Cyber Risk Quantificaiton
for insurance and underwriting transactions

FOCAL POINT
DATA RISK

Proprietary & Confidential

For Discussion Purposes Only

What Makes Focal Point Different

SKILLS YOU NEED

A unique combination of capabilities allows Focal Point to solve the biggest and most complex challenges facing your organization, without requiring a web of different vendors.

DATA IN OUR DNA

Our focus on the data helps you look at your business from a new vantage point – so you can understand your risks in a way not otherwise possible.

DELIVERABLES WITH INSIGHT

We skip the jargon and get to the point. We deliver actionable insights, prioritized recommendations, and practical strategies for achieving your business goals.

FOCAL POINT
DATA RISK

About Focal Point

WHAT WE DO

We measure, improve, and manage your risks - protecting your most important assets and helping you achieve your business goals.

HOW WE DO IT

Top experts from the most in-demand fields are embedded into each engagement and build deliverables that have a meaningful impact on your business.

WHO USES FOCAL POINT

Many of the most innovative organizations in the world, including 5 of the 10 largest companies in the U.S., rely on Focal Point to manage their key risks.

CORE SERVICE AREAS

- Enterprise risk management
- Cybersecurity
- Identity governance
- Data privacy
- Project advisory
- Workforce development
- Data analytics
- Internal and IT audit

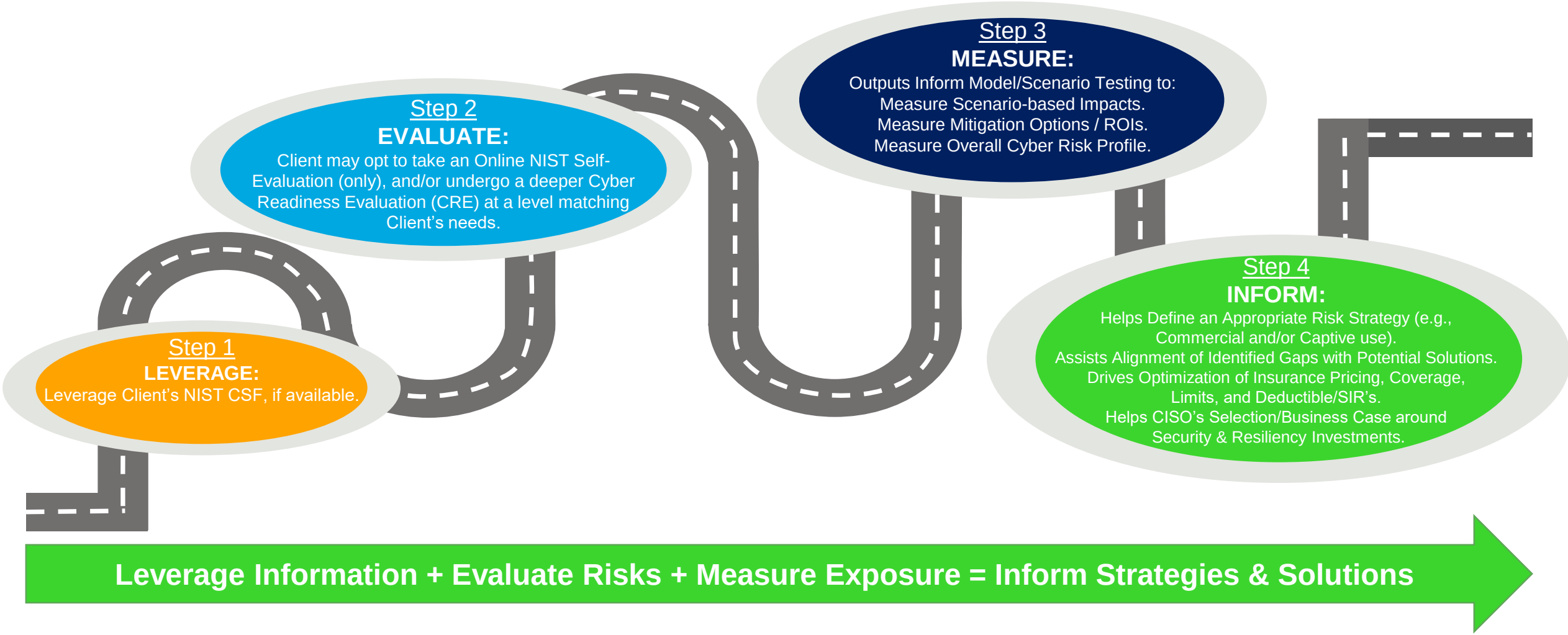
FOCAL POINT
DATA RISK

Cyber Risk Measurement Roadmap

FOCAL POINT

DATA RISK

Roadmap To Cyber Risk Measurement: Improving Insurance Strategy and Purchasing Decision Making



Leverage Information + Evaluate Risks + Measure Exposure = Inform Strategies & Solutions

FOCAL POINT DATA RISK

Step 1:

Leverage Current NIST CSF Scores

FOCAL POINT

DATA RISK

Basis for starting point risk model analysis: The NIST Cybersecurity Framework (NIST CSF)

The National Institute Of Standards & Technology (NIST) Cybersecurity Framework (CSF), or NIST CSF, is a risk-based framework created through collaboration between the U.S. government and private sector that frames a standardized set of cybersecurity concepts into best practices to help organizations manage cyber risks.

