2019

Combining two International Standards

# NIST CSF AND FAIR




RiskLens®





RiskLens®

# EXPECTATIONS FOR CISOs HAVE CHANGED





RiskLens®

# THE COMMUNICATION CHALLENGE

**CFO**

"How much risk do we have? Are we spending too little or too much on mitigation?"

**AUDIT**

"Did you fix those high priority issues?"

**BOARD/CEO**

"We don't want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?"

**CIO**

"Are we spending our cybersecurity budget on the right things? What is the ROI?"

**CISO**

"Εχουμε πάνω από δέκα χιλιάδες τρωτά σημεία , είναι συμβατό με το ογδόντα τοις εκατό"




RiskLens®

# NEW SEC GUIDANCE ON CYBER RISK DISCLOSURE

MERE ENUMERATION OF CYBER RISK FACTORS NO LONGER ACCEPTABLE

CYBERSECURITY RISKS AND INCIDENTS TO BE REPORTED IF "MATERIAL" TO THE FINANCES OF THE COMPANY

Disclosures to include:

- Frequency of cyber events
- Probability and magnitude of incidents - costs, in financial terms
- Adequacy of controls
- Potential reputational harm
- Potential fines and judgements

## Controls and procedures should enable companies to

- *identify cybersecurity risks and incidents,*
- *assess and analyze their impact on a company's business,*
- *evaluate the significance associated with such risks and incidents,*
- *provide for open communications between technical experts and disclosure advisors, and*
- *make timely disclosures regarding such risks and incidents.*

SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures – Feb. 26, 2018




RiskLens®

# COMPLIANT... BUT STILL IN THE DARK

1

Qualitative Checklists & Excel


2

Governance, Risk & Compliance Tools

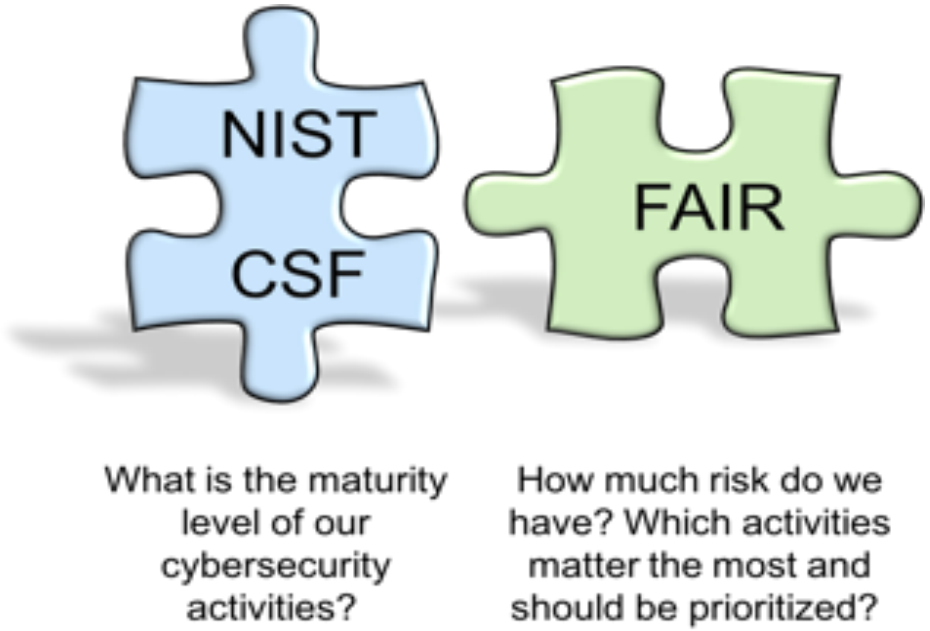

No embedded risk analytics capabilities in most GRC tools

The way most organizations measure risk today fails to quantify cybersecurity and operational risk in terms the business can understand and use




RiskLens®

# MARRYING NIST-CSF AND FAIR




"How is **FAIR** different from (or better than) a framework like **NIST's Cybersecurity Framework (CSF)**?"

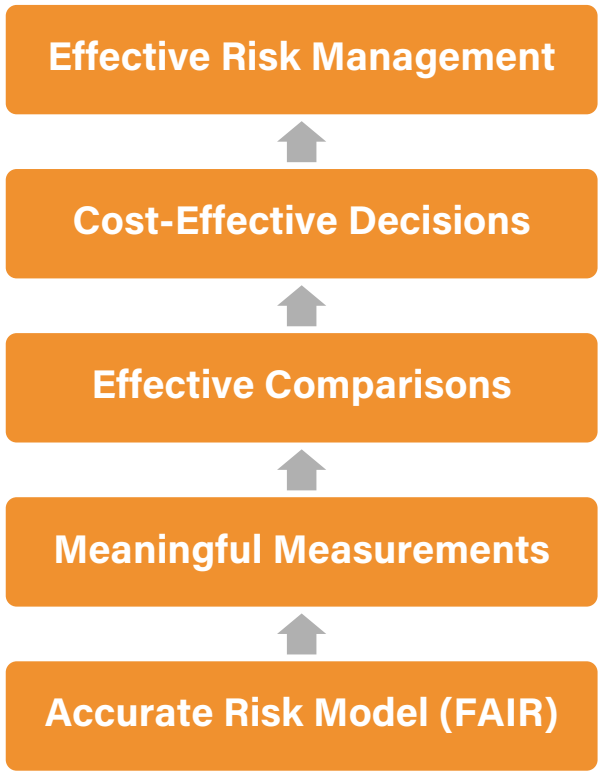
The simple answer:

FAIR isn't inherently better or worse - it is fundamentally different and, in fact, complementary.




