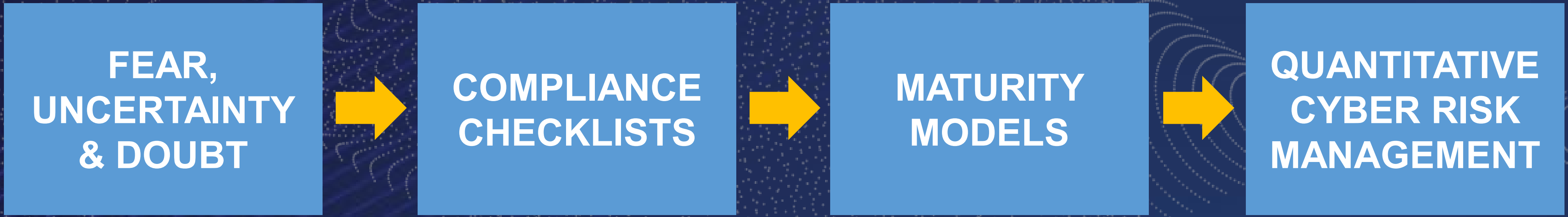
3 Step Guide on How CRQ Can Solve Your Business Problems *a FAIR Approach*

Presented by: Rebecca Merritt, Sr. Manager - RiskLens

AGENDA

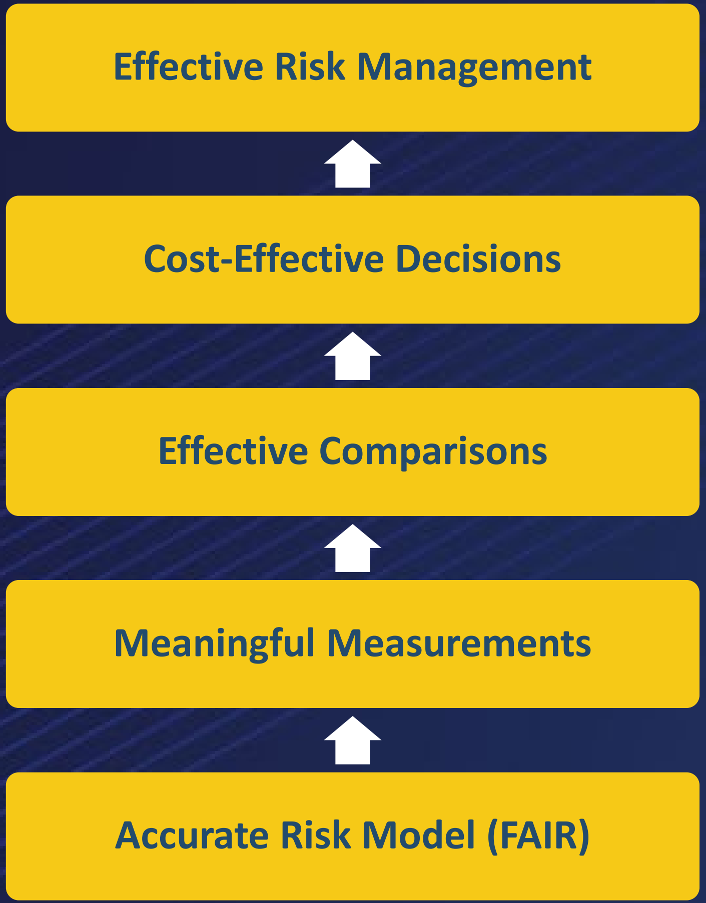
- Why FAIR?
- FAIR Model
- 3 Step Guide – Use Case
- Communicating Results
- Taking Action / Recommendations

Expectations for CISOs Have Changed



FEAR, UNCERTAINTY & DOUBT → COMPLIANCE CHECKLISTS → MATURITY MODELS → QUANTITATIVE CYBER RISK MANAGEMENT

Effective Risk Management



Effective Risk Management

Cost-Effective Decisions

Effective Comparisons

Meaningful Measurements

Accurate Risk Model (FAIR)

The combination of personnel, policies, processes and technologies that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure.

Source: “Measuring and Managing Information Risk: A FAIR Approach”

