Mastering Cybersecurity Risk with FAIR
An Introduction and Case Study

Welcome

Luke Bader

Director, Membership & Programs

Mission

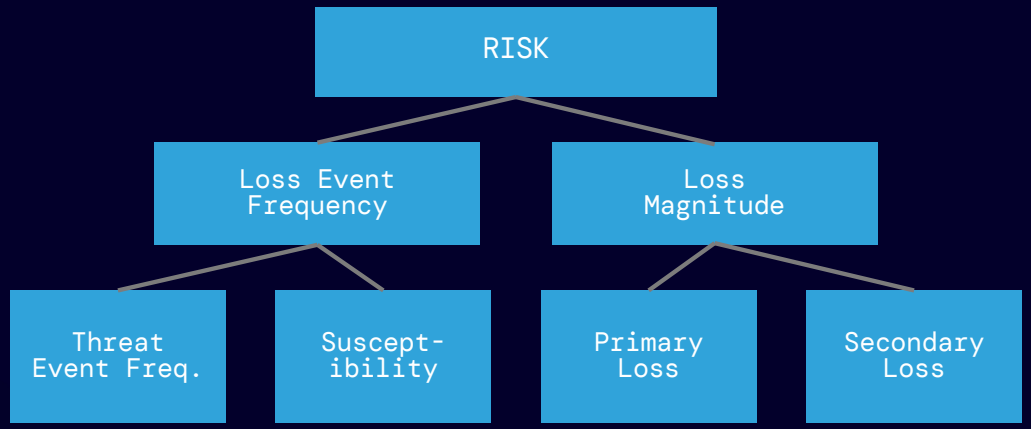
The FAIR Institute is a research-driven not-for-profit organization dedicated to advancing the discipline of cyber and operational risk management through education, standards and collaboration.

STANDARDS

EDUCATION

COLLABORATION

The FAIR Standard



The **FAIR standard** enables risk to be quantitatively defined, measured, managed and communicated

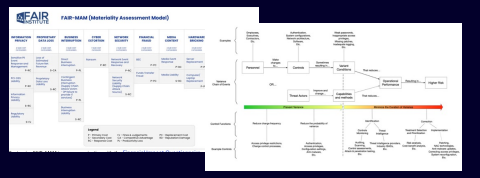
Accredited as an Industry Standard by THE Open GROUP

Complementary to Risk Frameworks

Information Security Management ISO 27001 Certified

NIST

Continuation of Standards



Education

- The FAIR Book: “Measuring and Managing Information Risk”
- Training
- Webinars
- Workshops
- Whitepapers
- FAIR Academy

FAIR Book Inducted in the Cybersecurity Canon

Collaboration

FAIR INSTITUTE
MEMBERSHIP LINK

15,000
Members Worldwide

50%
Fortune 1000

10,000+
FAIR Trained

> One of Three Most Important Industry Organizations of the Last 30 Years
>
> – SC Magazine

2024 FAIR Conference

When

Oct. 1-2, 2024

Where

Fairmont Hotel, Washington DC, Georgetown

Theme

Managing Risk at the Speed of the Business

www.fairconference.org

PREVIOUSLY FEATURED

CISO Roundtable on Generative AI

Objective: give CISOs/CXOs confidence to effectively shepherd their organizations' AI journey

- How generative AI is used to revolutionize practical AI apps
- How genAI models work & discuss their potential uses
- How a CISO organization can effectively manage genAI risks within their company
- Potential legal and ethical considerations

Scaling and Automating FAIR™ Happy Hour

When:

Tuesday, May 7 | 4:30-6:30 PM

Where:

Wine Down SF *(1 block from the Moscone Center, ~5 minute walk)*

Why Attend?

Hear firsthand from the CISO at IHG Hotels about their experiences implementing the FAIR methodology, leveraging automation, and scaling their risk management program all **in 90 days!**

REGISTER

Speakers

Jack Jones

Chairman Emeritus
FAIR Institute

Bernadette Dunn

Head of Education
FAIR Institute

INTRODUCTION TO FAIR

JACK JONES, CHAIRMAN EMERITUS

What we're going to cover today…

Part 1: Why bother? What problems does FAIR overcome?

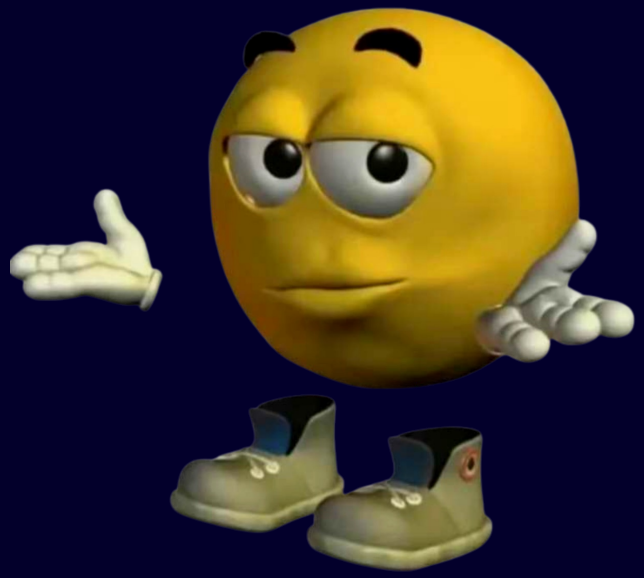
Part 2: Three criteria for good risk measurement

Part 3: FAIR Use Cases

Part 4: FAIR is an evolving model

Part 1:

Why bother…?



Medical “epochs”

Medicine as Craft

- Shamanism
- Reliance on placebo effect
- Bloodletting

Scientific but Reactive

(Focus is on diagnosis and treatment)

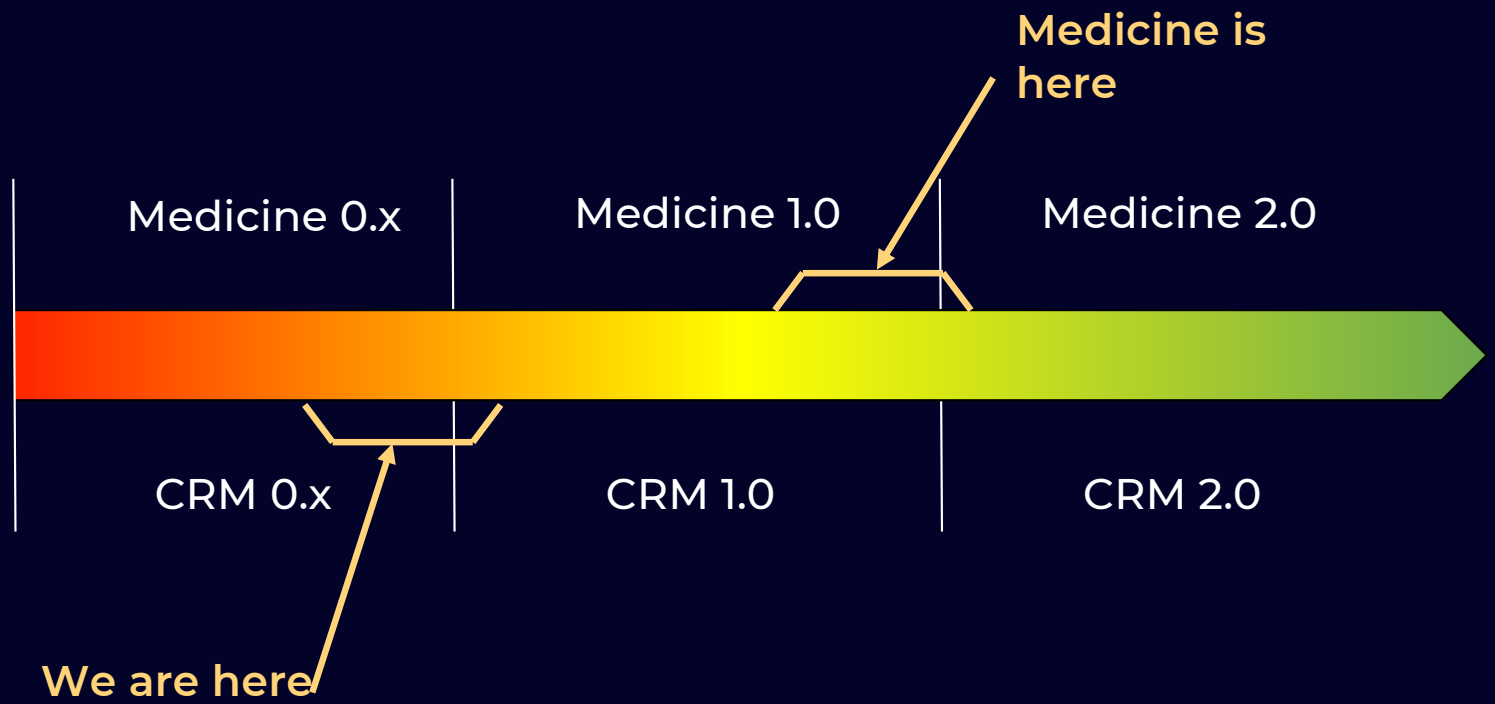
- Introduction of scientific methods
- Has given us advanced:
  - Diagnostics
  - Medicines
  - Surgeries
- Roughly doubled our lifespan

Proactive Medicine

(Focus is on “Health-span” — living longer and healthier)

- Reduces medical costs
- Understanding and treating root causes
  - Genetics
  - Environment
  - Lifestyle

Where is cyber risk management, maturity-wise?



What is the single most significant cybersecurity risk your organization faces?

How much risk reduction did your organization get from its most recent major cybersecurity initiative?