RiskLens®

# EFFECTIVE RISK MANAGEMENT




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"




RiskLens®

# FAIR: A STANDARD RISK SCOPING MODEL

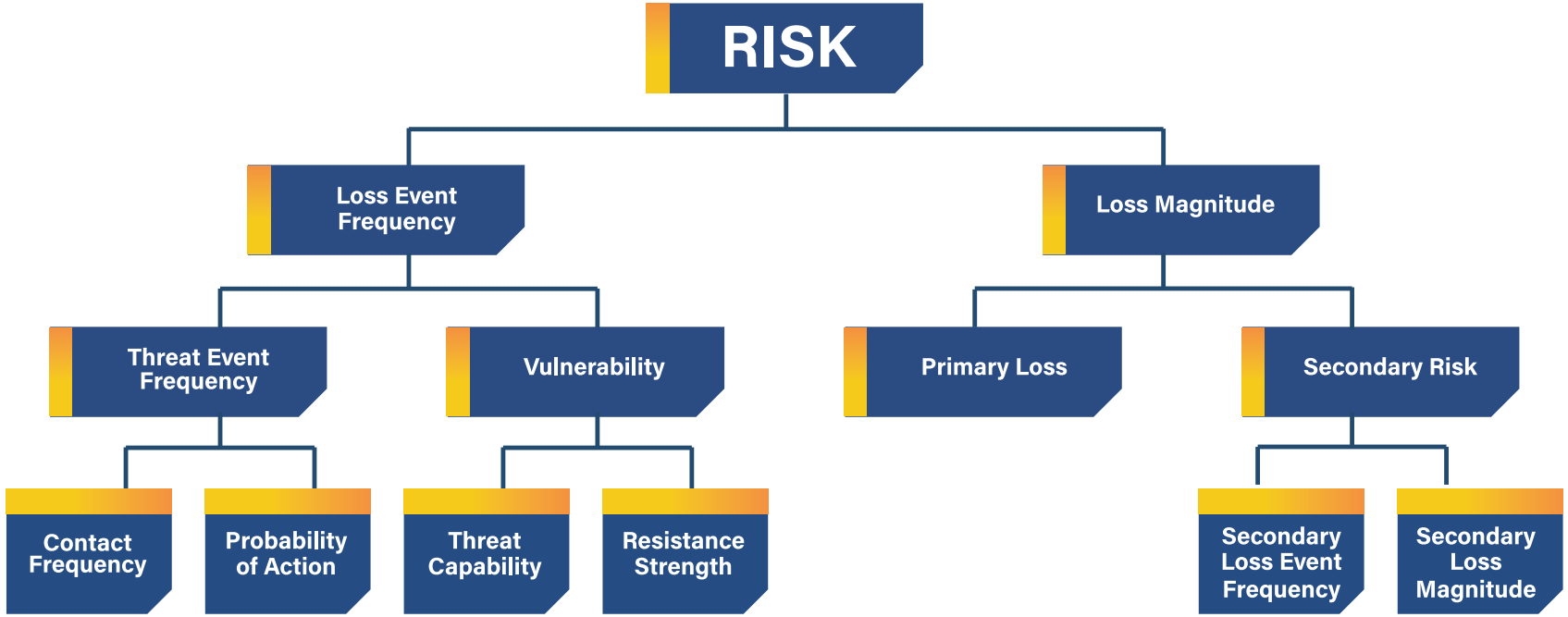
## WE CAN ONLY ASSESS THE RISK OF LOSS EVENTS


**RISK (LOSS EXPOSURE) SCENARIO**



RiskLens®

# FAIR: A STANDARD RISK ANALYTICS MODEL




**Accredited as an Industry Standard by**

THE Open GROUP

**Complementary to Risk Frameworks**

ISO 27001 NIST

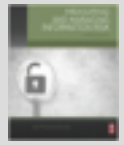
**Supported by a Fast Growing Community**

FAIR INSTITUTE

**Wide Industry Adoption 30% Fortune 1000**

FORTUNE 1000

**FAIR Book Inducted in Cybersecurity Canon**






RiskLens®

# IAN AMIT – CHIEF SECURITY OFFICER – CIMPRESS




RiskLens®

# INTRODUCTION

**Ian Amit**
**Chief Security Officer**
Cimpress

- Decades as a Security Practitioner
  - President of Board – BSides Las Vegas
  - Founding member of the PTES (Penetration Testing Execution Standard
  - Founding member IL-CERT and Tel-Aviv DEFCON Group
  - Formerly at ZEROFox, IoActive, Amazon, et al.
  - Frequent speaker at BlackHat, DEFCON, RSA, BSides, BlueHat, etc.