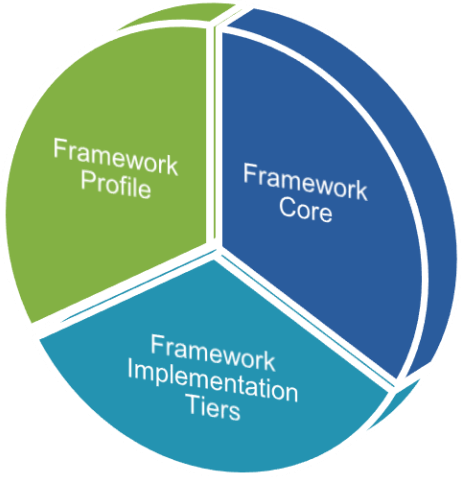
The Framework consists of three (3) parts; the Core, Implementation Tiers and the Profile.

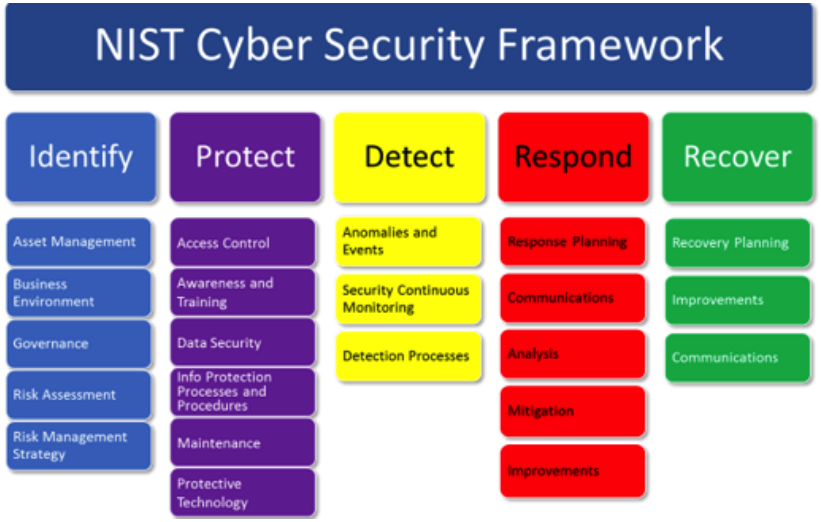
The **Framework Core** provides a set of five activities to achieve specific cybersecurity outcomes, divided into five functions: Identify, Protect, Detect, Respond, and Recover.

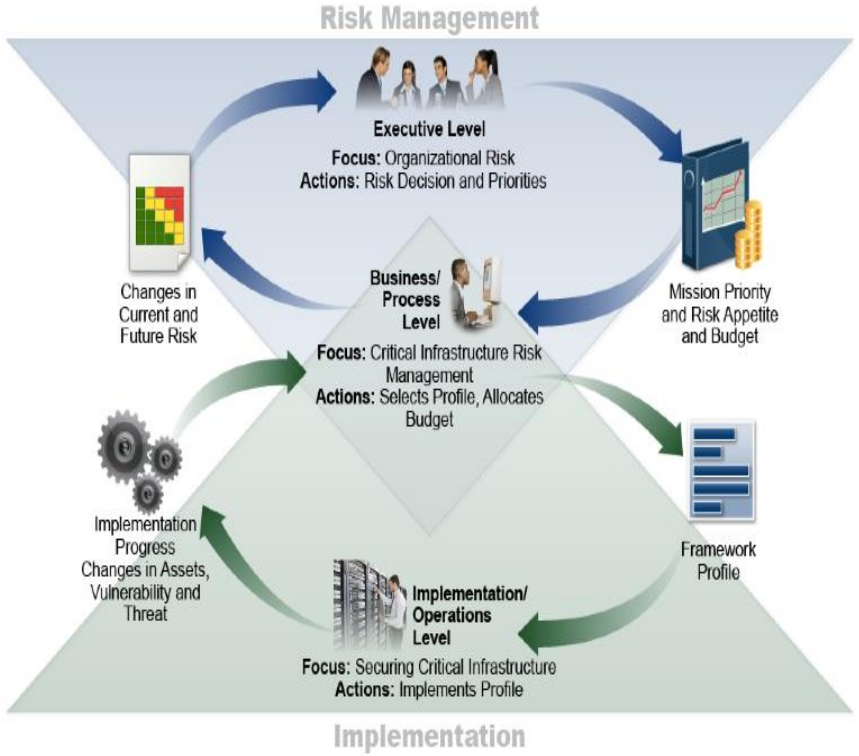
The **Implementation Tiers** provide context on how you view cybersecurity risk and your processes currently in place to manage risk.