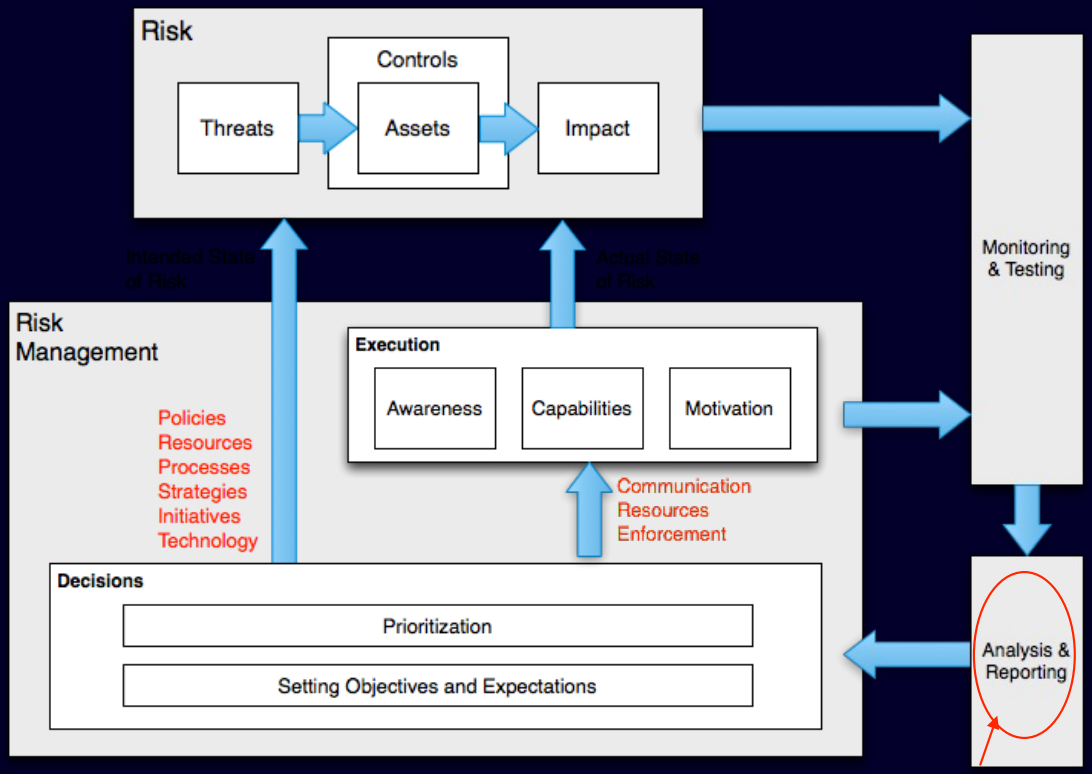
If your organization had to reduce cybersecurity costs, what would be cut from the program and how much more risk would there be?

Can you relate to one or more of these?

- “Religious battles” over risk ratings
- Too much to do — everything’s important
- How many mediums equals a high?
- Difficulty explaining expensive cybersecurity improvements
- What should the thresholds be for KRIs and KPIs?
- Executives that are too quick to accept risk

What do the answers to those questions have in common?

They’re all a function of poor risk measurement



This needs to work well!

Which of these are risks?

- Insiders
- Reputation
- Phishing
- Ransomware
- Weak passwords
- Poor cyber hygiene

Actually, none of them are risks…

- Insiders — Threat community
- Reputation — Asset
- Phishing — Method
- Ransomware — Method
- Weak passwords — Control deficiency
- Poor cyber hygiene — Control deficiency

The classic formula for risk

Risk = Likelihood x Impact

Likelihood and Impact of what?

Loss Event Scenarios

These aren’t loss events

- Insiders
- Reputation
- Phishing
- Ransomware
- Weak passwords
- Poor cyber hygiene

You can only assign likelihood and impact to loss event scenarios.

Clarifying what is and isn't a risk measurement model

Control Frameworks

ISO 2700x

CIS Center for Internet Security® Creating Confidence in the Connected World.

NIST CSF

NIST 800-53

Cybersecurity Maturity Models

C2M2 | Cybersecurity Capability Maturity Model

NIST CMMC

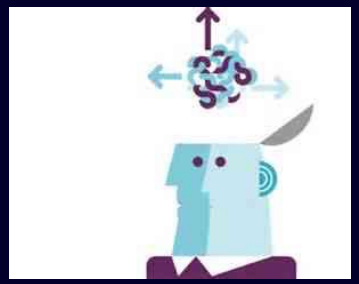
Risk Measurement Models

NIST 800-30

FAIR

Only these actually provide risk measurement

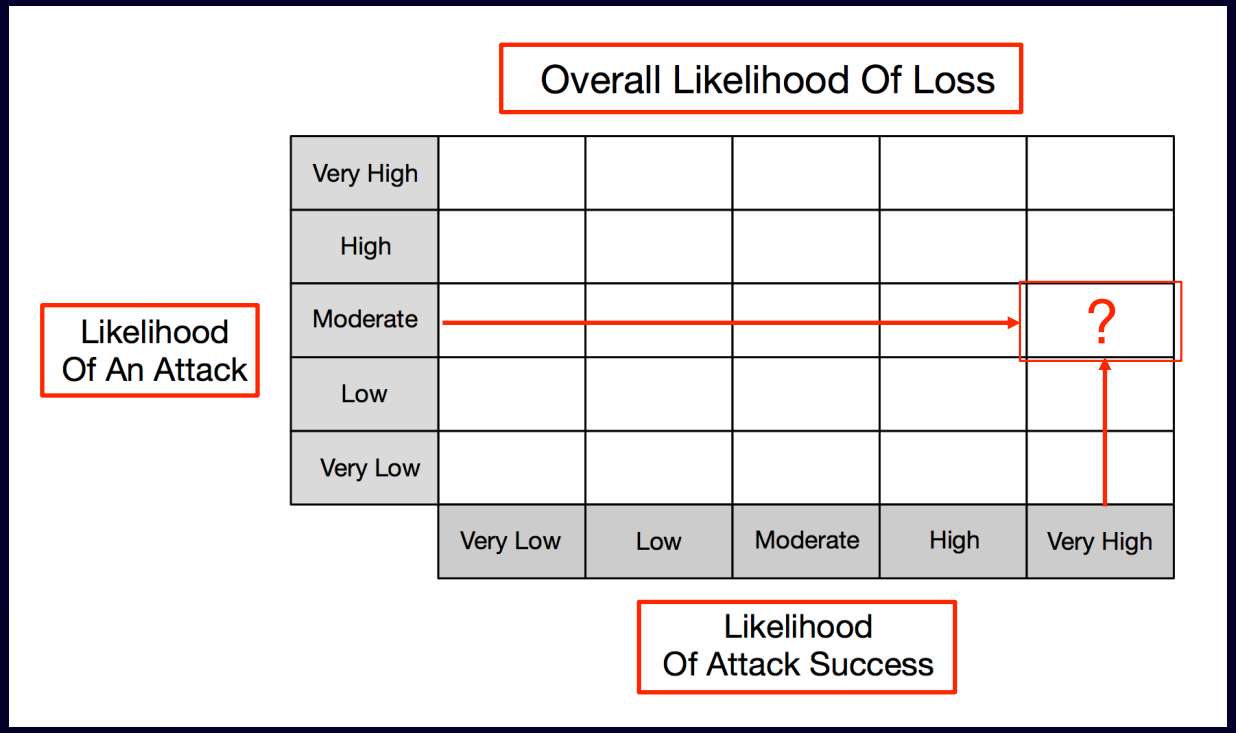
What's the most commonly used cybersecurity risk model?



Mental models

What scope? What variables? What data?

A broken cybersecurity risk model



A broken cybersecurity risk model

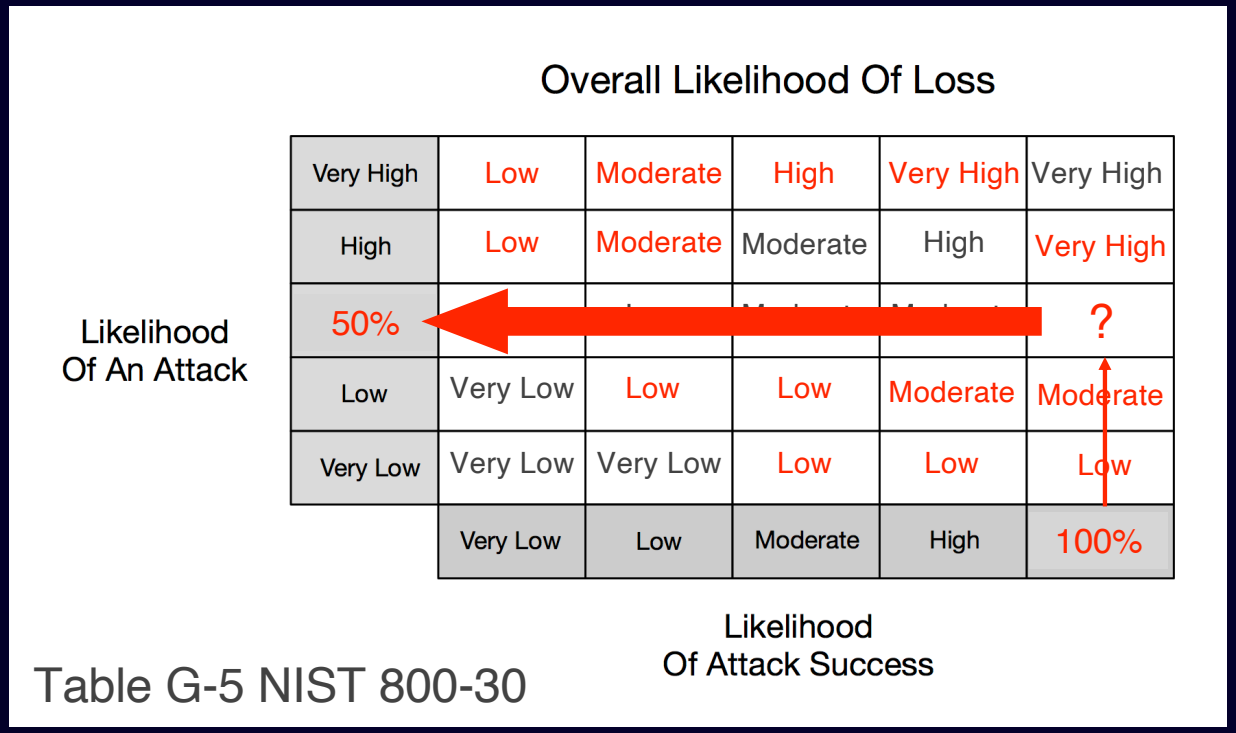
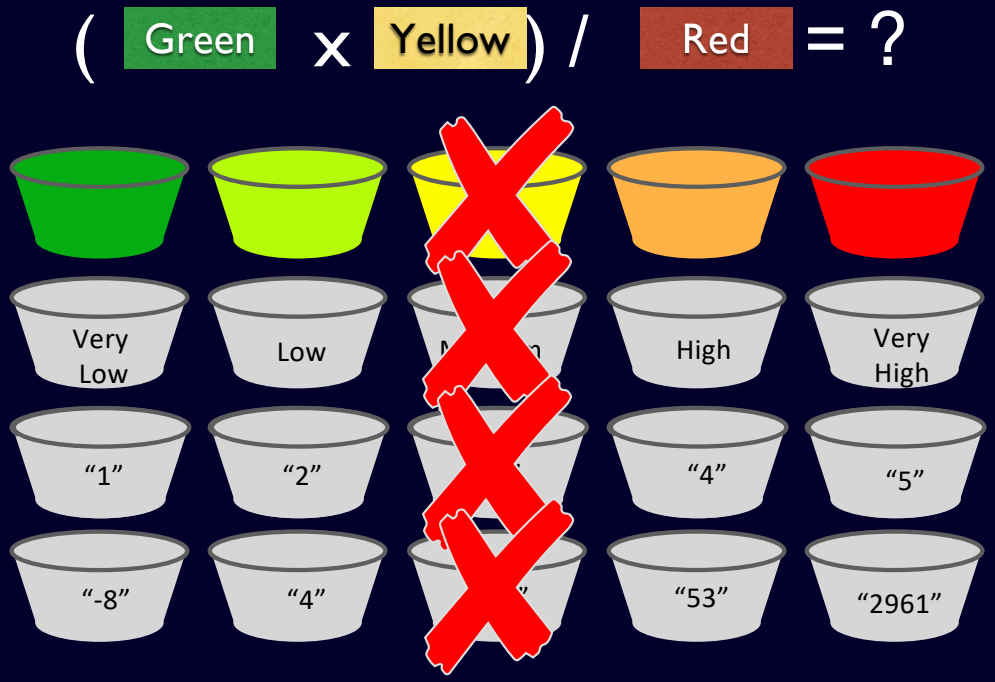


Table G-5 NIST 800-30

Math on colors



Over 70% of “high risk” findings
aren’t, in fact, high risk.