Quantitative Approach to Risk Management

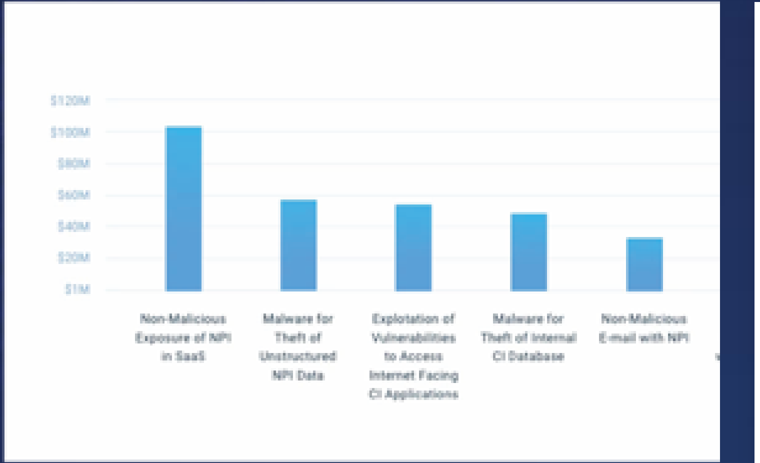
Current approach to risk mgt…

Medium Likelihood	High
Scenario 1	Severe Impact

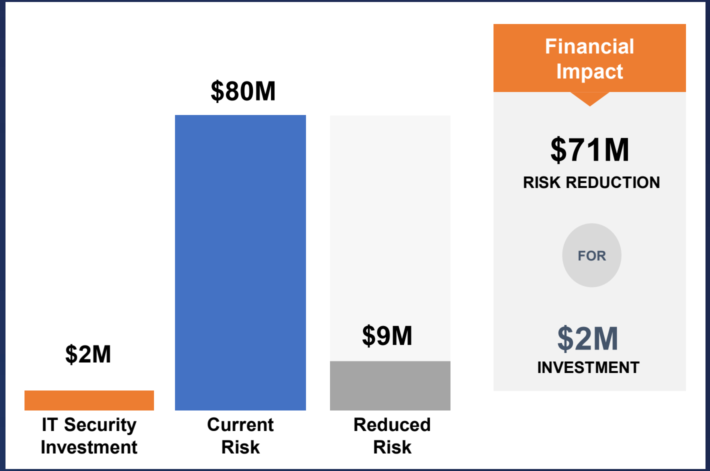
Medium Likelihood	High
Scenario 2	Severe Impact

*"We need to prioritize **multiple scenarios** for remediation because we're currently at high risk of experiencing a data breach. They are both rated **red** since the likelihood is medium and the impact is severe."*

Goal for effective risk management…



Top Risks



Cost Benefit

FAIR enables cost-benefit analysis and effective prioritization of risks in financial terms

The FAIR Model

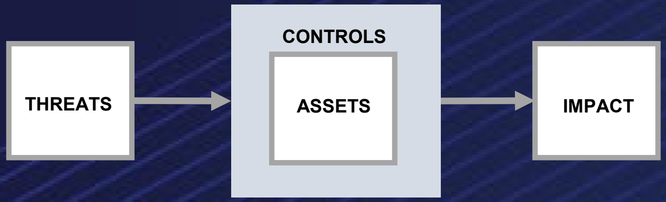
Factor Analysis of Information Risk

A model and method for defensible quantitative analysis of risk that produces results in financial and probabilistic terms, enabling cost-effective management of risk across the organization/enterprise.

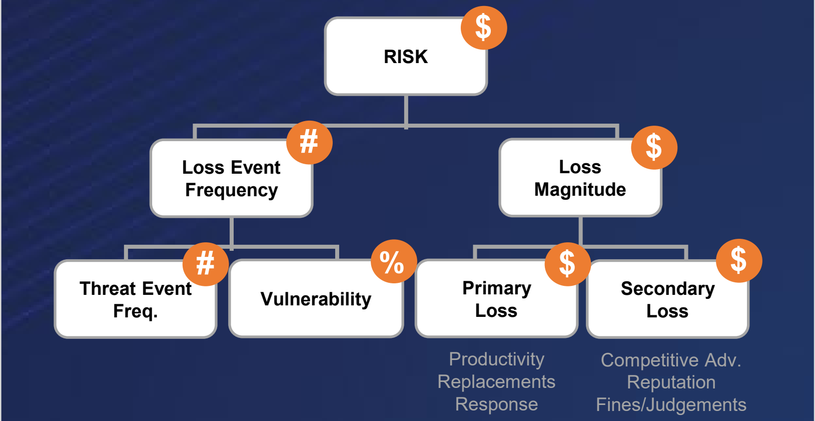
A FAIR View of Risk

FAIR provides the analytic model that enables risk to be quantitatively:

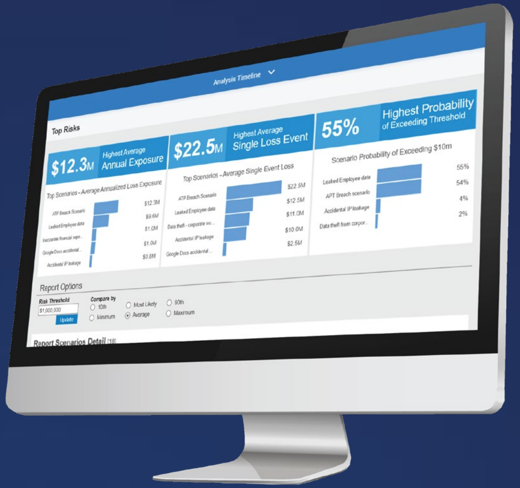
DEFINED



MEASURED



PRIORITIZED


Analysis Timeline
Top Risks
$12.3M Highest Average Annual Exposure
$22.5M Highest Average Single Loss Event
55% Highest Probability of Exceeding Threshold
Top Scenarios - Average Annualized Loss Exposure
ATP Breach Scenario
Leaked Employee data
Inaccurate financial repo...
Google Docs accidental...
Accidental IP leakage
$12.3M
$9.6M
$1.0M
$1.0M
$0.8M
Top Scenarios - Average Single Event Loss
ATP Breach Scenario
Leaked Employee data
Data theft - corporate wo...
Accidental IP leakage
Google Docs accidental ...
$22.5M
$12.5M
$11.0M
$10.0M
$2.5M
Scenario Probability of Exceeding $10m
Leaked Employee data
APT Breach scenario
Accidental IP leakage
Data theft from corpor...
55%
54%
4%
2%

Report Options

Risk Threshold: $1,000,000

Update

Compare by: ○ 10th ○ Minimum ○ Most Likely ● Average ○ 90th ○ Maximum

Report Scenarios Detail [18]

FAIR lays the groundwork for risk to be effectively MANAGED

FAIR INSTITUTE

Would it with be worth our investment to upgrade our electronic health record (EHR) system? We are constantly having issues with our legacy system, and I know our customers and employees are not happy with it. There’s so much that the system currently touches I don’t even know where we’d start!?”

