risk Landscape Clarity	Operational Decision Support	Strategic Decision Support	Automated decision support
Skills	Dedicated		✓		
	Not dedicated				
Data	Telemetry				
	Reusable libraries				
	Calibrated SME estimates		✓		
Tools	Commercial CRQ apps		✓		
	Home-grown CRQ apps				
	Spreadsheets				

Two prerequisites…

A clearly defined initial objective

Risk analysis training

Roadmap Considerations

👍 Executive Support

$ Budget

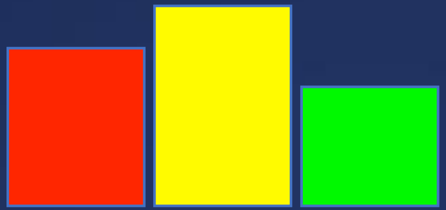
✋ Potential Obstacles

🧠 Critical Thinking Skills

How hard will it be?

Beliefs — The Biggest Hurdle?

“Too difficult”



"Good enough"

Demonstrate meaningful value at an acceptable cost

Beware of unrealistic expectations!

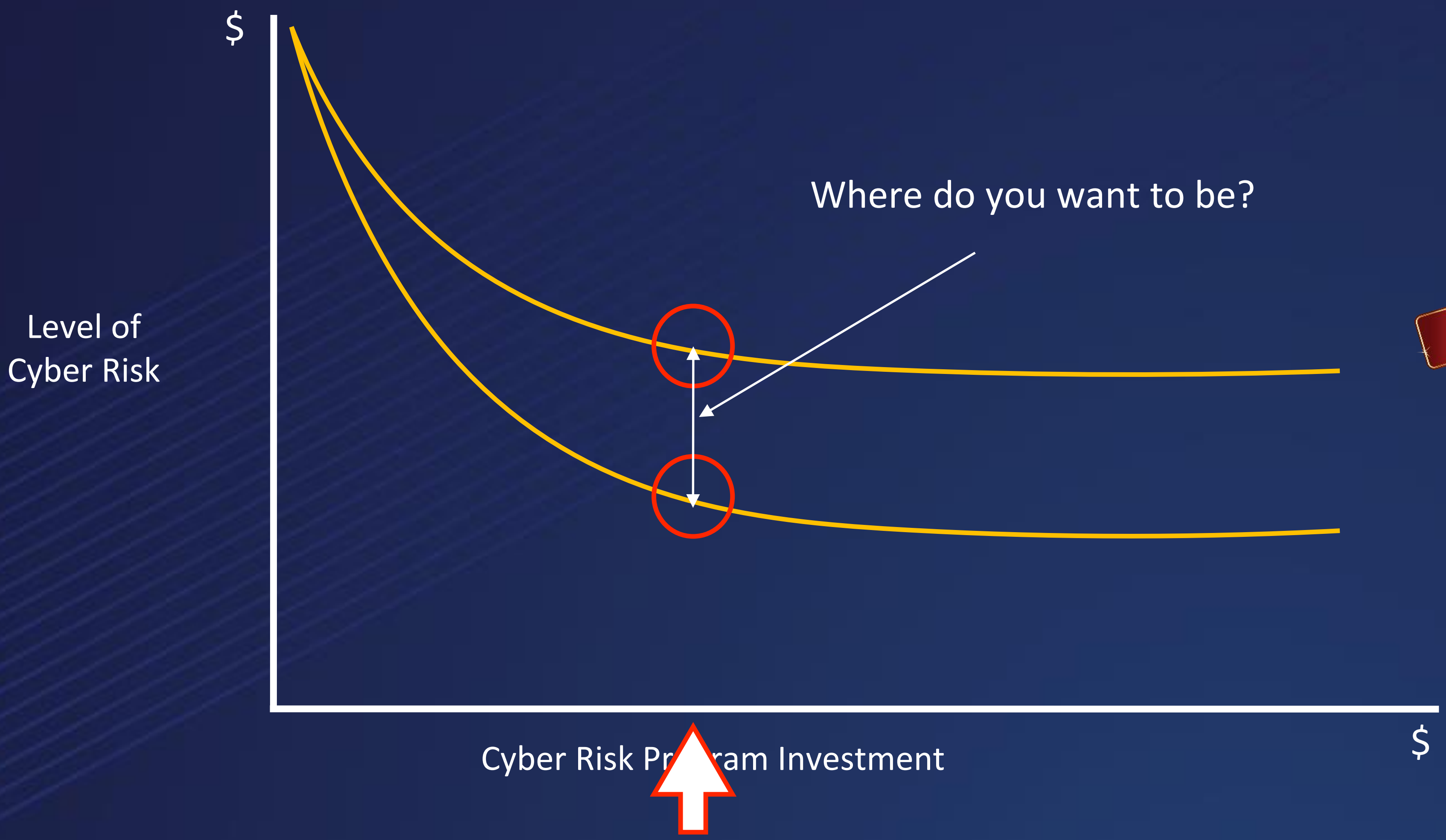
FOCUS on
☑ PROGRESS
□ PERFECTION

The first steps are the hardest

Start doing analyses

Avoid analysis paralysis

Why it matters…



Join the FAIR Institute

Members of the FAIR Institute take advantage of many benefits. The greatest benefit is access to the exclusive community of information risk officers, cyber security leaders and business executives who share their experience and knowledge on the growing discipline of information risk management.

Members also receive:

- Full access to our ever-growing Resource Library and content generated by the Institute,
- Discounts on events and the annual FAIR Conference,
- Weekly blog updates,
- Much more!

FAIR Institute Breakfast

When: February 26, 2020,

7:30 - 10:30 AM PST

Where: Parc 55 San Francisco,

Embarcadero Room (Level Three)

55 Cyril Magnin Street,

San Francisco, CA 94102

Building an Effective Cyber Risk Management Program that Actually Works

FAIR Institute Breakfast Meeting during RSAC2020

2020 FAIR Conference (FAIRCON2020)

October 6 & 7, 2020
Marriott Wardman Park
Washington, DC

FAIRCON20 brings leaders in information and operational risk management together to explore best FAIR practices that produce greater value and enable business-aligned communication.

Factor Analysis of Information Risk (FAIR) has emerged as the standard Value at Risk (VaR) framework for understanding, measuring and analyzing information risk, and ultimately, for enabling well-informed decision making.

The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk with FAIR.

- Explore best risk management practices that align with business goals
- Discover new FAIR-based products and services to help your program
- Expand your industry wide network

Reserve your Seat Today: http://www.fairinstitute.org/faircon20

FAIR INSTITUTE

FAIR Training Courses Discount

RSAC20FAIRTR

- **35% off** FAIR Analysis Fundamentals and/or FAIR Analyst Learning Path
- No minimum purchase requirement, available to everyone with the code.
- Limited to one discounted transaction per customer.
- Active through March 31.