No organization I’ve encountered in the past 5 years
had accurately identified their top 10 cyber-related risks.

Key take-aways…

- We exist as a profession to help our organizations manage the frequency and magnitude of loss event scenarios.
- Today's common risk measurement practices DO NOT support that objective.

This is NOT a question of qualitative vs. quantitative measurement.

Part 2:

Three criteria for good risk measurement…

Three criteria for accurate risk measurement…

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

How fast are they going?

Qualitatively

Challenges…

- Is your “Fast” the same as mine?
- Which car am I referring to?
  - One in particular? (Slowest? Fastest?)
  - An average for all of them?
- Which part of the track am I referring to?
  - Corners?
  - The straightaway?
  - Average over the entire track?
  - This lap, or an average for the entire race?

Getting clarity…

“Likelihood”, “Probability”

The probable frequency and probable magnitude of loss from Loss Event Scenarios.

“Impact”

These are the “risks” we’re trying to manage!

Example of a clearly scoped risk (loss event scenario)

Outage of key business systems due to cybercriminals performing a ransomware attack via a phishing e-mail.

Asset
Threat
Effect
Vector
Method

Example of a clearly scoped risk (loss event scenario)

Disclosure of sensitive government documents.by a malicious insider who misuses their privileged access.

Asset
Threat
Effect
Method

Example of a clearly scoped risk (loss event scenario)

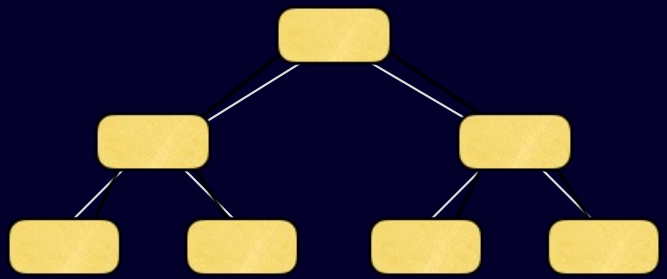
Corruption of customer financial information due to unintentional coding errors by software engineers in a new software release.

Asset
Threat
Effect
Method
Vector

Without clear scoping, the odds of measuring risk accurately are much lower…

…regardless of whether you're doing qualitative or quantitative measurement

Models



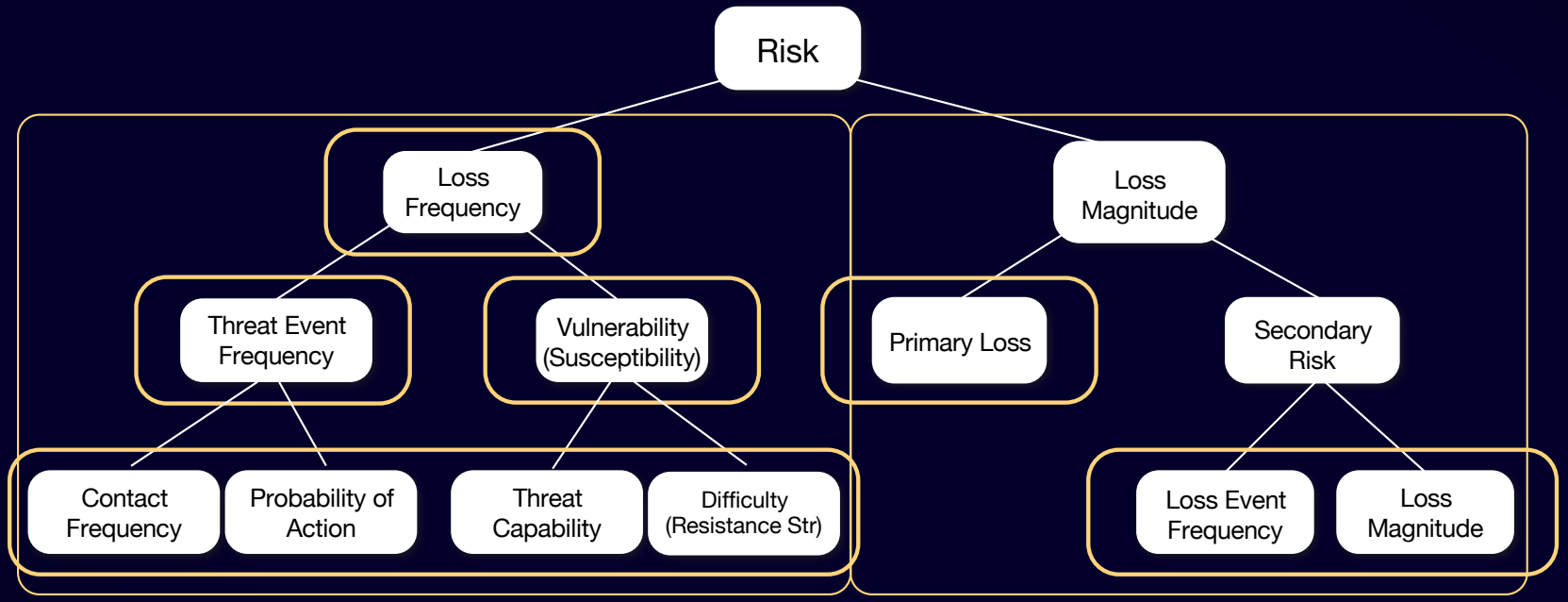
What is a model?

Models are simplified representations of a more complex reality.

Minimum risk model requirement

It must include measurement of both the probability and magnitude of loss.

The FAIR Model



Forms of Loss

- Productivity loss
- Response costs
- Replacement costs
- Competitive advantage
- Fines & Judgments
- Reputation damage

Key take-aways…

Risk measurement models enable the measurement of loss event frequency and magnitude.

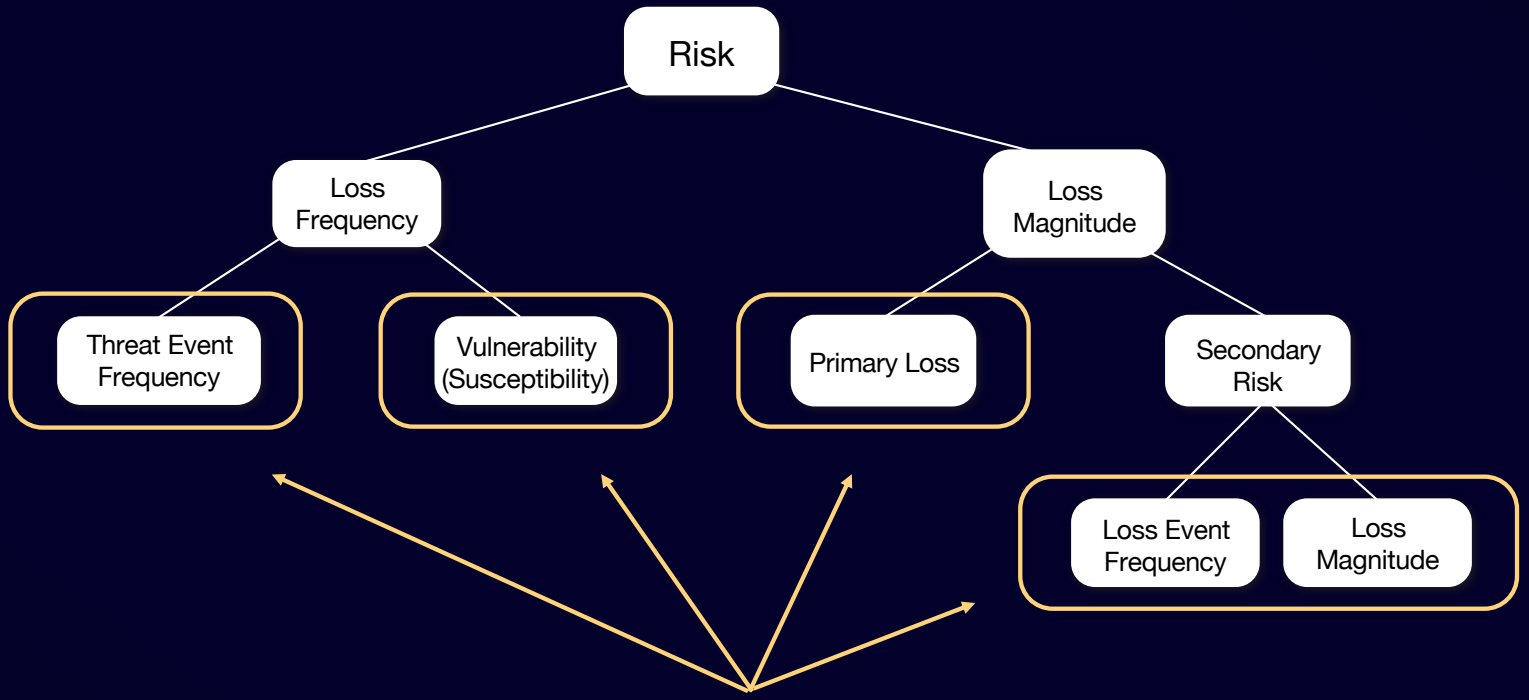
All risk measurement models involve assumptions.

Open models (e.g., FAIR, NIST 800-30) enable us to understand, challenge, and accept (or not) those assumptions.

But what about data?

What data do we need?

The FAIR Model



“We don’t have enough data.”

- “You have more data than you think you do.”
- “You need less data than you think you do.”

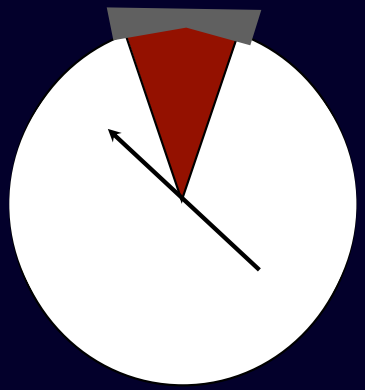
Douglas Hubbard

How tall am I?

Example

What is the wingspan of a Boeing 747?

- 1 to 1000 feet?
- 50 to 500 feet?
- 100 to 300 feet?
- 125 to 250 feet?



90% probability of landing in the white area.

For $1,000 place your bet…

What's the difference between a guess and an estimate?

An estimate is something you would place a meaningful bet on. You wouldn't place that same bet on a guess.

The problem of uncertainty…

Uncertainty is inevitable. It's simply a matter of whether it's accounted for in measurement inputs and outputs.