- CTO

To Upgrade or Not to Upgrade – **That is the Question**

Current Problem

1 Frequent Outages

- Short outages every month – less than 1 hour – still inconvenient to employees and patients
- Wasted resources to manage

2 Lack of Security Control

- Unable to implement advanced security settings – legacy system does not have the ability to monitor data leaving system
- Excessive user access

3 Overall Issues

- Does not empower patients to manage healthcare journey
- Manual backup process – lack of redundancies

Upgraded EHR

4 Better Uptime

- Upgraded system is expected to have less downtime
- Failover systems in place to reduce outage timeframe if occurred

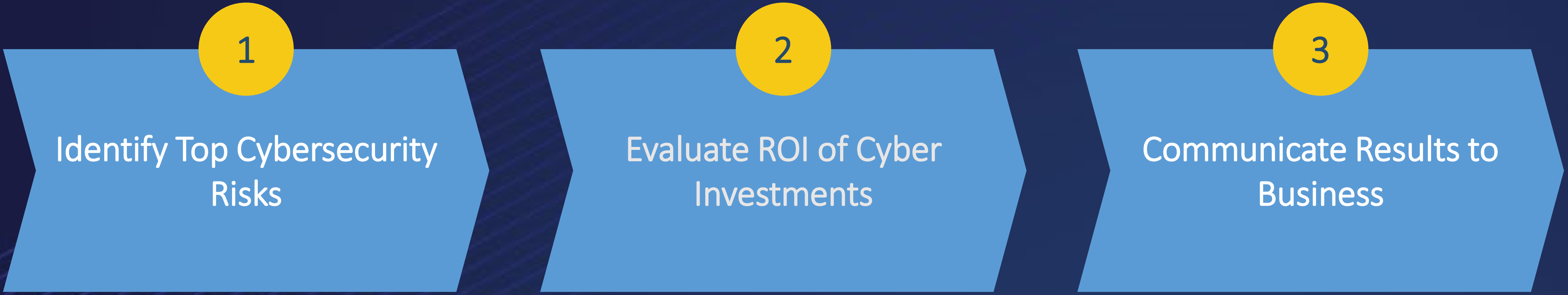
5 Strong Security Capabilities

- Ability to prevent insider data disclosure
- Advanced access controls – capabilities - MFA

6 Cons

- Large Investment – Total +$50M
- Unsure where to start – large rollout with conflicting prioritizes

3-Step Guide to Assessing EHR System Investment



1

Identify Top Cybersecurity Risks

2

Evaluate ROI of Cyber Investments

3

Communicate Results to Business

Rapid Risk Assessment

Identify and prioritize risk scenarios that serve as the baseline for future investment decision

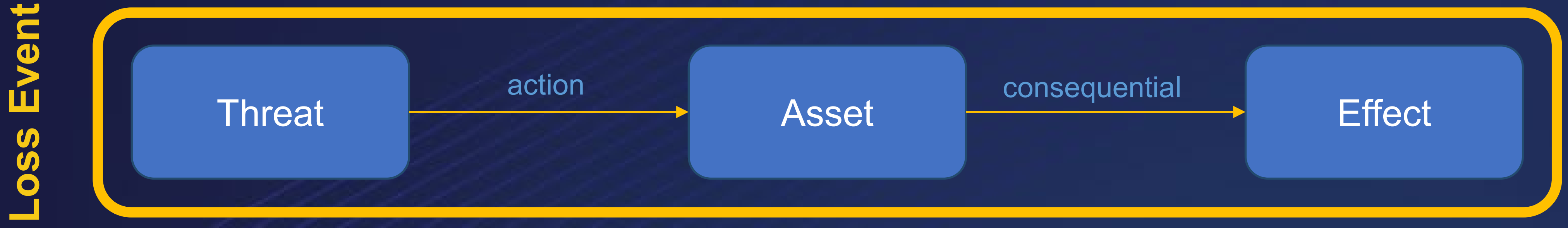
Cost Benefit Assessment

Evaluate ROI of security investments related to top cybersecurity initiatives to enable better prioritization

Executive Reporting

Customer-focused report to communicate results and drive cost effective decision making

Step 1: Scenario Scoping



Anything, actor or agent, capable of acting against an asset in a manner that can result in loss

Anything of value that can be affected in a manner that results in loss

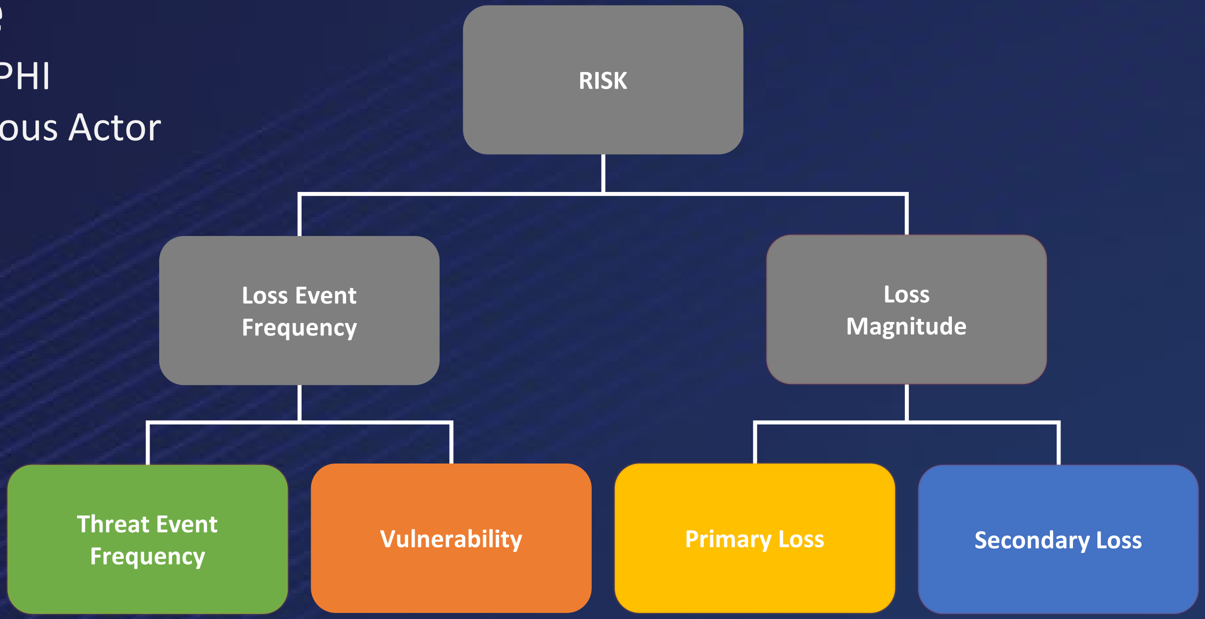
How loss materializes within a given asset