The **Framework Profile** represents the alignment of your cybersecurity activities with business requirements, risk tolerances, and resources.

The Framework enables you to describe your current and target cybersecurity postures, identify and prioritize opportunities for improvement, and evaluate your progress toward your target state.







FOCAL POINT DATA RISK

Step 1
LEVERAGE:
Leverage Client's NIST CSF, if available.

NIST CSF:
Leverage Client Outputs – Apply An Existing NIST Cyber Evaluation (if any)

CORE	SUBCATEGORY	Risk Score
IDENTIFY	Asset Management	2.35
	Business Environment	2.15
	Governance	1.75
	Risk Assessment	1.25
	Risk Management Strategy	2.25
	IDENTIFY CORE - TOTAL SCORE	1.95
PROTECT	Access Control	1.50
	Awareness and Training	2.00
	Data Security	2.50
	Information Protection and Procedures	1.75
	Maintenance	2.75
	Protective Technology	2.50
	PROTECT CORE - TOTAL SCORE	2.17
DETECT	Anomalies and Events	2.35
	Security Continuous Monitoring	1.85
	Detection Processes	2.25
	DETECT CORE - TOTAL SCORE	2.15
RESPOND	Response Planning	1.75
	Communications	2.50
	Analysis	2.85
	Mitigation	1.25
	Improvements	1.75
	RESPOND CORE - TOTAL SCORE	2.02
RECOVER	Recovery Planning	1.25
	Improvements	1.25
	Communications	1.75
	RECOVER CORE - TOTAL SCORE	1.42
	GRAND TOTAL SCORE	1.94

FOCAL POINT DATA RISK

Step 2:

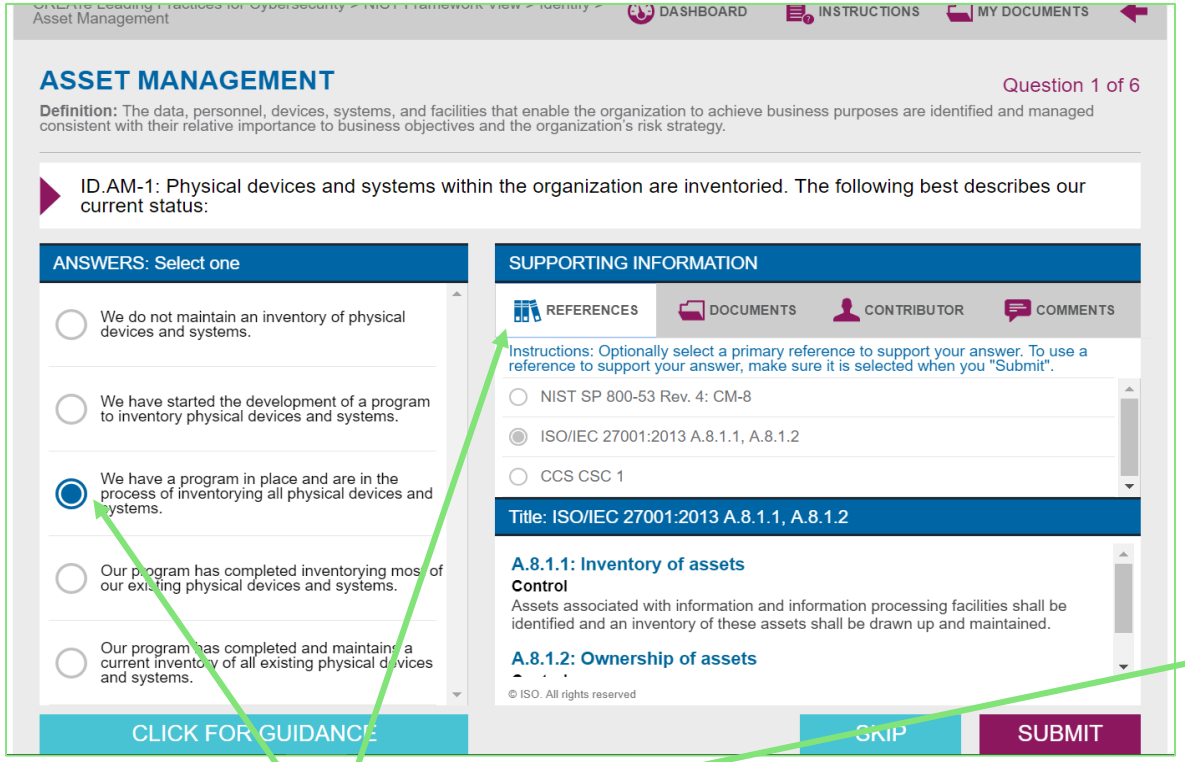
NIST CSF
Online Scoring and/or Detailed Evaluation