Using ranges and distributions to faithfully reflect uncertainty is crucial for accurate quantitative risk measurement.

Key take-aways…

Data scarcity is never a legitimate argument for not doing quantitative risk measurement.

There are well-established methods for dealing with sparse data

You have the data you have. You just need to faithfully represent uncertainty in your inputs and outputs.

The next time someone says something is “high”/“medium”/“low” risk, consider…

- Are they measuring a “risk” (a loss event scenario)?
- Has it been clearly scoped?
- What model was used?
- What data were used?
- Was it a guess or an estimation?

Back to our CRM epochs…

Today vs. the future of CRM

CRM 0.x

CRM as craft

- FUD
- Reliance on "common practice"
- Focus on compliance
- Reliance on mental models
- Reliance on qualitative measurement

CRM 1.0

Scientific but reactive

(Focus on diagnosis and treatment)

- Introduction of science
  - Formal analytic models
  - Quantitative measurement
  - Use (and sharing) of data
- Diagnosis
  - Event detection
  - Malware recognition
  - Behavioral analysis
  - Loss magnitude forecasting
- Treatment
  - Accurately prioritized remediation
  - "Personalized" solution recommendations

CRM 2.0

Proactive CRM

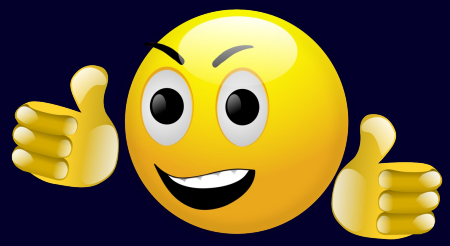
(Focus on improving organization "health-span")

- Reduce costs
- Advanced scientific methods
  - Advanced application of AI
  - Synthetic risk experimentation
  - Cyber "genetic engineering"
- Understanding and treating root causes
  - Organization environmental factors
  - Organizational "Life style" choices
  - Organization "genetics"

Part 3:

CASE STUDY

From personal life to cyber risk management examples.



Case Study Objectives

- ✓Learn how FAIR helps improve decision-making.
- ✓Practice defining risk in FAIR.
- ✓Understand the types of data used in FAIR assessments.
- ✓Interpreting results for effective decision-making.

Risk Measurement

It always starts with understanding what decision needs to be made.

What is the risk?

1- Clarify what is being measured.

I want to analyze the risk of my travel plans changing due to my boss asking me to change my logistics.

Asset

I want to analyze the risk of my travel plans changing due to my boss asking me to change my logistics.

Asset: Travel Plans/logistics

Threat

I want to analyze the risk of my travel plans changing due to my boss asking me to change my logistics.

Threat: Boss

Loss Effect

I want to analyze the risk of my travel plans changing due to my boss asking me to change my logistics.

Loss Effect: Change

2 – Accurate Risk Model

What is the probability (loss event frequency) of my travel plans changing, and what is the probable loss magnitude?

3 – Accurate Data

Over the last year:

- # of trips booked
- % of trips changed
- Travel costs:
  - Flights
  - Hotels
  - Car Rental
  - Misc. (Studio Space)
  - Travel Protection

This is Risk Assessment with Measurement!

Option A:

90% Trip Changes

Avg Cost: $5K

Fees: $160/Trip

$0 LM/Trip

ALE: $1300

Option B:

50% Trip Changes

Avg Cost: $5K

Fees: $80/Trip

$1000 LM/Trip

ALE: $2700

Option C:

2%Trip Changes

Avg Cost: $5K

Fees: $0/Trip

$5000 LM/Trip

ALE: $500

Cyber Risk Analysis Case Study

Imagine you are the leader of cybersecurity of a hospital.

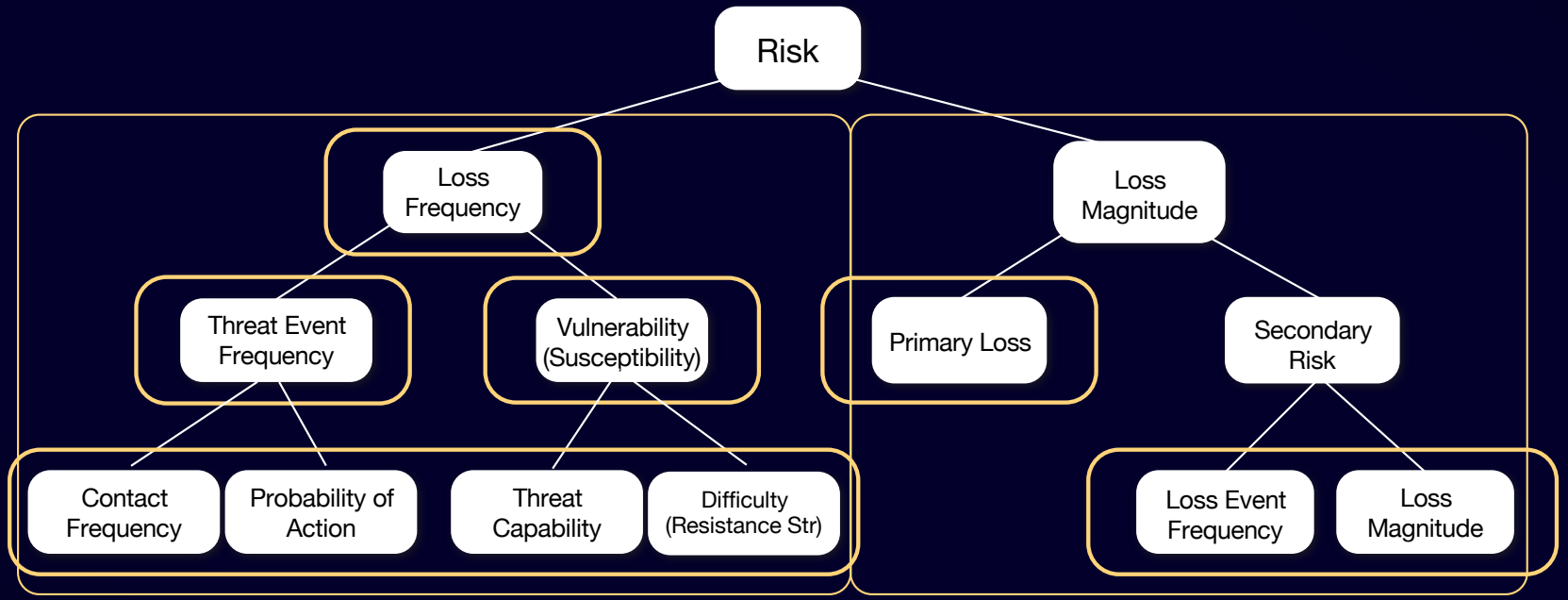
Which security controls should you invest in?

What is the risk scenario?

1- Clarify what is being measured.

- Analyze the risk of ransomware impacting the availability of the hospital's critical network system via phishing.
- Analyze the risk of ransomware impacting the confidentiality of the patient's sensitive data on the critical network system via phishing.

2- The FAIR Model



3 - TEF (Accurate) Data Sources

- Internal:
  - Secure Email Gateway detections
  - # of EDR/Malware detections
  - Reported phishing attempts
- External
  - Verizon Data Breach Investigations Report (DBIR)
  - Microsoft Digital Defense Report (MDDR)
- Research sourcing: Perplexity.ai

3 - Susceptibility (Accurate) Data Sources

- Internal:
  - Derived from layered technologies (e.g., anti-malware)
  - Anti-phishing testing
  - Coverage and reliability data
  - Attack & penetration exercises
- External
  - Vendor reports
  - Academic research
- Research sourcing: Perplexity.ai

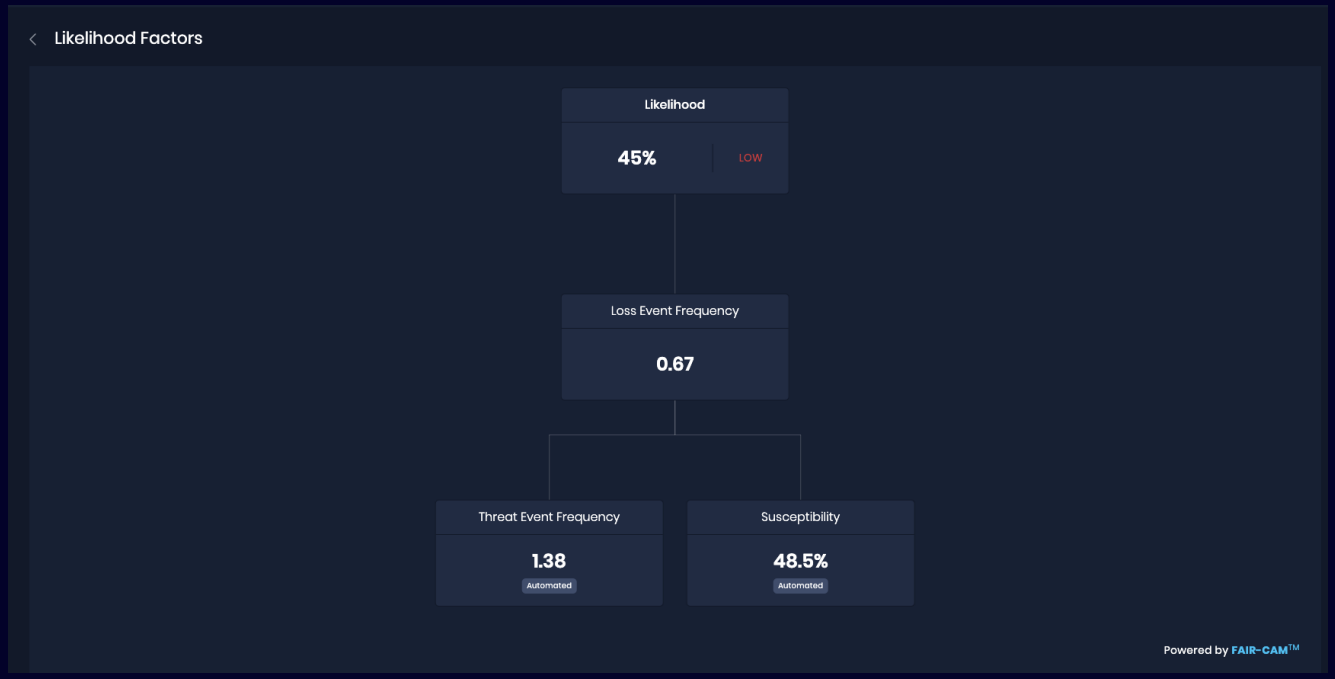
3 - High-quality Data on Various Subjects

- Cyentia Institute: cyentia.com
- The FAIR Institute: fairinstitute.org

Run the Analysis

FAIR-U tool or other FAIR Institute-approved vendors.