Risk = A measurement of the **probable frequency** and the **probable magnitude** of **future loss**.

Step 1: External Breach of Electronic Health Record System

Scenario Scope

Asset: EHR containing PHI
Threat: External Malicious Actor
Effect: Confidentiality
Method: Phishing



RISK

Loss Event Frequency

Loss Magnitude

Threat Event Frequency

Vulnerability

Primary Loss

Secondary Loss

Employee Turnover

- Cost to replace malicious employee

Customer reactions

- Service credits/customer settlements
- Customer churn

Fines and Judgments

- Regulatory fines/penalties

Incident Management

- Incident Management (Person Hours)
- External Notification/Response

Attempts to cause harm

- Historic events
- Informed estimations

Preventative Measures

- Endpoint Protection
- Network Segmentation
- Identity Access Management

Step 1 – Diving In: External Breach of Legacy EHR

Scenario Assumptions

Probability of external breach

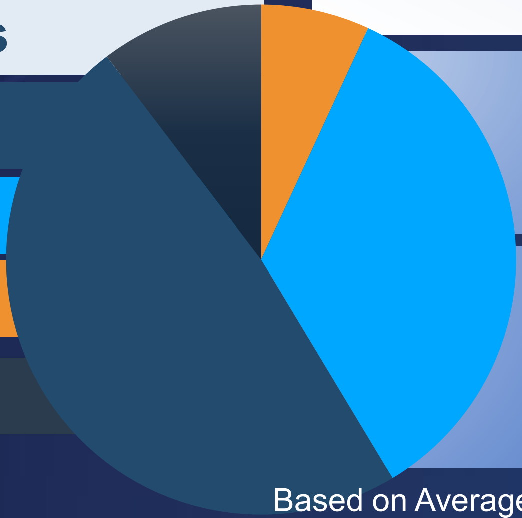
7 - 22%

resulting in compromise of

1M – 11M records

Concentration of Loss

- **Fines and judgments**
- **Responding** to stakeholders
- **Responding** to incident
- **Reputation** damage to patient



Based on Average

Key Takeaways

On average, expected loss **per event** of **$42M**

with an average **forecasted loss** every **7 years**

and an average **annualized** loss of **$7M**

$0 - $50M

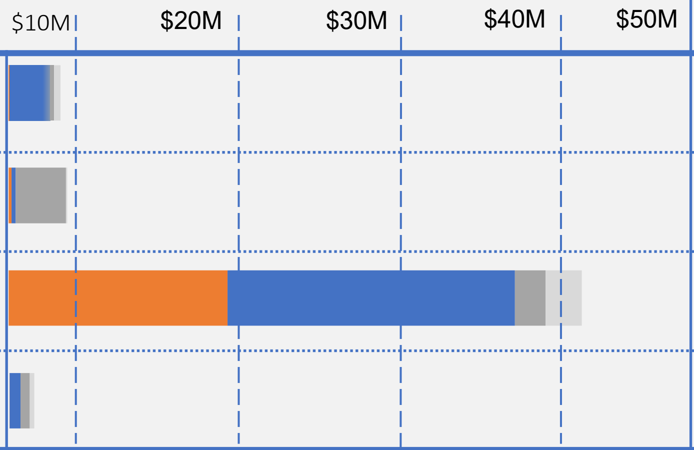
range of probable loss

15%

probability of exceeding $1M in a given year

Step 1: How Much Risk Do We Currently Have?

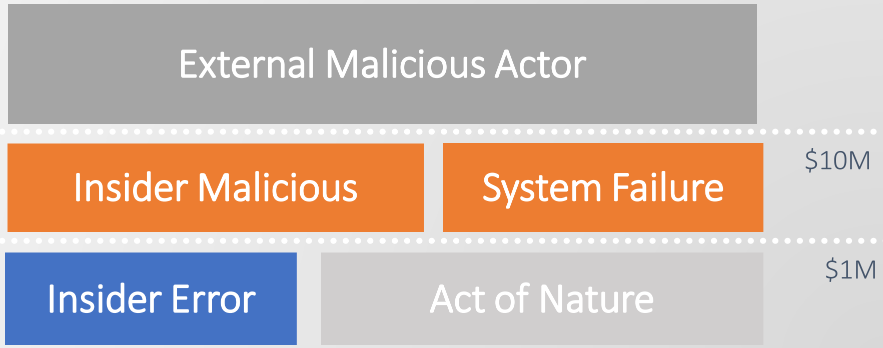
Includes **20 risk scenarios** identified for **4 risk categories**



Risk Categories Aggregated risk scenarios, 10th - 90th %	Annualized Loss	Roadmap Initiative
Insider Access Loss caused by priv. insiders (malicious or error)	$100K - $6M	• Multifactor Authentication • Priv. Access Management
Endpoint Security Loss from end user software or devices	$0 - $8M	• Endpoint Detection
Customer Data Compromise Loss due to customer data being compromised	$0 - $42M	• Network Access Controls • Data Loss Prevention
System Outage Outage of system due to legacy settings	$100K - $5M	• Failover system • Increased redundancy