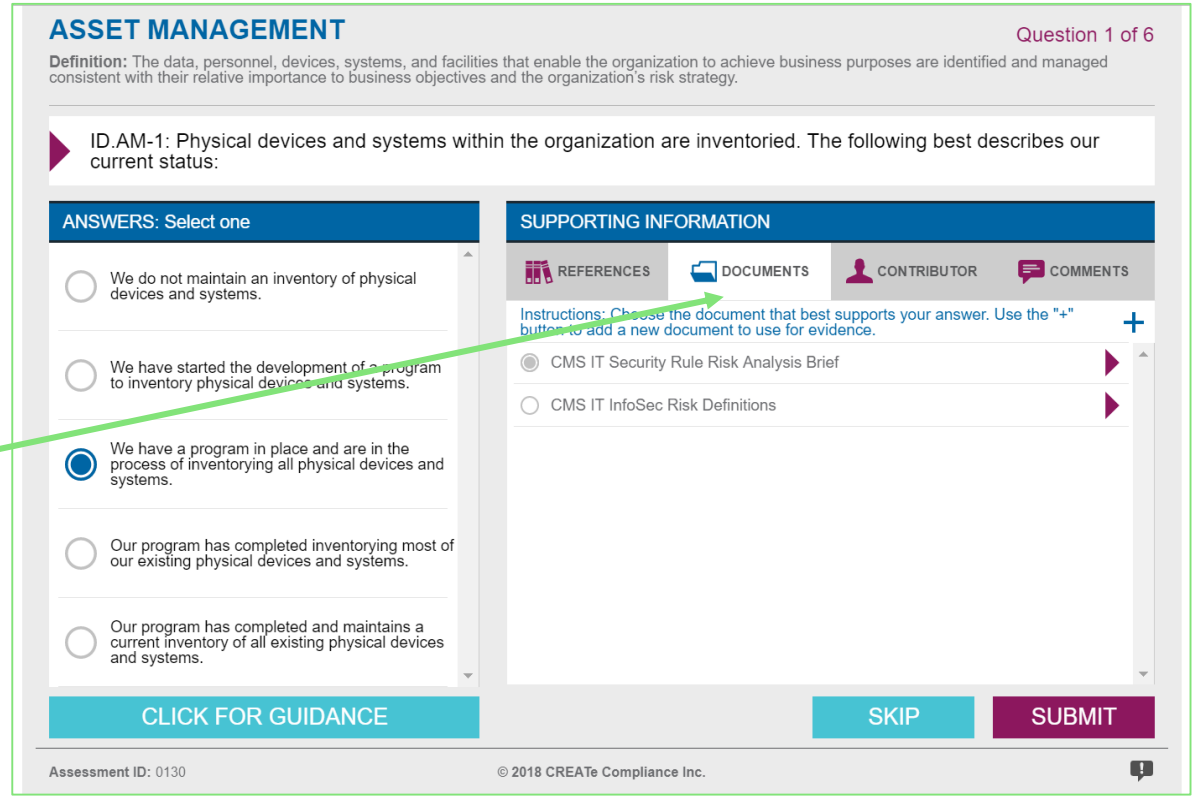
FOCAL POINT

DATA RISK

Step 2
EVALUATE:
Client may opt to take an Online NIST Self-Evaluation (only), and/or undergo a deeper Cyber Readiness Evaluation (CRE) at a level matching Client's needs.

Online NIST CSF Self-Evaluation: Easy Answer/Framework Selection and Document Referencing





Samples

FOCAL POINT DATA RISK

Online NIST CSF Self-Evaluation: Sample Scoring Outputs

Step 2
EVALUATE:
Client may opt to take an Online NIST Self-Evaluation (only), and/or undergo a deeper Cyber Readiness Evaluation (CRE) at a level matching Client's needs.

Summary Scoring & Benchmarking Results

Scoring Summary

Target Score: 2.6 Self-Assessment: 3.3 Independent Evaluation:

FUNCTION / CATEGORY	TARGET SCORE	SELF-ASSESS.	BENCH-MARK	IND. EVALUATION	BENCH-MARK
Identify	**2.4**	**2.8**	**2.7**		
Asset Management	2.3	2.7	2.9		
Business Environment	2.0	3.7	2.6		
Governance	3.0	3.1	2.4		
Risk Assessment	2.5	3.7	3.2		
▲ Risk Management Strategy	2.3	0.9	2.3		
▲ **Protect**	**2.7**	**2.5**	**2.2**		
Access Control	2.2	2.5	1.8		
▲ Awareness and Training	2.6	2.2	2.8		
▲ Data Security	2.7	2.5	2.4		
Information Protection Processes and Procedures	2.9	3.2	2.6		
▲ Maintenance	3.5	1.6	1.1		
Protective Technology	2.0	3.0	2.6		
Detect	**2.2**	**3.0**	**3.3**		
Anomalies and Events	2.0	2.6	2.8		
Security Continuous Monitoring	2.1	3.0	3.6		
Detection Processes	2.6	3.4	3.6		
Respond	**3.0**	**4.3**	**3.2**		
Response Planning	2.0	5.0	5.0		
Communications	2.2	4.0	3.0		
Analysis	3.3	3.7	1.6		
Mitigation	3.3	4.0	2.3		
Improvements	4.0	5.0	4.0		
Recover	**2.8**	**4.1**	**2.2**		
Recovery Planning	3.0	5.0	3.0		
Improvements	2.5	5.0	1.0		
▲ Communications	3.0	2.3	2.7		

Comparative Scoring Analysis

Scoring Summary / Comparative Chart

Target Score: 2.6 Self-Assessment: 3.3 Independent Evaluation:

Detailed Scoring Results (optional)

Identify
Target: 2.4 Self-Assessment: 2.8 Independent Evaluation:

Asset Management
Target: 2.3 Self Assessment: 2.7 Independent Evaluation: Deviation +/-: 1.5

ID.AM-1 Physical devices and systems within the organization are inventoried. The following best describes our current status:

SA	IE	Minimum: 1.0 | Self Assessment: 3.0 | Target: 2.0 | Independent Evaluation:
		We do not maintain an inventory of physical devices and systems.
		We have started the development of a program to inventory physical devices and systems.
◉		We have a program in place and are in the process of inventorying all physical devices and systems.
		Our program has completed inventorying most of our existing physical devices and systems.
		Our program has completed and maintains a current inventory of all existing physical devices and systems.

PRIMARY REFERENCE: ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
CONTRIBUTOR: Doug Richter
RELATED DOCUMENT: CMS IT Security Rule Risk Analysis Brief

ID.AM-2 Software platforms and applications within the organization are inventoried. The following best describes our current status:

SA	IE	Minimum: 1.0 | Self Assessment: 4.0 | Target: 2.0 | Independent Evaluation:
		We do not maintain an inventory of software platforms or applications.
		We have started the development of a program to inventory software platforms and applications.
		We have a program in place and are in the process of inventorying all software platforms and applications.
◉		Our program has completed inventorying most of our software platforms and applications.
		Our program has completed and maintains a current inventory of all existing software platforms and applications.

PRIMARY REFERENCE: ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
CONTRIBUTOR:
RELATED DOCUMENT:

Key: SA = Self Assessment | **IE** = Independent Evaluation | **TRG** = Target Score | **MIN** = Minimum Score
Code: = Target Not Achieved or Below Min | = Outside Standard Deviation | = Comment | = Skip Logic

Samples

Current and Target Risk Comparison

FOCAL POINT DATA RISK

Cyber Readiness Evaluation (CRE) Components: A Deeper Analysis To Inform More Robust Cyber Measurement

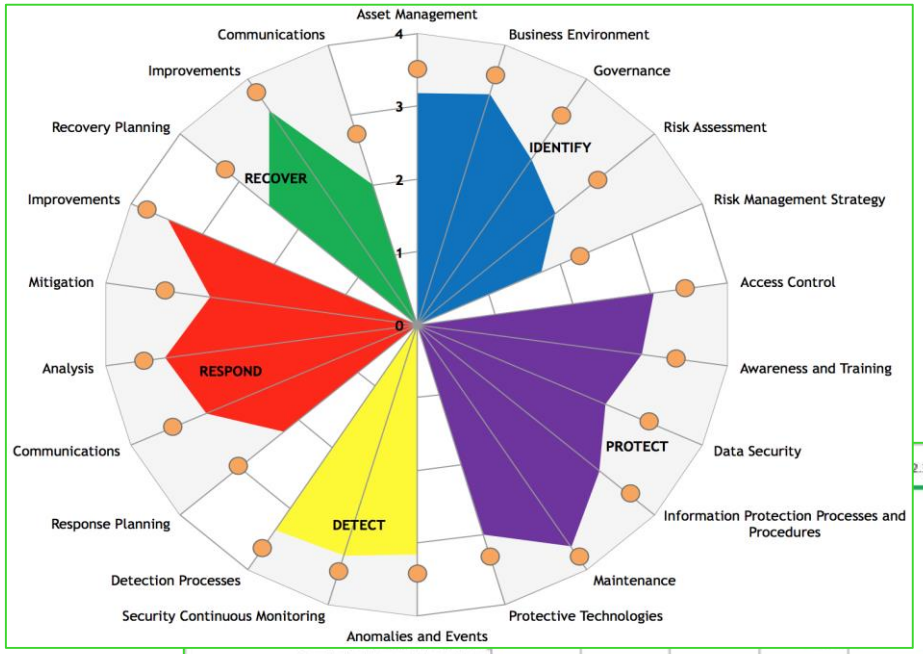
Step 2
EVALUATE:
Client may opt to take an Online NIST Self-Evaluation (only), and/or undergo a deeper Cyber Readiness Evaluation (CRE) at a level matching Client's needs.