FAIR Risk Measurements (Ransomware Outage)

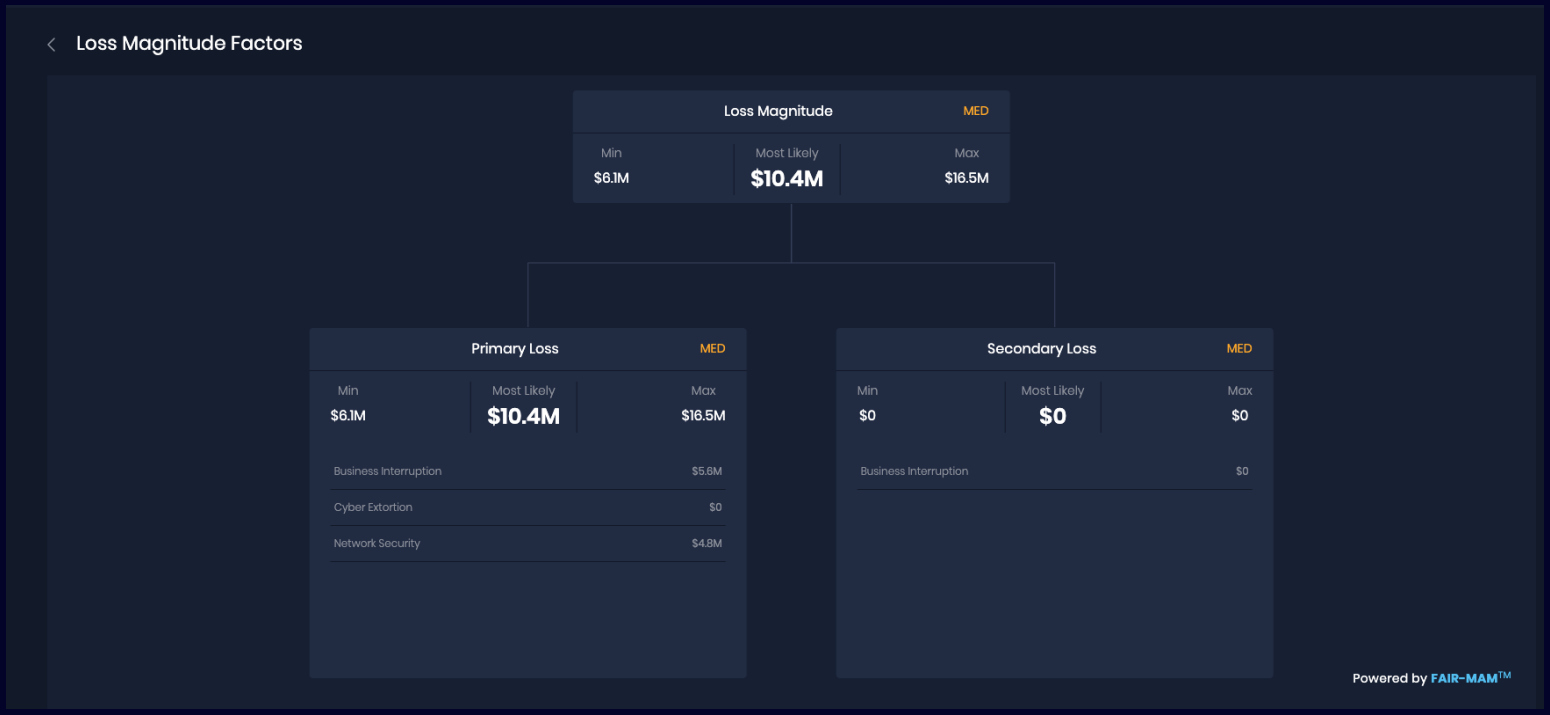


FAIR Risk Measurements (Ransomware Data)

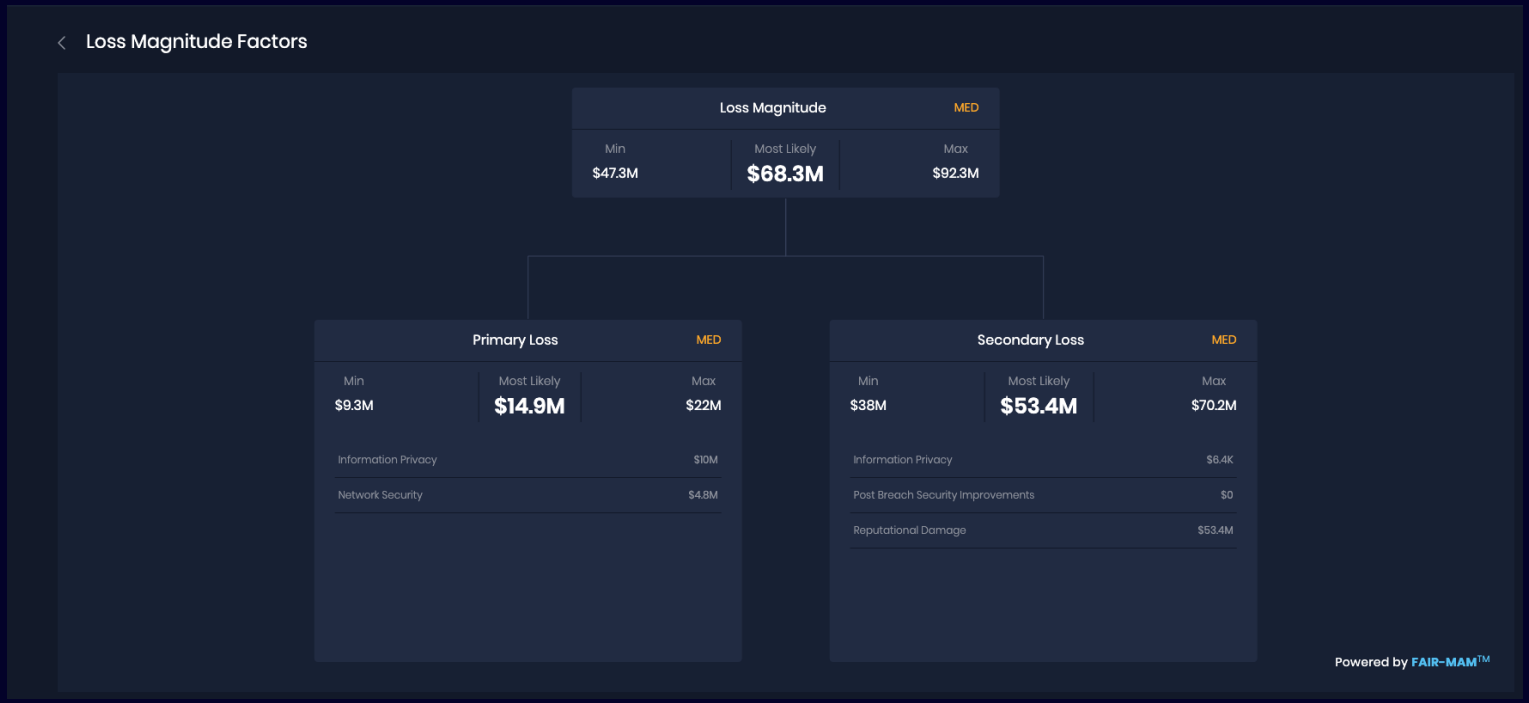
3 – Loss Magnitude (Accurate) Data Sources

- Annual Revenue
- # of unique record holders (PII, PCI, PHI)
- Hourly wage
- Incident Response
- Regulations, litigation, fines, etc.
- Gross profit margins
- Internal Department Resources: Legal, HR, IT, Finance

FAIR Risk Measurements (Ransomware Outage)

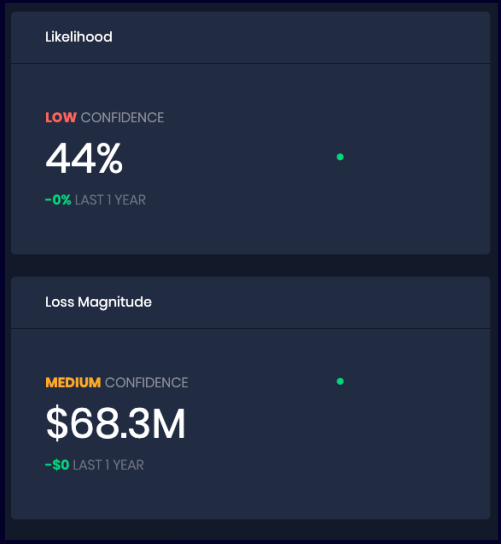


FAIR Risk Measurements (Ransomware Data)

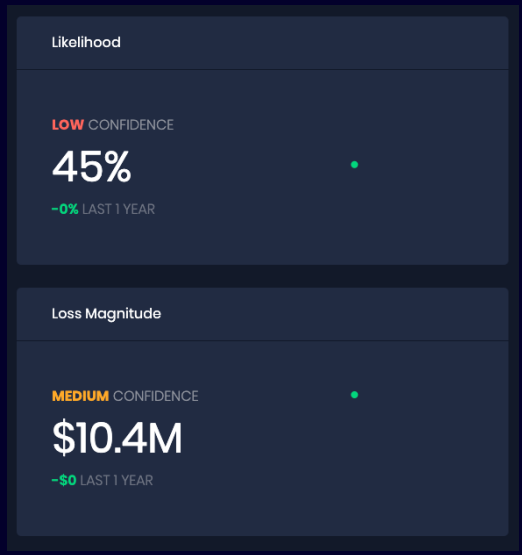


Hospital Ransomware Risk Scenarios

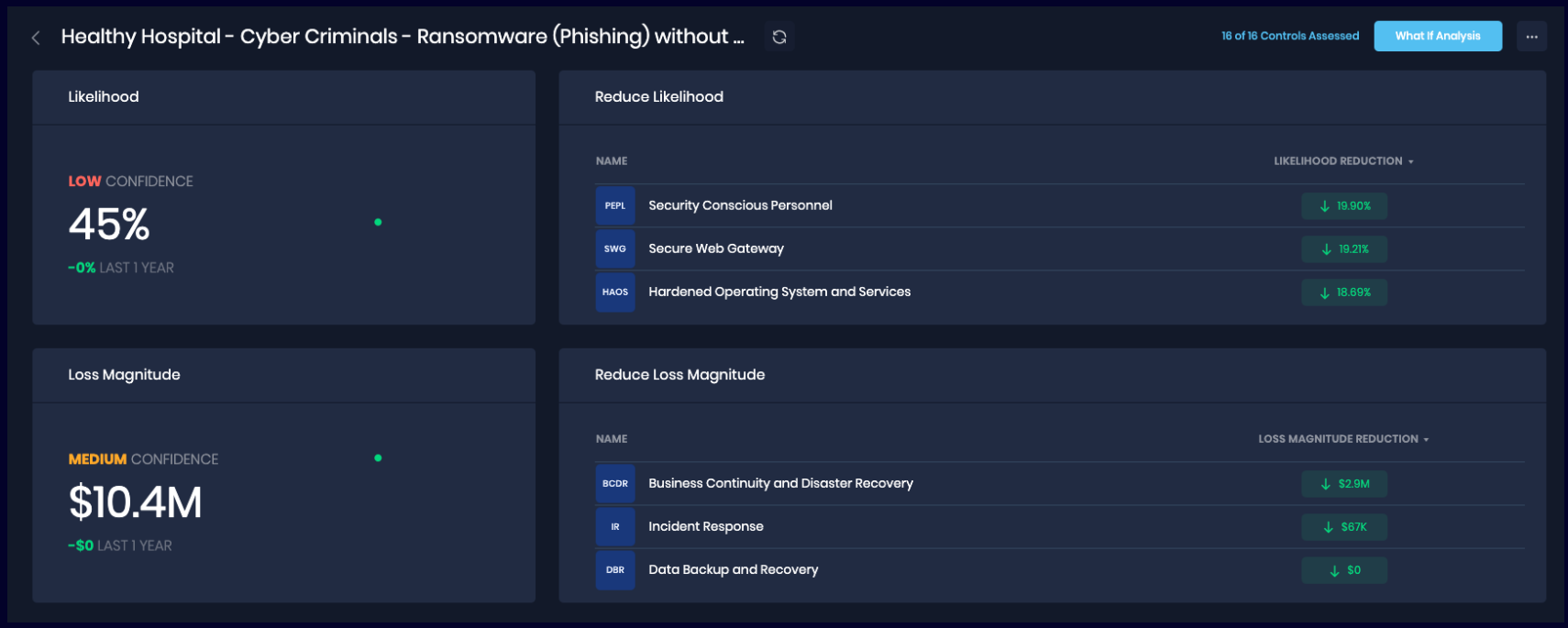
Impacting Patient Data



Impacting Critical Network



FAIR Risk Measurements (Ransomware Outage)