Highest Risk Threats

Average Annualized Loss Exposure



External Malicious Actor

Insider Malicious

System Failure

$10M

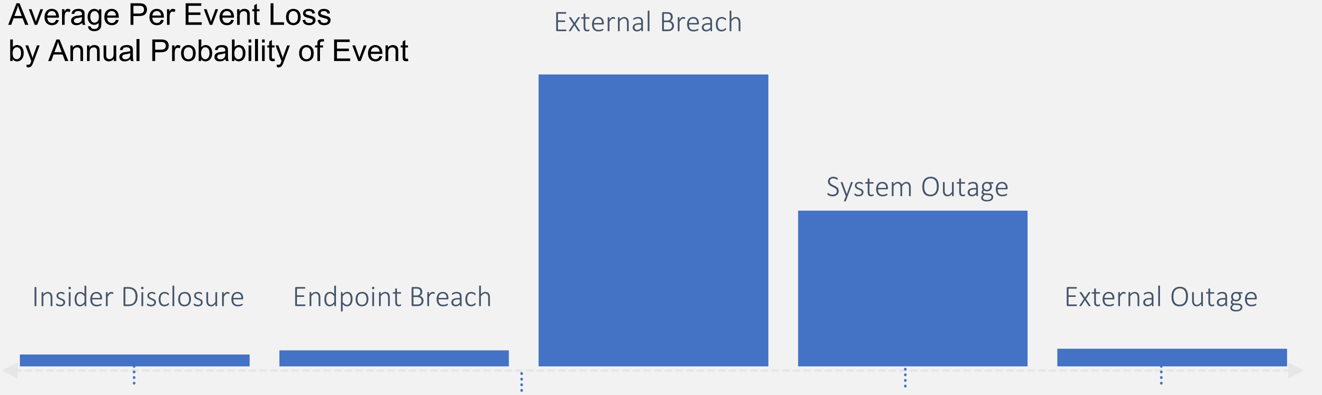
Insider Error

Act of Nature

$1M

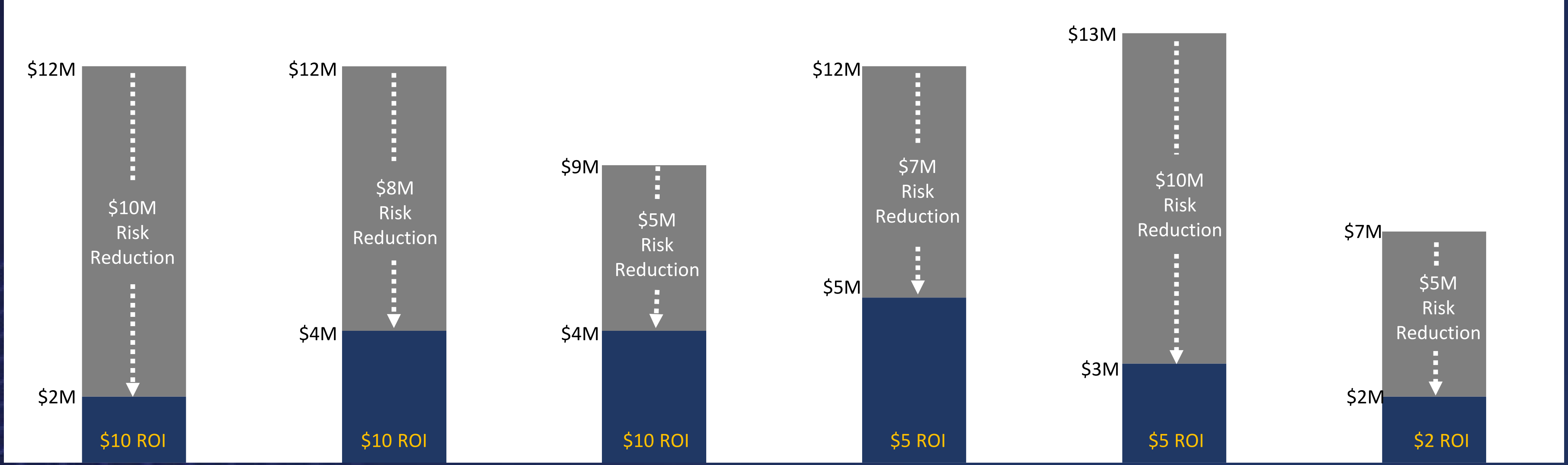
Top Risk Scenarios

Average Per Event Loss
by Annual Probability of Event



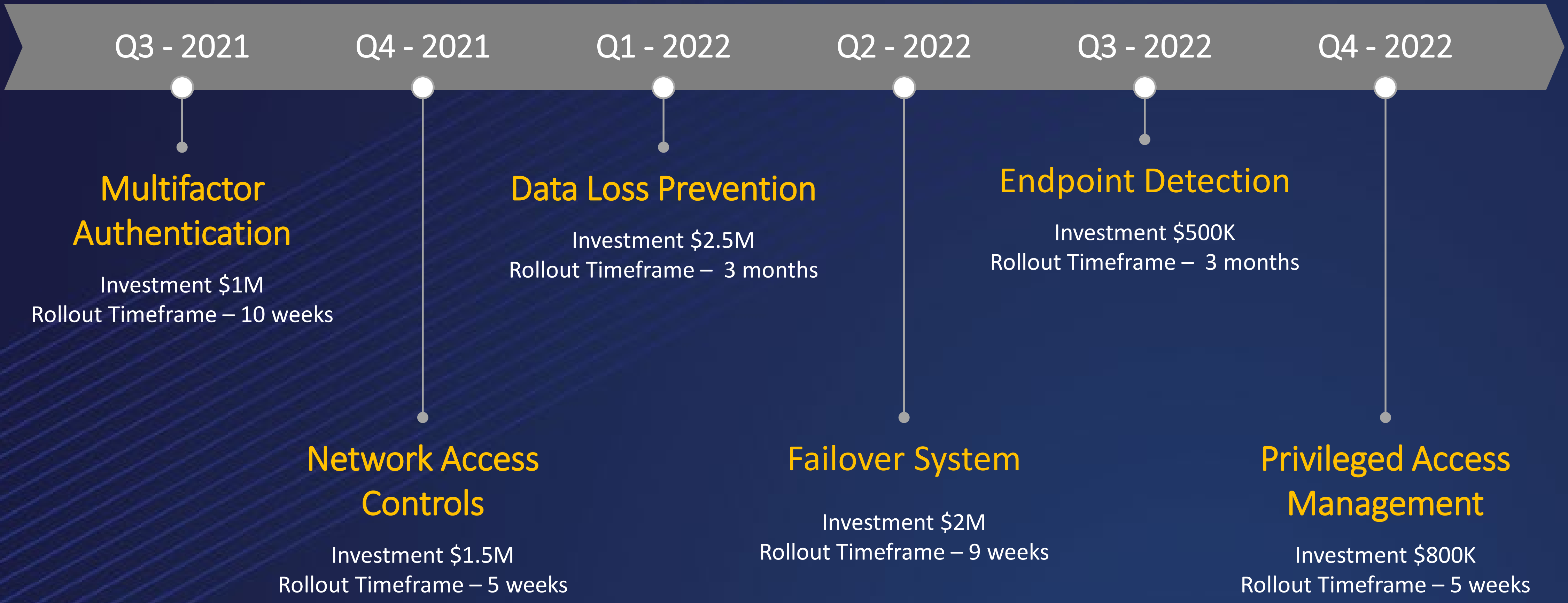
Step 2: What Control Gives the Biggest ROI?

An overview of initiatives that the organization could implement to reduce risk across the business.



	Multifactor Authentication	Privileged Access Management	Endpoint Detection	Network Access Controls	Failover System	Data Loss Prevention
Risk Reduction	-$10M	-$8M	-$5M	-$7M	-$10M	-$5M
Investment	$10M	$800K	$500K	$1.5M	$2M	$2.5M
ROI per $	$10	$10	$10	$5	$5	$2

Step 3: Proposed Rollout Plan



Q3 - 2021