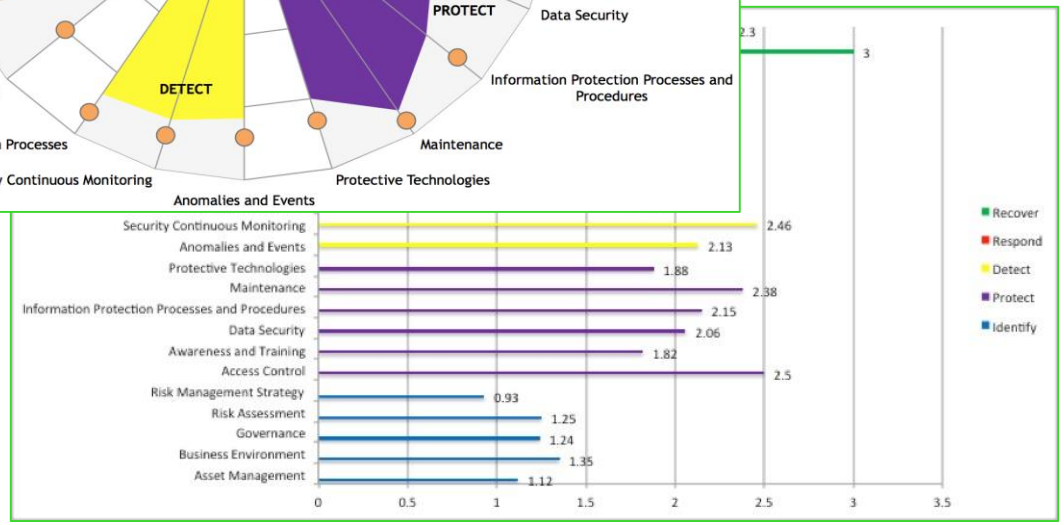
NIST CSF Evaluation	• Evaluate and score current state of cybersecurity framework using NIST standards, mapped to the NIST Cybersecurity Framework (CSF).
Cyber Vulnerability Evaluation	• Identify existing vulnerabilities (people, process, technology) that could be exploited by malicious actors.
Cyber Compromise Evaluation	• Identify current or historical compromise of information/data through analysis of system artifacts.
Cyber Threat Management Exercise	• Conduct a cyber threat simulation exercise that enables executives and staff to build practical experience responding to cyber threats.
Cyber Attack & Response (Pen Testing)	• Validate the maturity of the incident response and cyber protection controls through a targeted cyber attack.
Internal and External Threat Actor Profiling	• Review data access policies/standards and determine opportunities for internal and external threat actors to access sensitive corporate or other protected information.

Step 2
EVALUATE:
Client may opt to take an Online NIST Self-Evaluation (only), and/or undergo a deeper Cyber Readiness Evaluation (CRE) at a level matching Client's needs.

Cyber Readiness Evaluation (CRE) Sample Deliverables: A Deeper Analysis To Inform More Robust Cyber Measurement

Current And Target State Positions





Sample Written Recommendations

Finding 8

Network Access Control (NAC) is inconsi
NAC solution provides coverage to on
computing devices are located. Additional
fail in an open status when the back-end ca
that this fail-open configuration ensures
approved existing connections but also
presence without the prerequisite health ch

Gap A

Finding ID	Impact	
MED-001	Broad	

Remedi

E

Recom

Network Access Control should be deploye
- This coverage should extend to all
- This coverage should extend to all

Network Access Control should be configu
a closed state preventing de-facto approval
the unavailable system. recognizes th
recognizes the attack vector that unapprove

Externa

HiTrust v8:
01.m, 01.n, 01.o, 01.w, 09.m, 09.u, 09.v, 09.w, 09.x, 09.y, 09.z, 10.b, 10.c, 10.d, 10.f 10.g, 10.i

Finding 24

The process and established roles and responsibilities for ensuring that the root cause of an incident and associated remediation steps are not adequately extrapolated across the enterprise to like systems, applications, networks, and databases to proactively remediate similar risks needs improvement. Once an incident has been remediated and the root cause documented, there is no process in place to evaluate the rest of the enterprise for similar risks, vulnerabilities, open policy exceptions, or insecure processes and practices. During review of sample incidents, the root cause of an incident was a one-off process with poor quality assurance checking. Interviews with the incident response team indicated that there was no effort made to seek out any similar one-off processes across the enterprise to proactively improve the quality assurance processes in the same manner the process specific to the incident was remediated.