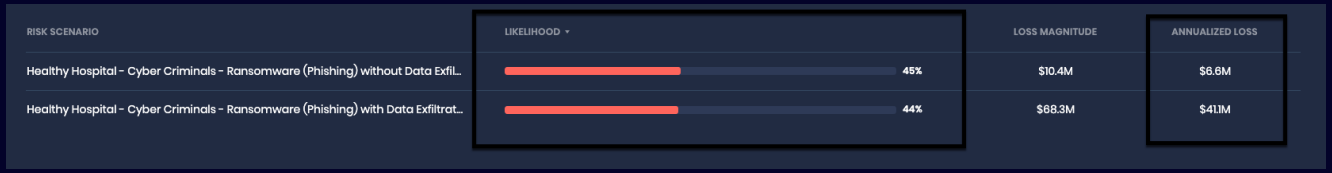


FAIR Risk Measurements (Ransomware Data)

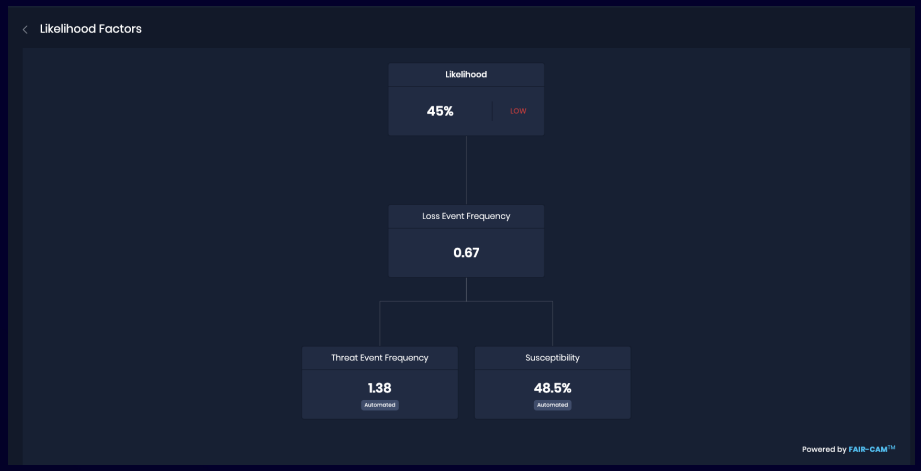
Control Improvements:

- Security Personnel Training
- Secure Web Gateway
- Incident Response

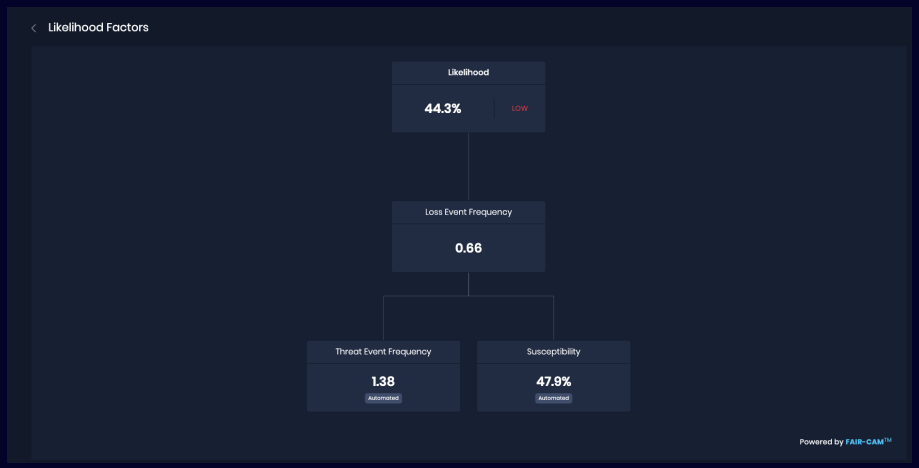
Change in Risk:



FAIR Risk Measurements (Ransomware Outage)



FAIR Risk Measurements (Ransomware Data)



Key take-aways…

- Risk Measurement (FAIR) informs decision-making.
- Clarify what risk needs to be measured.
- Use an accurate model for risk measurement.
- Practice big and small risk scenarios!

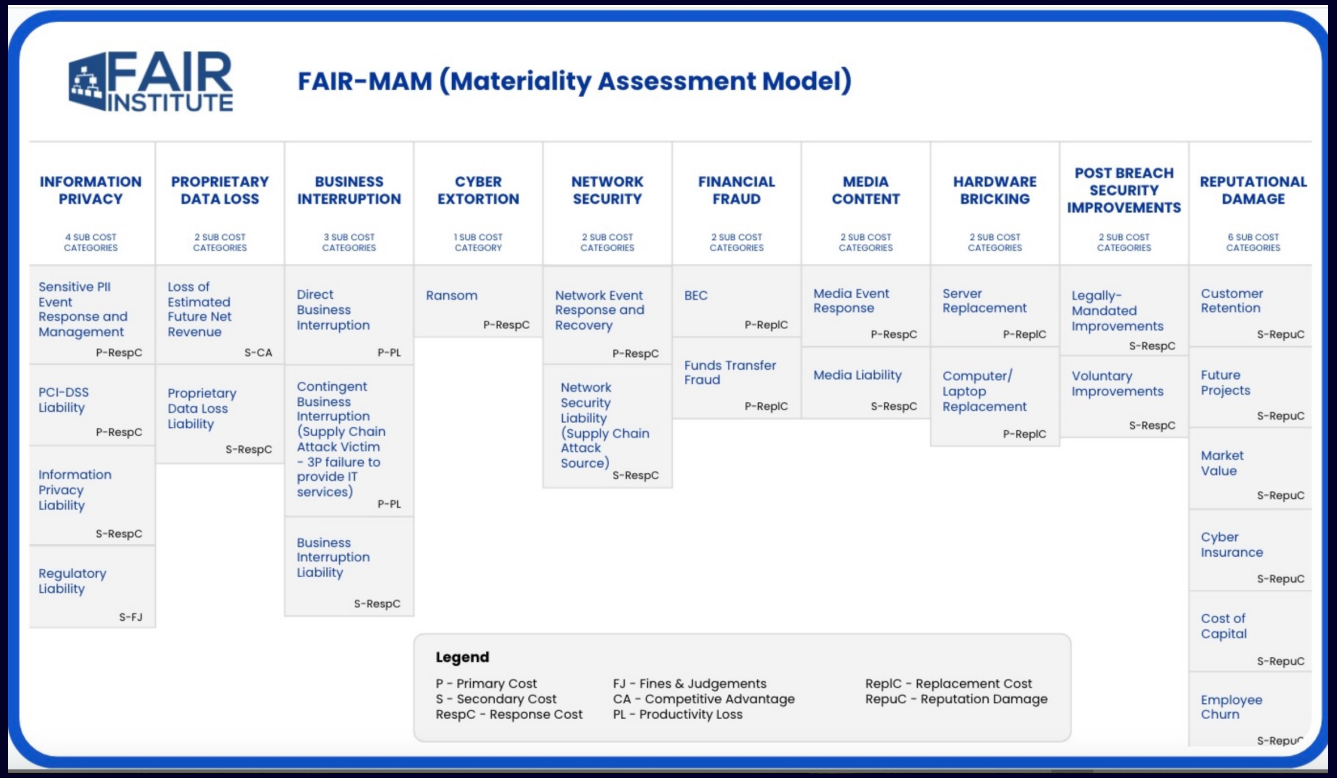
Thank you to the FAIR Institute's technical advisor, Safe Security for the use of their platform:

Part 4:

FAIR is an Evolving Model

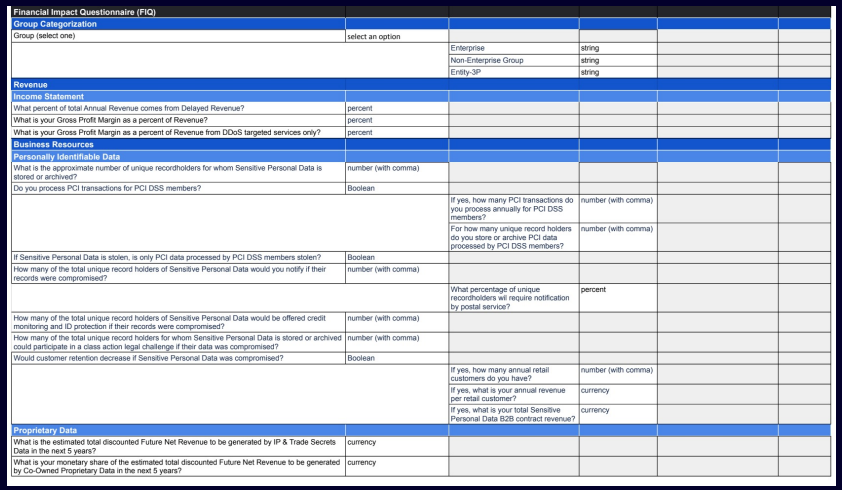
FAIR-MAM…

FAIR-MAM (Materiality Assessment Model)