cimpress

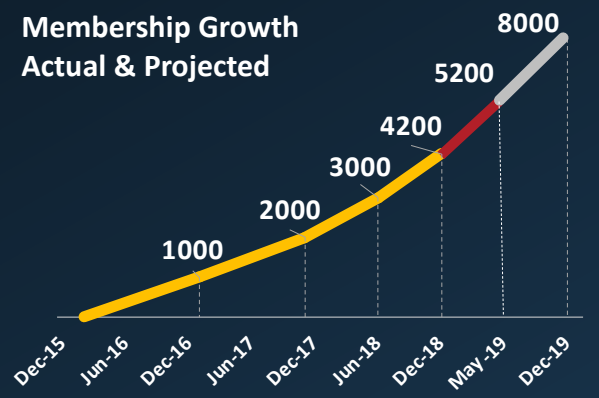


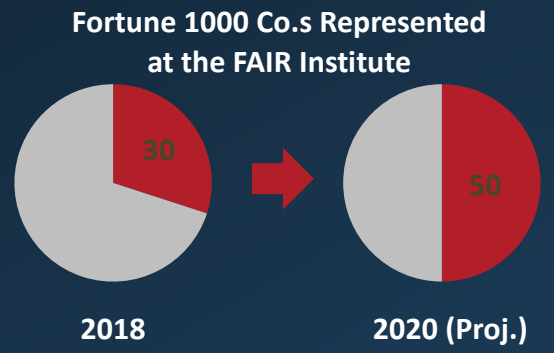

RiskLens®

# FINDING FAIR – MY HISTORY

- Realization: We need better risk management in cyber
  - As a consultant – trying to find better ways to help my customers build and manage security programs
  - Ran across FAIR in 2010, and realized it codified a lot of what I was practicing
  - Enabled quantification where we had previously been led to believe impossible
  - FAIR trained in 2010
    - On-line training resources available
    - On-site training for larger teams
    - www.fairinstitute.org
  - Been practicing ever since ;-)

FAIR INSTITUTE







RiskLens®

# MARRYING NIST-CSF AND FAIR

## NIST-CSF

- Maturity framework driving our strategy at Cimpress
- Tactical level view of specific security capabilities

## FAIR

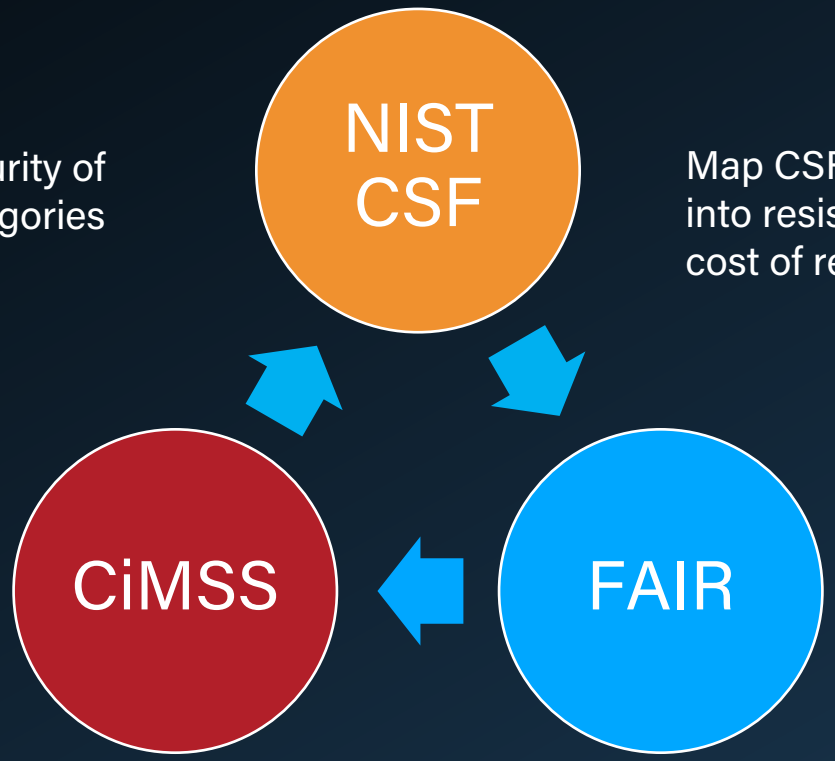
- Risk framework driving our strategy at Cimpress
- Top down risk approach for the organization

We balance the two frameworks
Tie them together with CSF affecting specific elements of FAIR
Enables more independent risk measurements with less reliance on SMEs for providing resistance strength




RiskLens®

# OUR NIST-CSF | FAIR WORKFLOW







RiskLens®

# OUR NEAR TERM ROADMAP

- Add more automation and reporting capabilities around FAIR loss scenarios and risk analysis
  - Recently became a RiskLens Platform client
- Add more automation in updating the NIST-CSF maturity levels
- Further the use of FAIR through other risk practices – ERM specifically