Multifactor Authentication

Investment $1M
Rollout Timeframe – 10 weeks

Q4 - 2021

Network Access Controls

Investment $1.5M
Rollout Timeframe – 5 weeks

Q1 - 2022

Data Loss Prevention

Investment $2.5M
Rollout Timeframe – 3 months

Q2 - 2022

Failover System

Investment $2M
Rollout Timeframe – 9 weeks

Q3 - 2022

Endpoint Detection

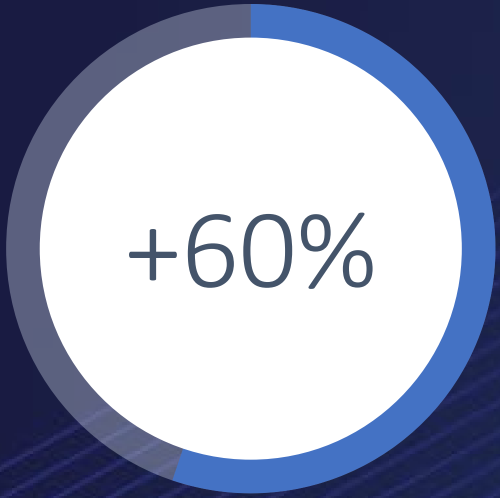
Investment $500K
Rollout Timeframe – 3 months

Q4 - 2022

Privileged Access Management

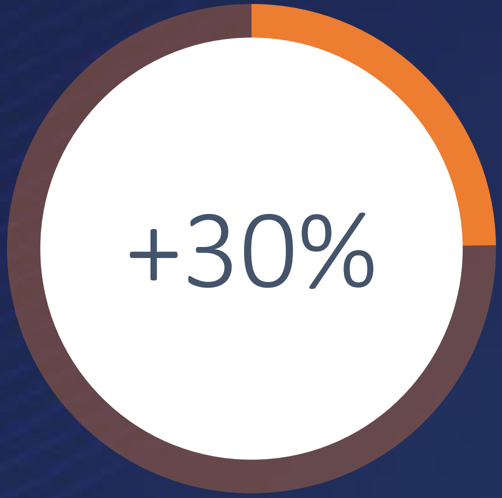
Investment $800K
Rollout Timeframe – 5 weeks

Step 3: Cost Savings Driven by FAIR



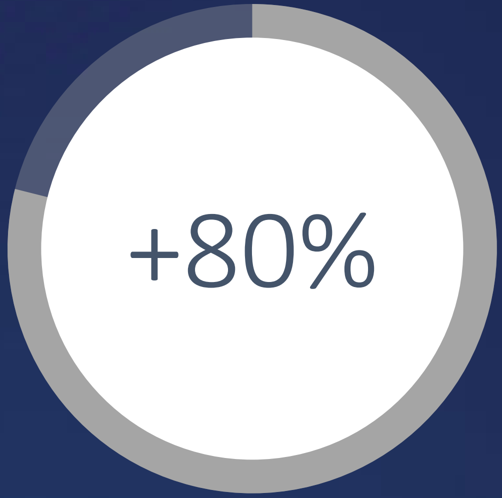
Improved Uptime

The upgraded system experiences infrequent outages. If an outage were to occur there is a failover system to ensure outage duration is under 15mins.