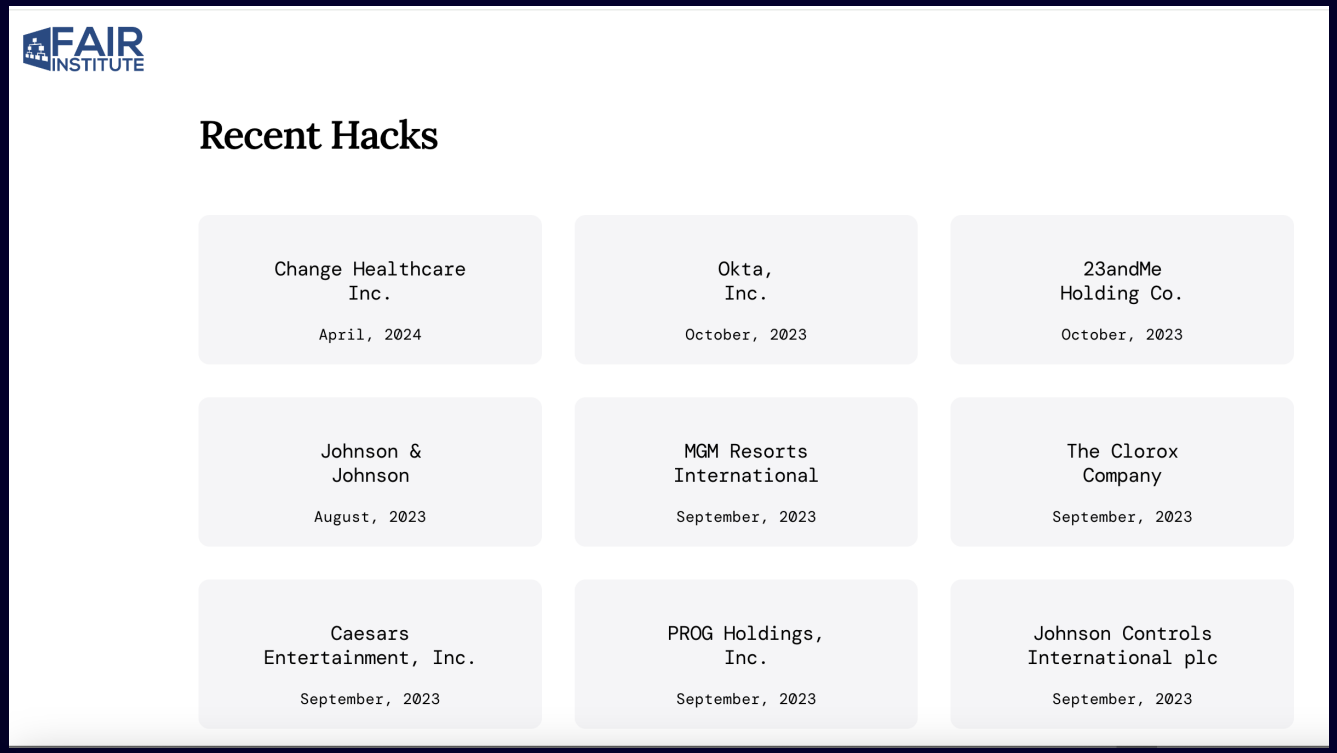
FIQ – Financial Inquiry Questionnaire

- Customize FAIR-MAM for your most accurate cyber loss.
- Download: https://www.fairinstitute.org/resources/financial-impact-questionnaire-fiq



Financial Impact Questionnaire (FIQ)					
Group Categorization					
Group (select one)	select an option				
		Enterprise	string		
		Non-Enterprise Group	string		
		Entity-3P	string		
Revenue					
Income Statement					
What percent of total Annual Revenue comes from Delayed Revenue?	percent				
What is your Gross Profit Margin as a percent of Revenue?	percent				
What is your Gross Profit Margin as a percent of Revenue from DDoS targeted services only?	percent				
Business Resources					
Personally Identifiable Data					
What is the approximate number of unique recordholders for whom Sensitive Personal Data is stored or archived?	number (with comma)				
Do you process PCI transactions for PCI DSS members?	Boolean				
		If yes, how many PCI transactions do you process annually for PCI DSS members?	number (with comma)		
		For how many unique record holders do you store or archive PCI data processed by PCI DSS members?	number (with comma)		
If Sensitive Personal Data is stolen, is only PCI data processed by PCI DSS members stolen?	Boolean				
How many of the total unique record holders of Sensitive Personal Data would you notify if their records were compromised?	number (with comma)				
		What percentage of unique recordholders wil require notification by postal service?	percent		
How many of the total unique record holders of Sensitive Personal Data would be offered credit monitoring and ID protection if their records were compromised?	number (with comma)				
How many of the total unique record holders for whom Sensitive Personal Data is stored or archived could participate in a class action legal challenge if their data was compromised?	number (with comma)				
Would customer retention decrease if Sensitive Personal Data was compromised?	Boolean				
		If yes, how many annual retail customers do you have?	number (with comma)		
		If yes, what is your annual revenue per retail customer?	currency		
		If yes, what is your total Sensitive Personal Data B2B contract revenue?	currency		
Proprietary Data					
What is the estimated total discounted Future Net Revenue to be generated by IP & Trade Secrets Data in the next 5 years?	currency				
What is your monetary share of the estimated total discounted Future Net Revenue to be generated by Co-Owned Proprietary Data in the next 5 years?	currency				

www.HowMaterialIsThatHack.org



FAIR-CAM: Defining controls “physiology”…

“Half of your marketing dollars are wasted.

You just don’t know which half.”

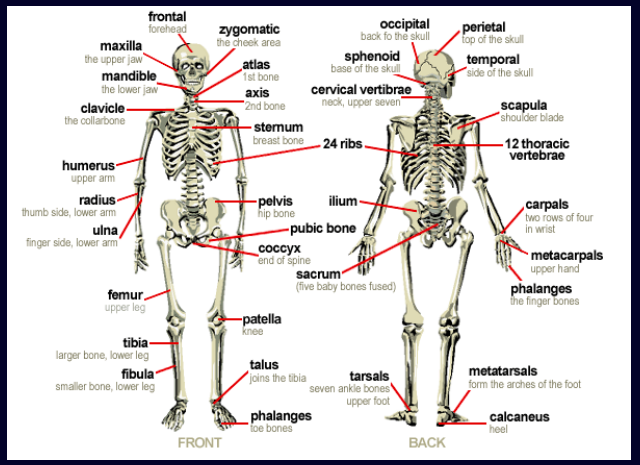
An old marketing proverb

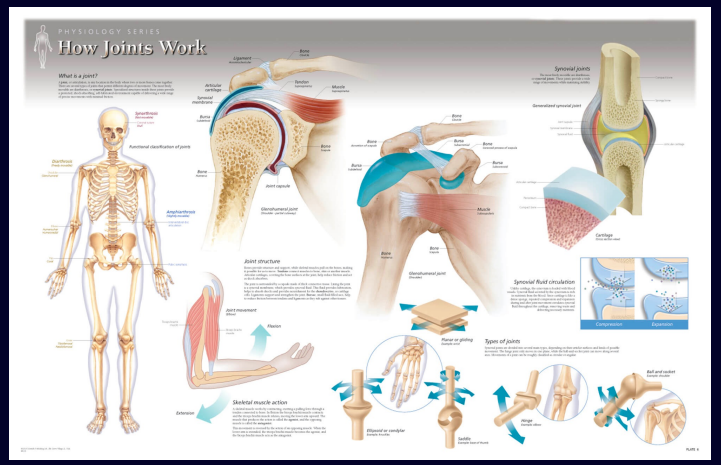
In the practice of medicine, which is more important?

Anatomy?
(The parts of the system)

OR

Physiology?
(How the system works)