# CHIP BLOCK – VICE PRESIDENT – CONVERGED SECURITY SOLUTIONS

# INTRODUCTION

Chip Block– Vice President, Chief Solutions Architect

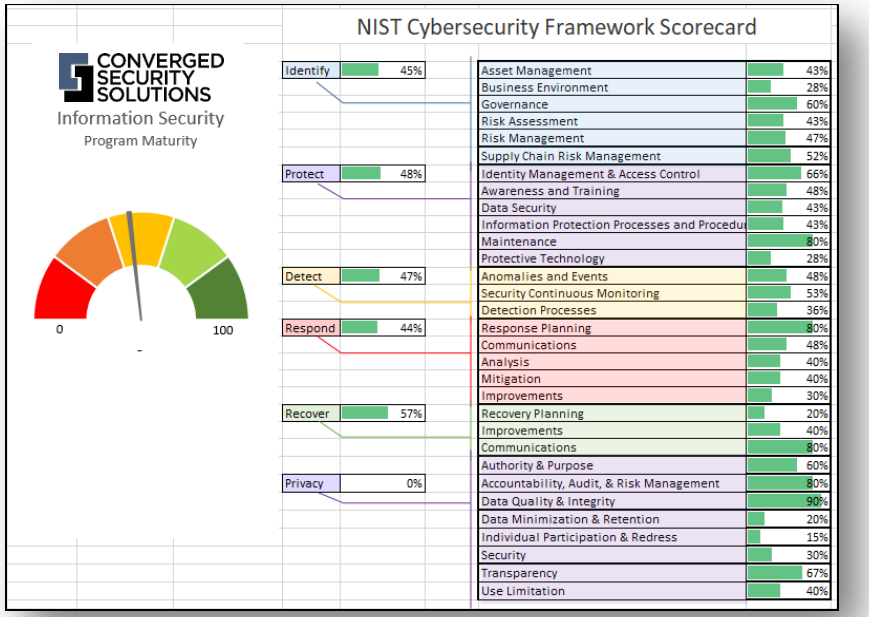
Converged Security Solutions

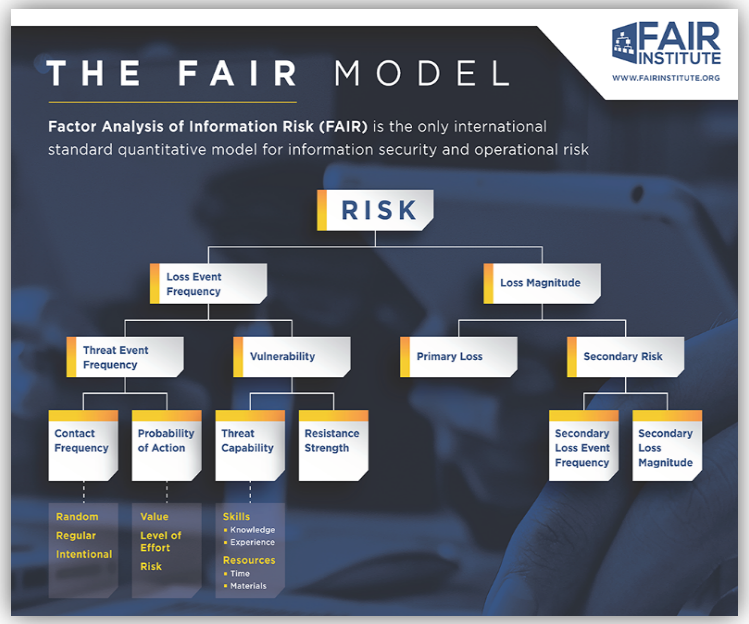
- Works extensively in cyber research, development & operations for Federal, Commercial/Financial & Legal Clients
- Architect of CSS' Cyber Risk Ecosystem
- Frequent author and speaker on cybersecurity, cyber risk, and cyber insurance
- Awarded several high level honors for his advanced technological achievements
- Chair, DC FAIR Chapter




RiskLens®

# APPLYING NIST-CSF 800-53 to FAIR ANALYSES




Leveraged Existing Maturity Evaluation To Do FAIR Analysis

Leveraged FAIR Analysis To Do Maturity Evaluation



RiskLens®

# SURPRISING FINDINGS

FAIR analyses are specific to the organization…much more so than the generic NIST-CSF framework.

FAIR shows that it is often times better to invest in a control area that is already mature than improving a less mature control

Dozens of Engagements Across Verticals





RiskLens®

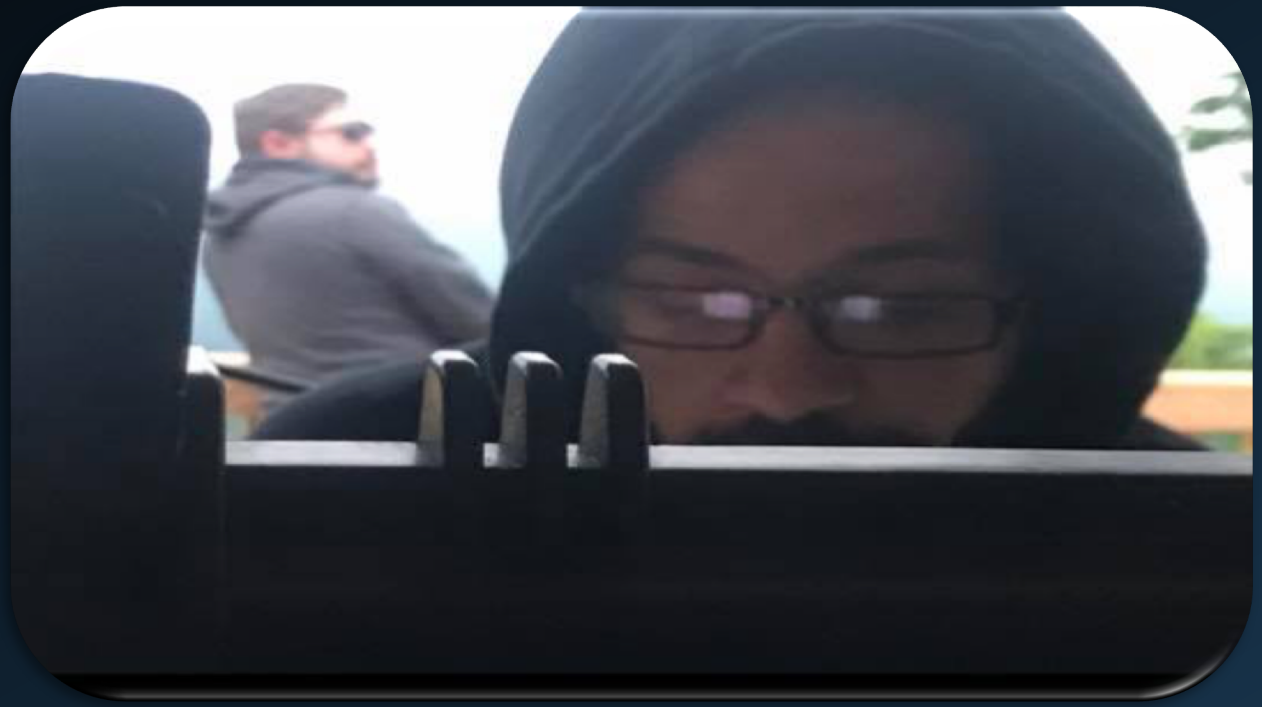
# CONTROL EVALUATIONS – IN THE FAIR MODEL