Threat Resistence

Advanced security controls allow for the organization to have improved insight into the IT environment. Controls allow for a reduction in external interface with system.



Customer Satisfaction

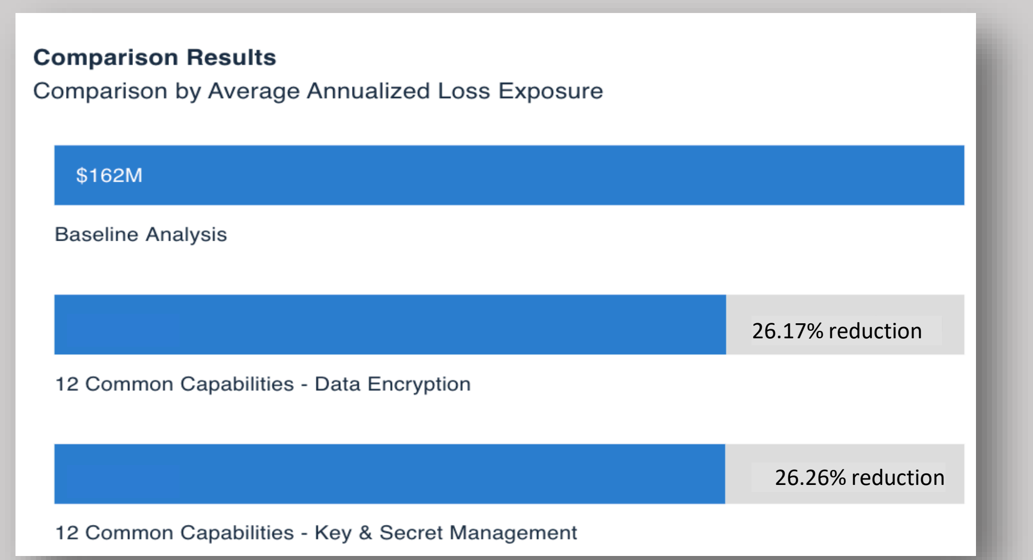
Customers can access their data through multiple channels – online, phone application, etc.

Additionally, upgraded system has improved user interface to better experience.

Colors or Numbers – What Do You Prefer?

The way most organizations define and measure cyber risk, fails to quantify the value of cybersecurity in terms the business can understand and use

FAIR-Based Reporting



Comparison Results

Comparison by Average Annualized Loss Exposure

$162M

Baseline Analysis

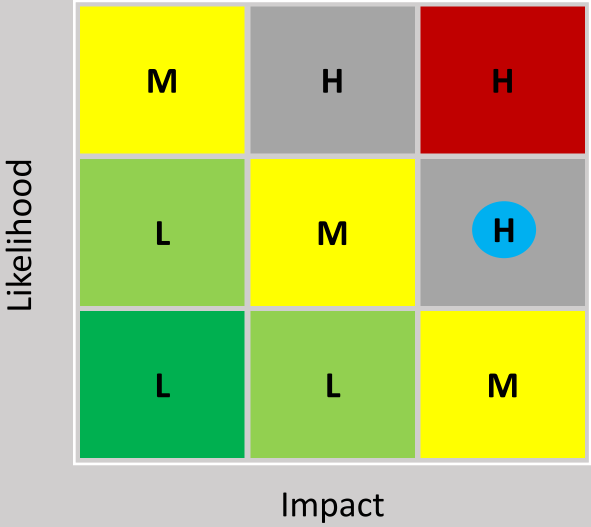
26.17% reduction

12 Common Capabilities - Data Encryption

26.26% reduction

12 Common Capabilities - Key & Secret Management

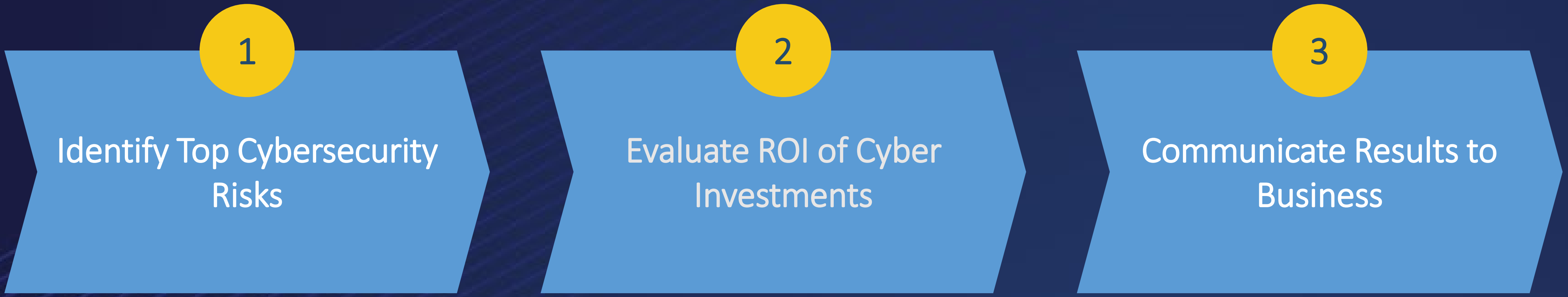
Qualitative Reporting



M	H	H
L	M	H
L	L	M

FAIR helps to ensure every dollar spent is worth the investment

3-Step Guide to Across Any Investment



1

Identify Top Cybersecurity Risks

2

Evaluate ROI of Cyber Investments

3

Communicate Results to Business

Rapid Risk Assessment

Identify and prioritize risk scenarios that serve as the baseline for future investment decision