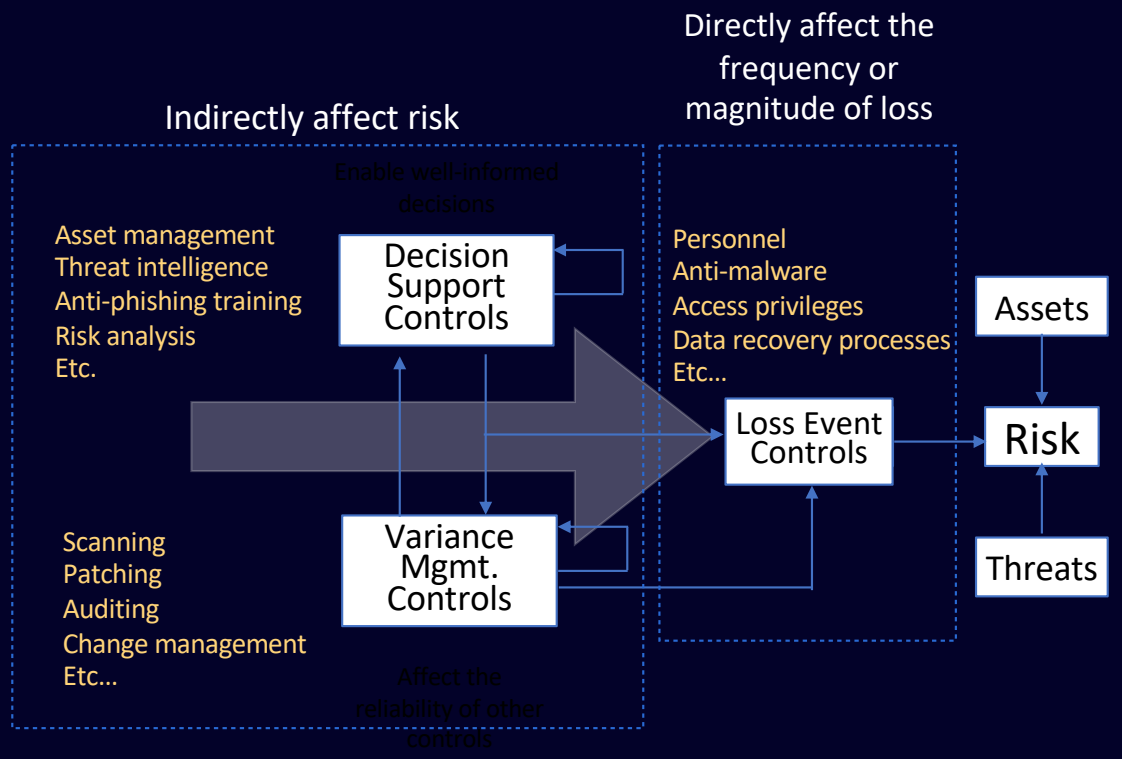


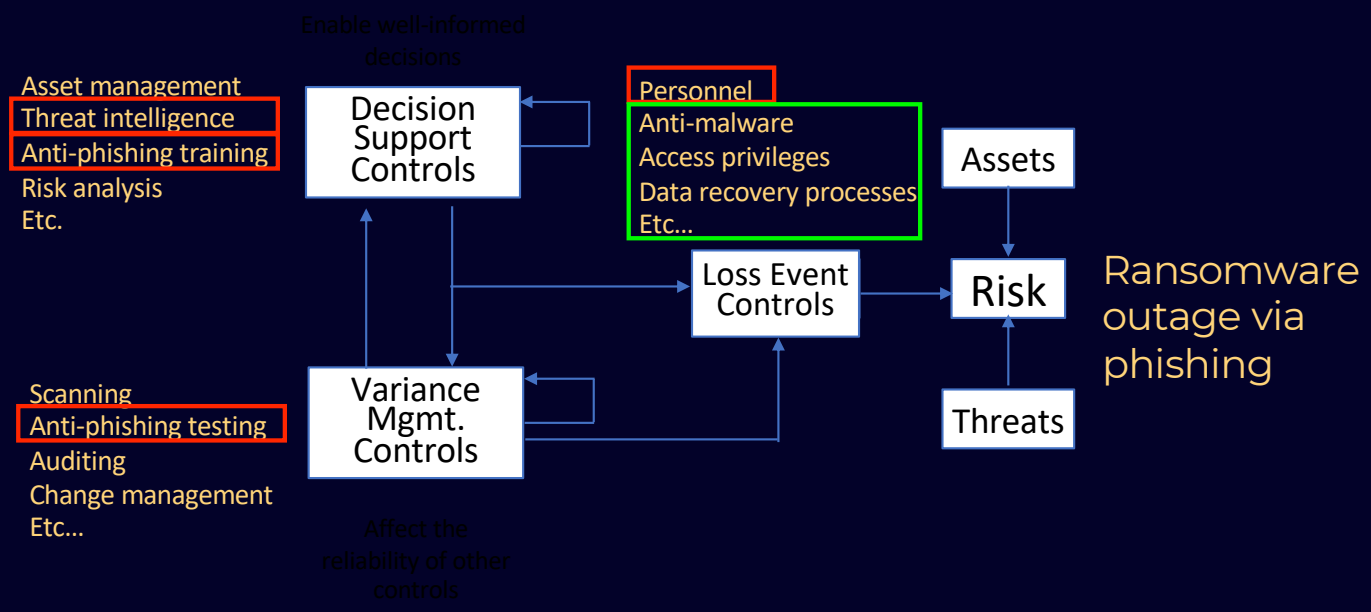
Neither. You need to know both.

Existing control frameworks describe control anatomy.

To-date, there has been no equivalent to control physiology.

Direct vs. indirect effects on risk





The FAIR Controls Analytics Model (FAIR-CAM)

FAIR-CAM defines control physiology — i.e., how the control landscape works as a complex system of interdependent parts.

This enables us to evaluate and empirically measure the efficacy and risk reduction value of controls.

Supporting Automation and AI

Automated risk measurement…

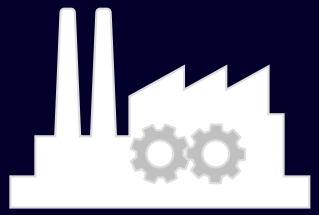
Threat intelligence services
Organization's own logs

Cybersecurity telemetry
CIS controls scores

FAIR Institute
Verizon DBIR
Insurance providers

NIST CSF scores
System config data
Program maturity scores

Which of these is more important?



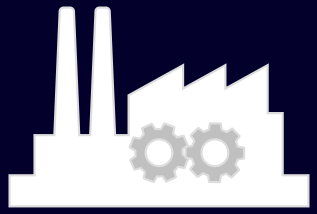
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Is it twice as important? Three times…?

Control relevance is context sensitive!

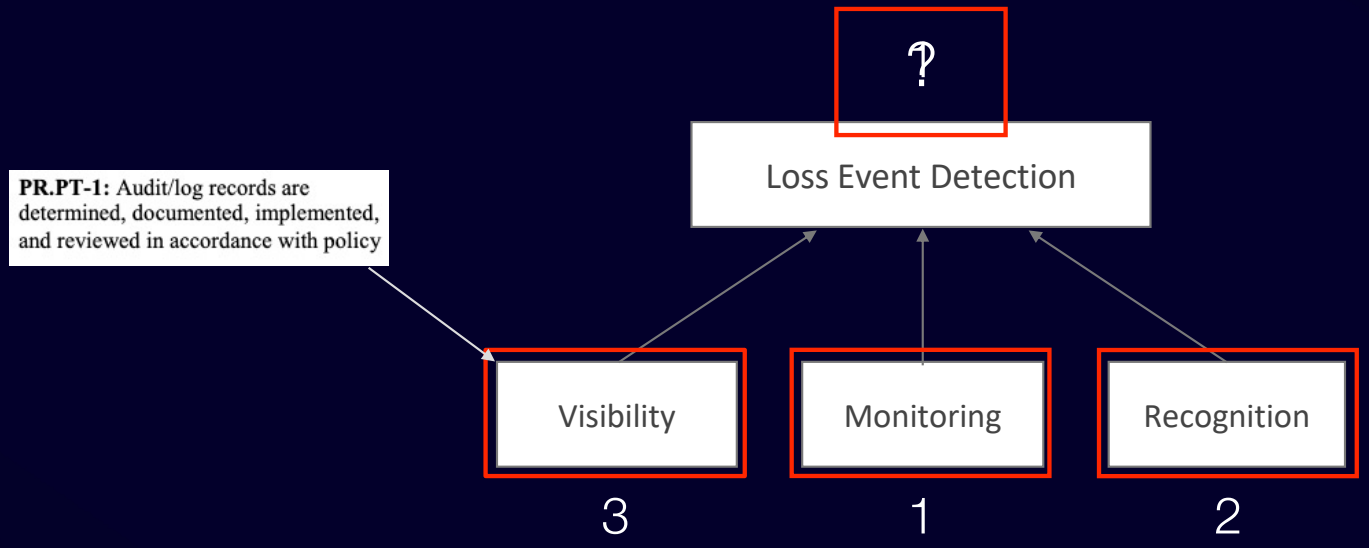
How does a control affect risk?



Does logging affect likelihood, or magnitude?

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Control dependencies…

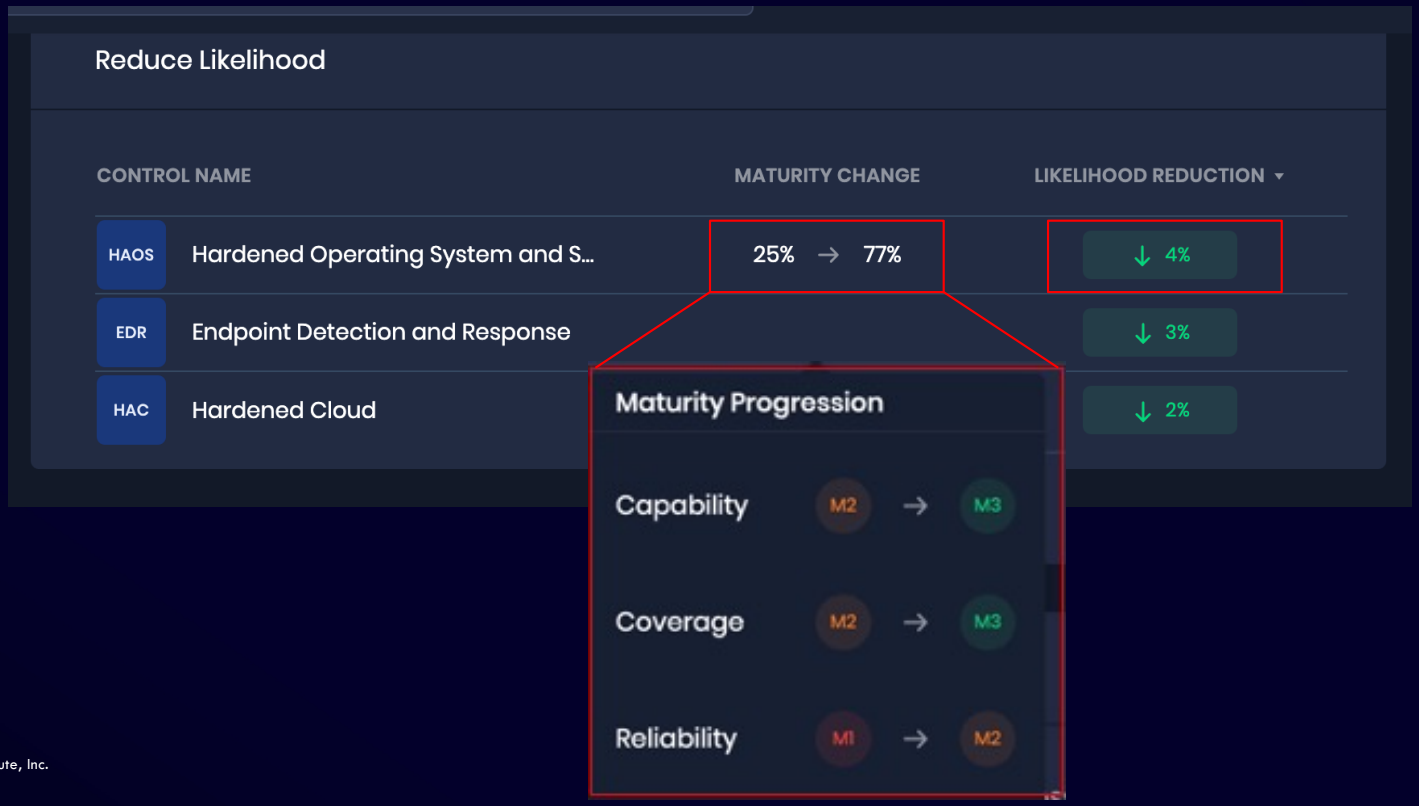


VISIBILITY: There has to be data that contains evidence of a breach (e.g., logs)

MONITORING: Someone or something has to review the data (e.g., manual reviews, SIEM, etc.)

RECOGNITION: Exploit signatures, malware signatures, baselines of normal activity, etc.

Example automation output



Key take-aways…

- How controls affect risk is not well understood.
- Control relevance is highly context sensitive.
- Controls often have key dependencies with other controls.
- If automation fails to account for control physiology, analysis results will be inaccurate.

Control data we need…

- Intended condition (design and configuration)
- Reliability (frequency and duration of deficiencies)
- Coverage

Controls telemetry sources

- Anti-malware and xDR solutions
- DLP solutions
- Anti-phishing solutions
- Configuration management tools
- Vulnerability scanners
- Continuous control monitoring solutions
- Etc…

Wrapping up

Summary

- We measure risk in order to make decisions and take actions that affect the frequency and magnitude of loss event scenarios.
- Common risk measurement practices today do not enable us to measure risk reliably.
- Risk measurement best practices require:
  - Clarity: You can't reliably measure what you haven't clearly defined
  - An accurate model: Note that all models require assumptions
  - Explicit consideration of data: Data will always have uncertainty. The key is to faithfully account for and communicate uncertainty.
- Those requirements are true for qualitative or quantitative risk measurements.

The value of FAIR-based risk measurement

- Enables accurate risk measurement in economic terms
  - Significantly improves prioritization
  - Supports cost-benefit analysis of security efforts
  - Economic expression of risk is familiar to many executives
  - Enables comparing risk vs. other economically measured organization imperatives (revenue, cost, etc.)
- Also…
  - Surfaces assumptions so they can be recognized and challenged
  - Improves risk-related conversations and collaboration

Thank You!