RiskLens®

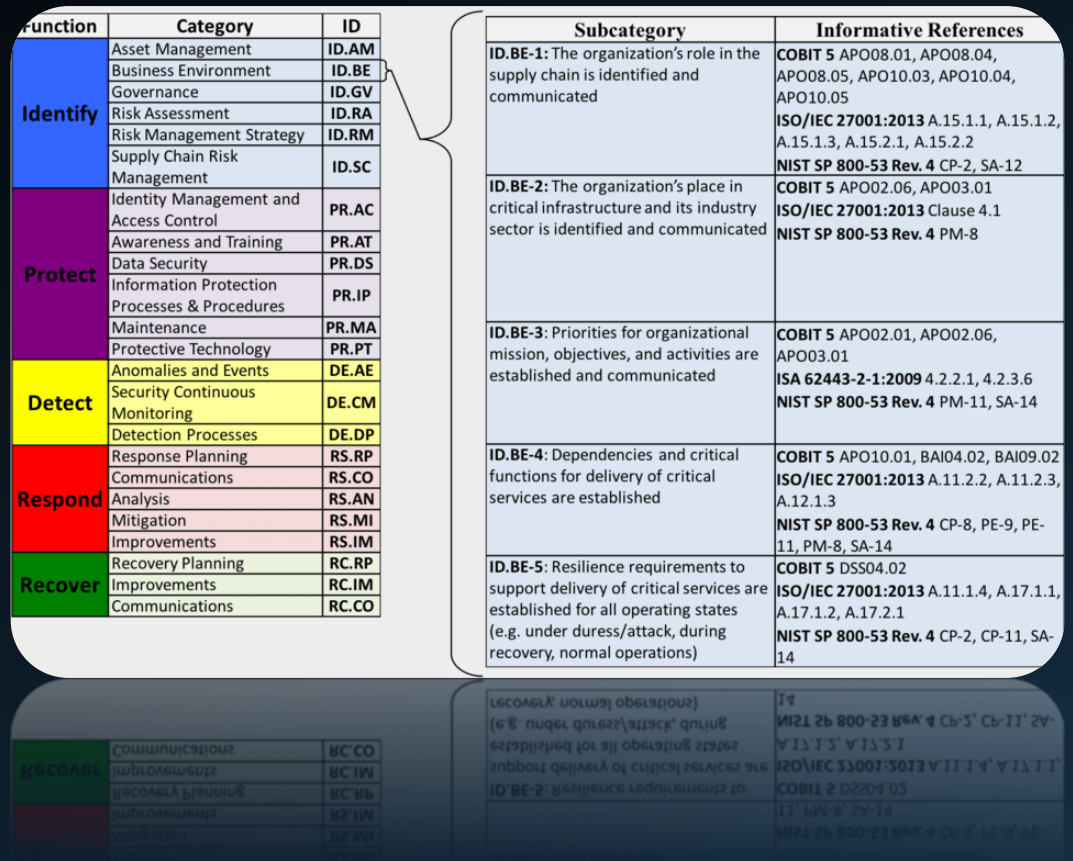
# RUNNING FAIR ANALYSIS of NIST 800-53 AGAINST A THREAT COMMUNITY






RiskLens®

# QUANTIFICATION BY MAJOR CONTROL FAMILIES



| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| | Supply Chain Risk Management | ID.SC |
| Protect | Identity Management and Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2<br>**NIST SP 800-53 Rev. 4** CP-2, SA-12 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | **COBIT 5** APO02.06, APO03.01<br>**ISO/IEC 27001:2013** Clause 4.1<br>**NIST SP 800-53 Rev. 4** PM-8 |
| **ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated | **COBIT 5** APO02.01, APO02.06, APO03.01<br>**ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6<br>**NIST SP 800-53 Rev. 4** PM-11, SA-14 |
| **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | **COBIT 5** APO10.01, BAI04.02, BAI09.02<br>**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>**NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5**: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | **COBIT 5** DSS04.02<br>**ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>**NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14 |

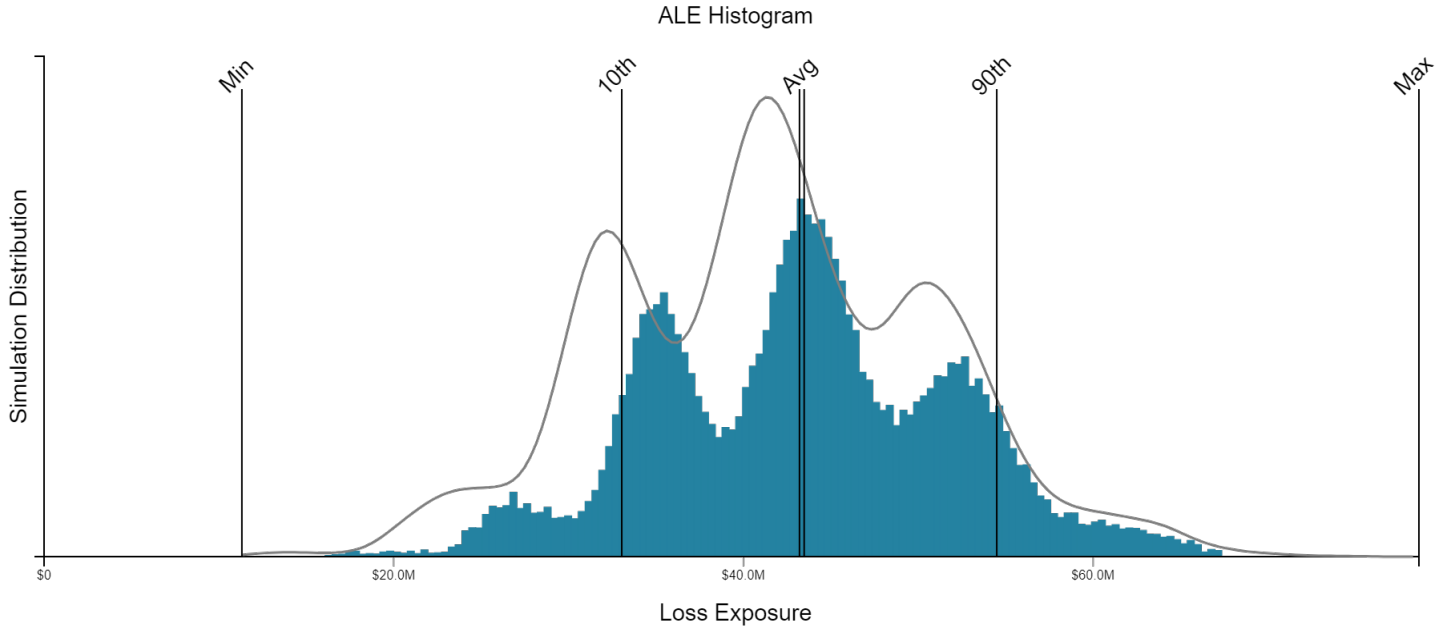
- Consider working at Control Family first
- Measure based on variance, not necessarily discrete values
- Recognize the threat scenarios core to the business
- Cover all Loss categories