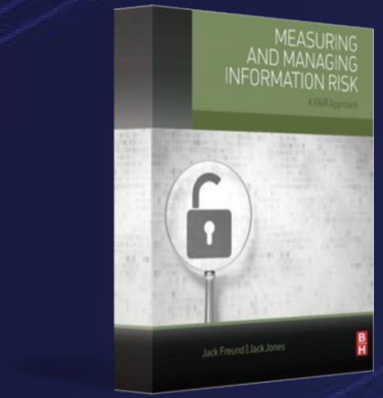
Cost Benefit Assessment

Evaluate ROI of security investments related to top cybersecurity initiatives to enable better prioritization

Executive Reporting

Customer-focused report to communicate results and drive cost effective decision making

FAIR Resources



FAIR BOOK

FAIR BLOG

RESOURCE LIBRARY

FAIR TRAINING & CERTIFICATION

FAIR-U TOOL

FAIR UNIVERSITY CURRICULUM

For more information, become a member at www.FAIRInstitute.org

Step 1: Six Forms of Loss

Productivity

Reduction in an organization's ability to generate its primary value proposition (producing goods or services, etc.)

Response

Expenses associated with managing or responding to a loss event

Replacement

Capital expense associated with replacing or repairing lost or damaged assets

Competitive Advantage

Losses associated with competitors obtaining and using trade secrets

Fines and Judgments

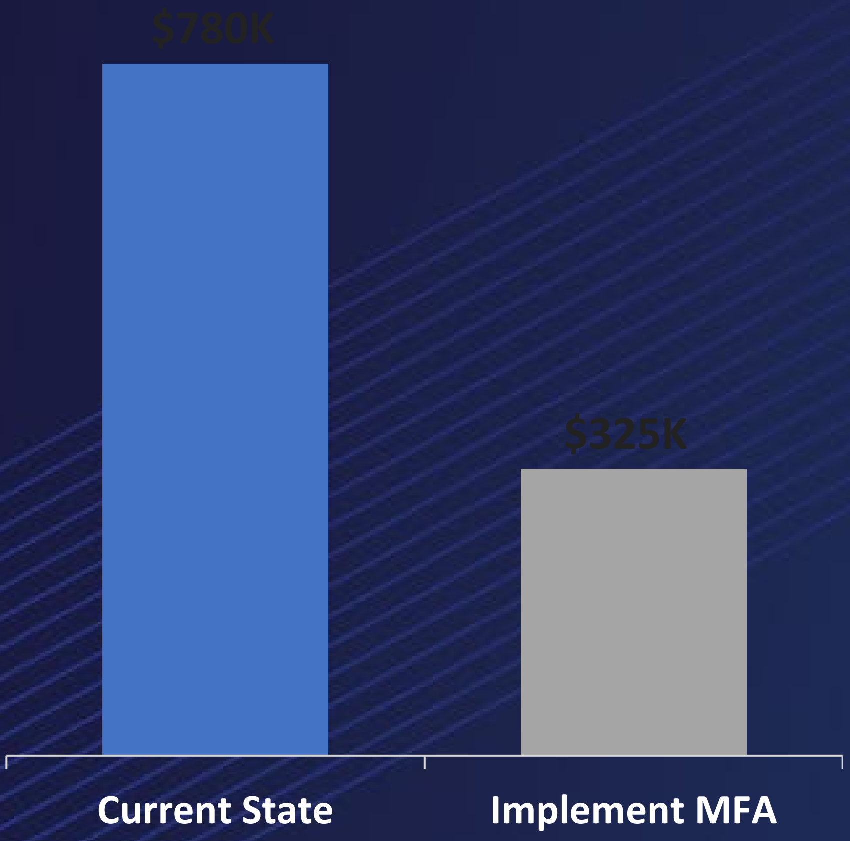
Losses from legal or regulatory actions levied against an organization through civil, criminal, or contractual actions.

Reputation

Losses associated with an external perception that an organization's value, competency, or ethics have diminished.

Step 1: External Breach of Electronic Healthcare Record System

AVERAGE ANNUALIZED LOSS EXPOSURE

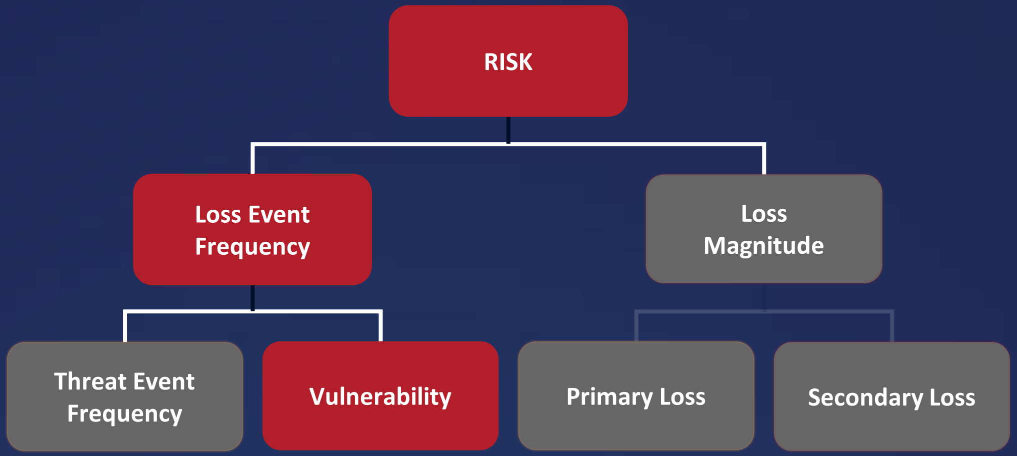


Risk Reduction: Implement MFA

$455K Reduction

FOR

$2 – 25K Investment



	Min	Most Likely	Max
Current State	5%	6.5%	15%
Proposed Change	1%	1.5%	3%

Rationale: Implementing MFA will increase the difficulty for external actors to compromise the application after gaining a foothold in the network.

Expected vulnerability reduction: **80%**