RiskLens®

# REAL WORLD ANALYSIS – BASELINING

| 10th Percentile | | Most Likely | | 90th Percentile |
|---|---|---|---|---|
| $33.0M | | $43.2M | | $54.5M |
| Min $11.3M | | Average $43.5M | | Max $78.6M |

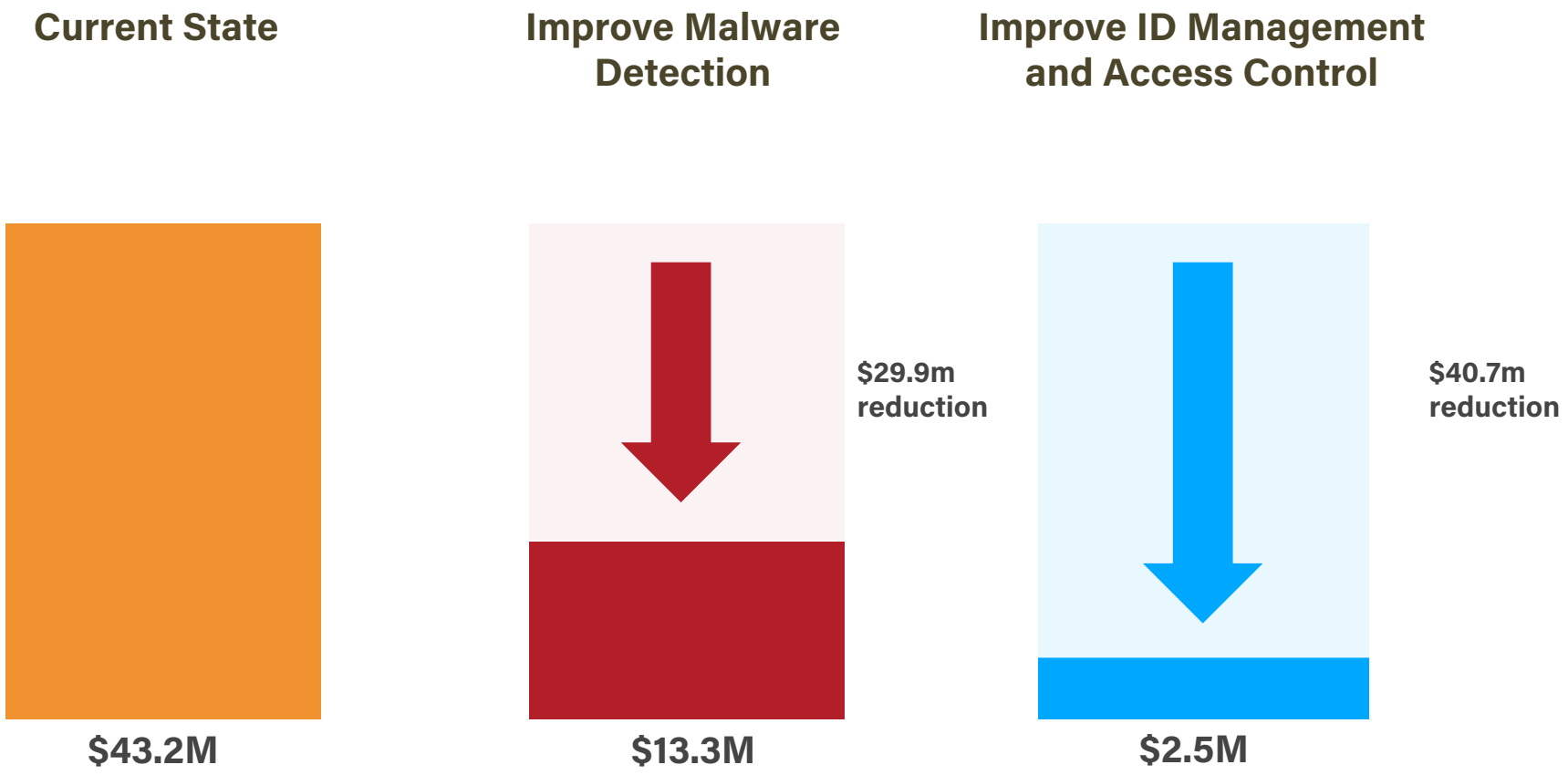



Baseline FAIR Analysis for Ransomware Attack



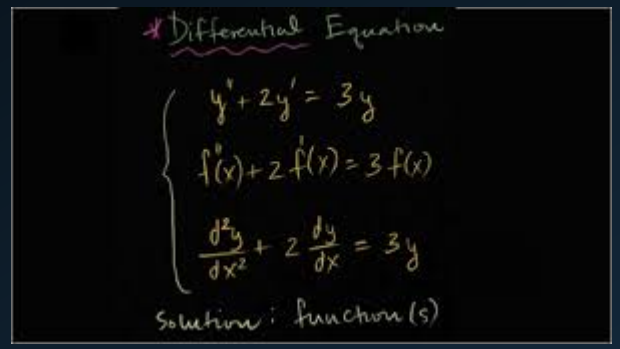

RiskLens®

# REAL WORLD ANALYSIS – RISK REDUCTION COMPARISONS



# THINGS TO AVOID LIKE THE PLAGUE

Rabbit Holes




Complex Math Calculations


Unmeasured Controls

# PATHWAY TO COMBINING NIST-CSF AND FAIR

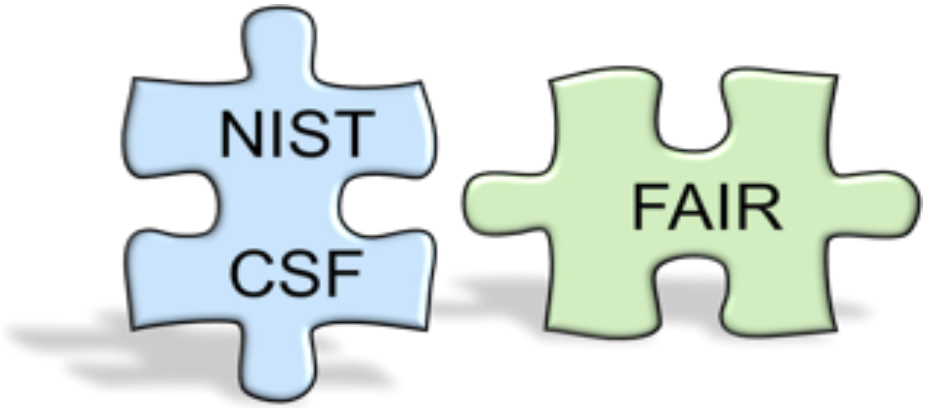



RiskLens®

# DEEP INTO NIST-CSF?

1. Put on the 'air brakes' and immediately move to quantifying **TOP RISKS**
2. Blanket investments in people, process and technology across **ALL** maturity categories **IS NOT** addressing risk reduction
3. Identify and **QUANTIFY TOP RISKS** – including current activity maturity level corresponding to NIST-CSF
4. Use this current state assessment to run what-if? Scenarios. What does an increase in actitivty maturity buy me?
5. You'll now be focused on maturity improvements against **TOP RISKS** – prioritizing investments where the business needs it most

**"If it doesn't tie into reduction of your top risks – it shouldn't be today's priority…"**



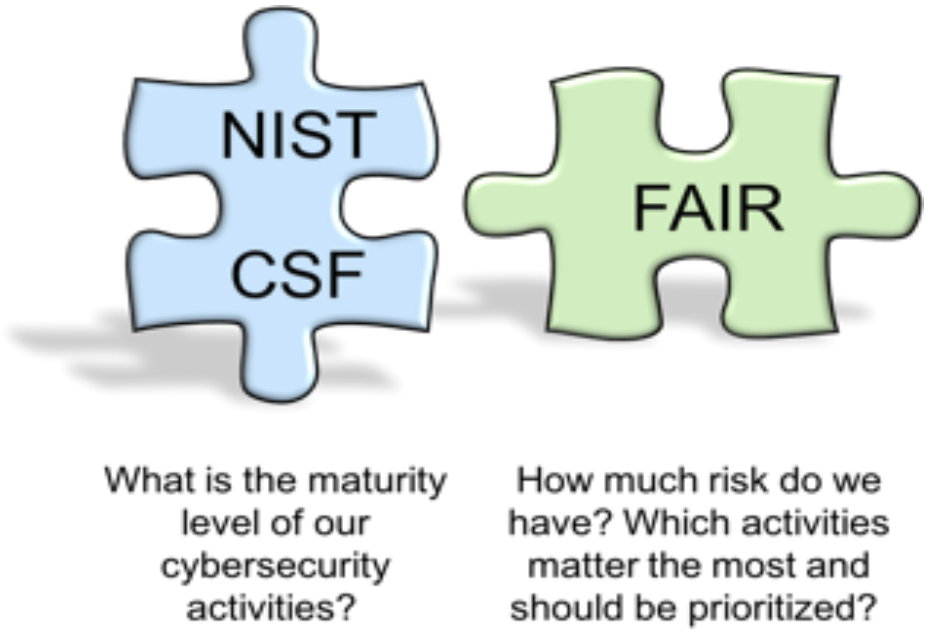




RiskLens®

# ALREADY DOING FAIR?

**“If it doesn’t tie into reduction of your top risks – it shouldn’t be today’s priority…”**

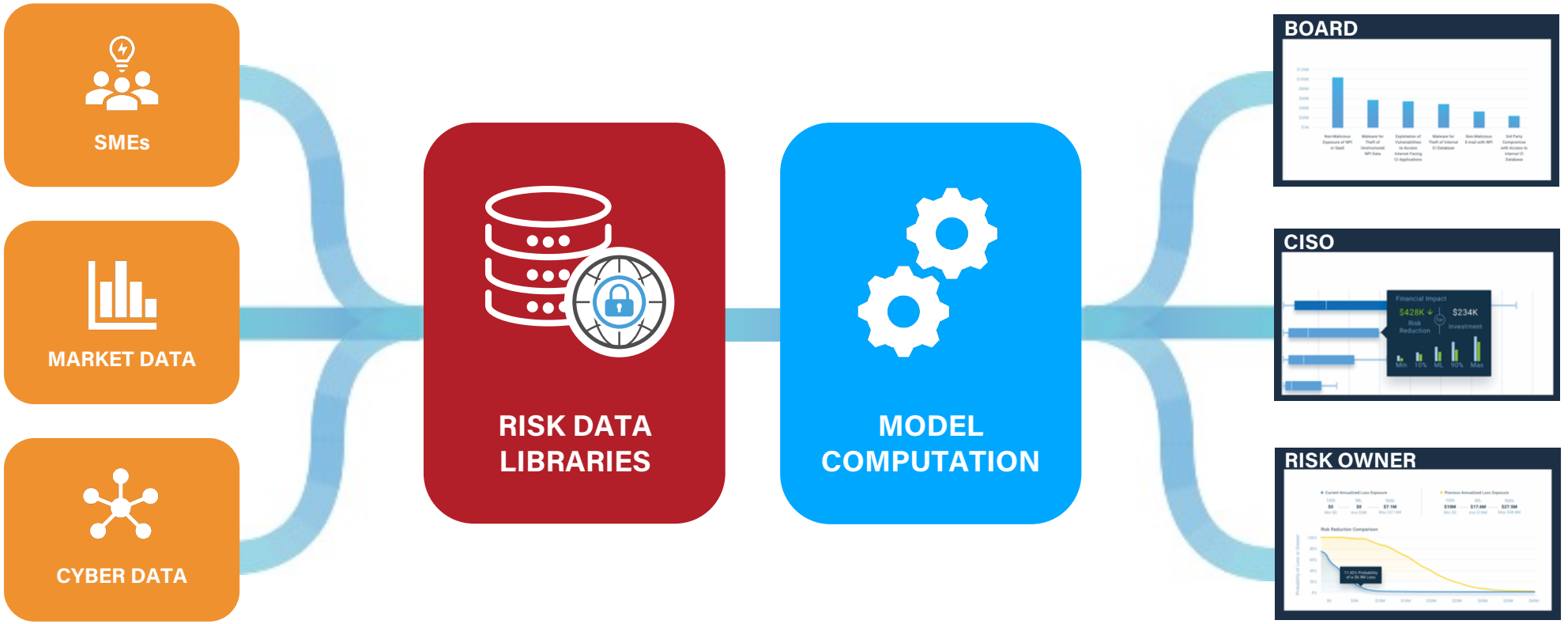



1. **TOP RISKS** are likely already quantified – if not, they should be as your very next project
2. Apply what you know about activity maturity level corresponding to NIST-CSF to your TOP RISK scenarios
3. Use this current state assessment to run what-if? scenarios. What does an increase in activity maturity buy me?
4. You’ll now be focused on maturity improvements against **TOP RISKS** – prioritizing investments where the business needs it most




RiskLens®

# RISKLENS PLATFORM: PURPOSE BUILT ON FAIR





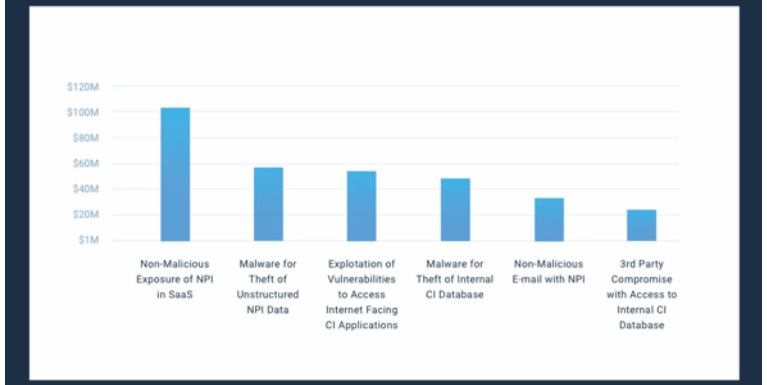


RiskLens®

# DRIVE BETTER COMMUNICATION & DECISION MAKING

## HOW MUCH RISK DO WE HAVE?

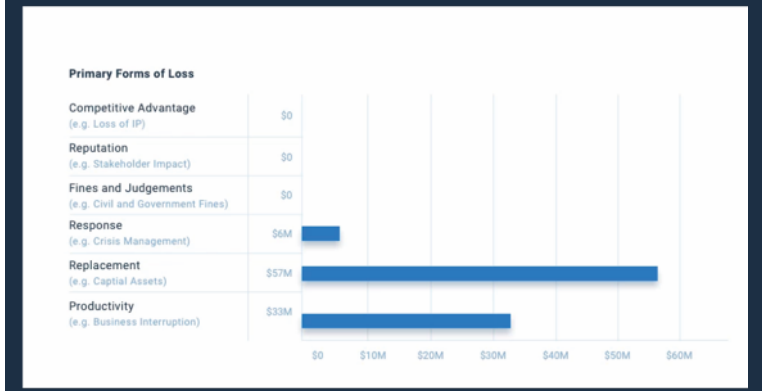

## WHAT ARE OUR TOP RISKS?




## HOW IS RISK TRENDING VS APPETITE?


## HAVE WE REDUCED RISK?


## WHAT TYPES OF LOSS CAN WE EXPECT?




## WHAT IS THE COST-BENEFIT OF THIS PROJECT?





RiskLens®

# CYBER RISK ECONOMICS IS HERE




RiskLens®