Gap Assessment

Finding ID	Impact	Priority	CSF Function
LOW-002	Broad	Low	ID.RA-4, RS.AN-2

Remediation Effort

Extensive

Recommendation

Develop a process and document responsibility for applying the lessons learned from any security or privacy incident across the enterprise. The process should include:
- Seeking out like systems, applications, networks, and databases that may be susceptible to the same vulnerability or risk
- Searching the Risk Review and Risk Register records for similar policy exceptions and unmediated instances of non-compliance which share the same vulnerabilities or risks and reevaluating their risk ratings and remediation time frames
- Identifying similar processes or practices across the enterprise which may suffer from the same vulnerabilities and risks
- Creating and driving remediation of those vulnerabilities or risks everywhere it is discovered

External References

HiTrust v8:	COBIT v5:
03.b, 03.d, 07.d, 10.k, 10.m, 11.d, 11.e, 12.b	DSS04.02

FOCAL POINT DATA RISK

Step 3: Measurement

FOCAL POINT

DATA RISK

Use An Organized NIST CST Risk Taxonomy: Leveraging NIST Framework/Outputs For Model Preparation

CORE	SUBCATEGORY	Risk Score
IDENTIFY	Asset Management	2.35
	Business Environment	2.15
	Governance	1.75
	Risk Assessment	1.25
	Risk Management Strategy	2.25
	IDENTIFY CORE - TOTAL SCORE	1.95
PROTECT	Access Control	1.50
	Awareness and Training	2.00
	Data Security	2.50
	Information Protection and Procedures	1.75
	Maintenance	2.75
	Protective Technology	2.50
	PROTECT CORE - TOTAL SCORE	2.17
DETECT	Anomalies and Events	2.35
	Security Continuous Monitoring	1.85
	Detection Processes	2.25
	DETECT CORE - TOTAL SCORE	2.15
RESPOND	Response Planning	1.75
	Communications	2.50
	Analysis	2.85
	Mitigation	1.25
	Improvements	1.75
	RESPOND CORE - TOTAL SCORE	2.02
RECOVER	Recovery Planning	1.25
	Improvements	1.25
	Communications	1.75
	RECOVER CORE - TOTAL SCORE	1.42
	GRAND TOTAL SCORE	1.94

Framework Implementation Tiers

Scoring and Gap Prioritization

Tier 1 – Partial: cybersecurity risk management practices are either not formulated or are ad-hoc

Tier 2 – Risk Informed: cybersecurity risk management practices are not organization-wide

Tier 3 – Repeatable: there is an organization-wide management of cybersecurity risk

Tier 4 – Adaptive: cybersecurity risk management is part of the organizational culture

FOCAL POINT DATA RISK

Monte Carlo Simulation Overview: What Is It And Why We Use It

Modeling a real system to learn about its behavior

Building a set of mathematical and logical relationships

Establishing and varying conditions to test different scenarios

Providing a helpful solution when you do not have historical loss data

FOCAL POINT DATA RISK

Monte Carlo Outputs: Understanding The Monte Carlo Simulation Process

Random Number Generation

- Simulates the uncertainty in the assumptions
- The program selects a value for the assumption, recalculates the spreadsheet, plots the forecast and repeats

Application of Model

- We build frequency and severity distributions for each selected Cyber Risk Factor (e.g., Access Control, Protective Technology, etc.)
- We perform up to 50,000 year loss simulations and apply it to selected Cyber Risk Factors
- The model simulates different loss outcomes and applied correlation and aggregate views to link results
- This then provides an overall loss distribution along with a view of the associated variability around mean estimate (average) calculations

Develop Key Modeling Assumptions: Samples

Derivation of Assumptions:

- **Used the scores from the Cyber Risk Evaluation to estimate ABC's frequency scores.**
- **Used ABC's revenue numbers and general industry patterns to estimate ABC's severity scores.**
- **Used offsets from ABC's frequencies and severities to estimate XYZ's frequencies and severities.**

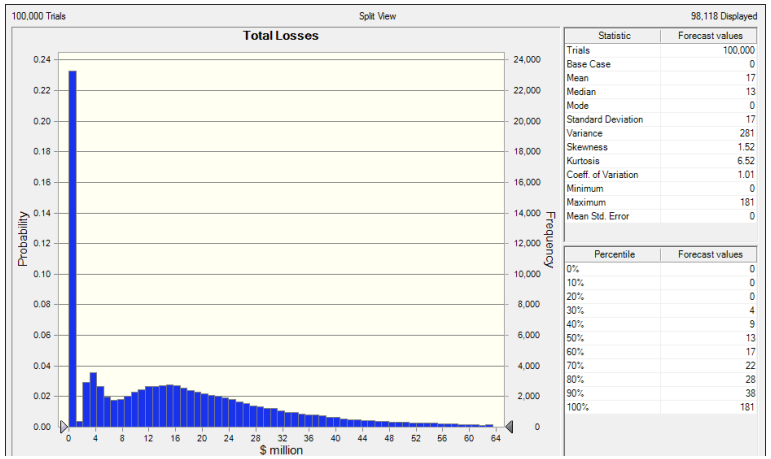
Key Assumptions:

- **The frequencies of each of the cyber risks range between a 6 and a 10 (between 3% and 50%).**
- **The severities of each of the cyber risks follows profiles which are common in the industry.**
- **The average severity loss among the cyber risks is around $17 million: a significant part of ABC's revenue is from conferences.**
- **XYZ's risks are mostly around 1/2 as severe as ABC's, since despite small revenue, its liabilities will grow rapidly given the new cloud exposure.**

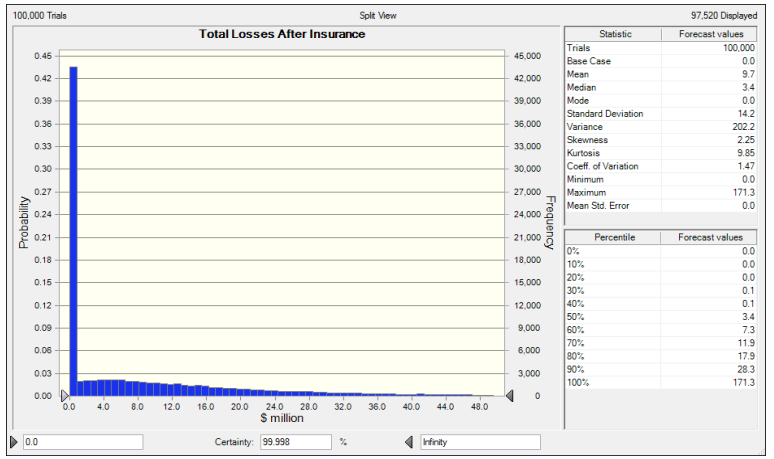
Step 3
MEASURE:
Outputs Inform Model/Scenario Testing to:
Measure Scenario-based Impacts.
Measure Mitigation Options / ROIs.
Measure Overall Cyber Risk Profile.

Conduct Simulated Cyber Loss Scenarios: Inform Your Cyber Risk Profile And Optimize Your Risk Strategies

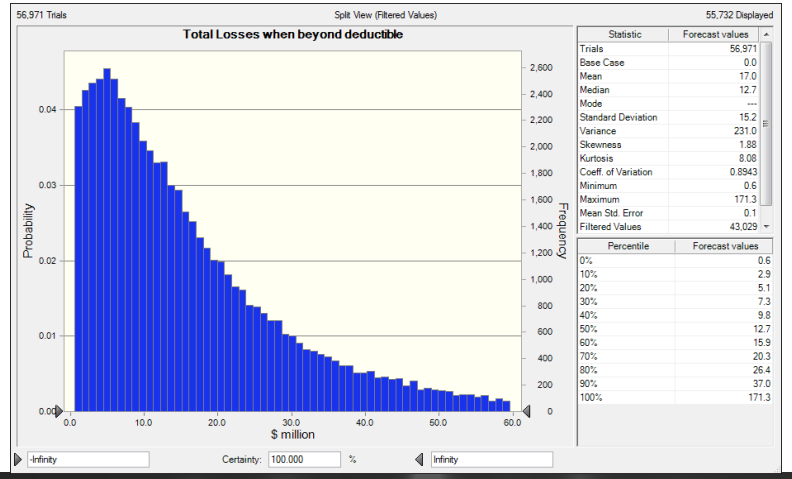
Total potential losses with no insurance



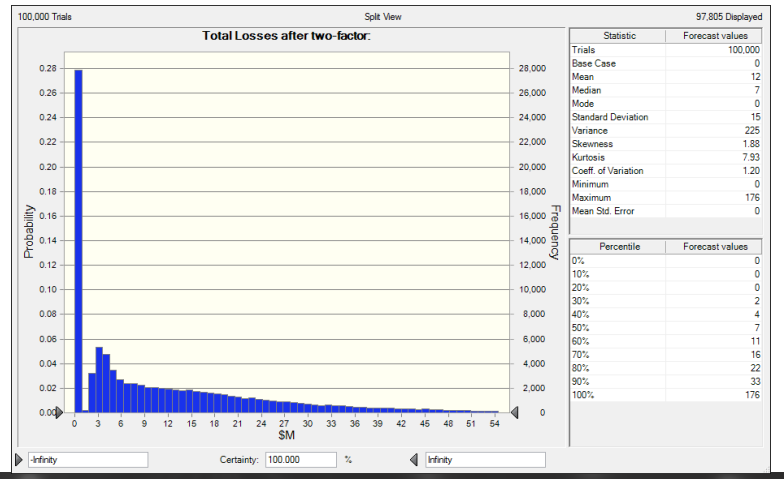
Total potential losses after insurance



Total potential losses beyond $50k deductible



Total potential losses using two-factor authentication

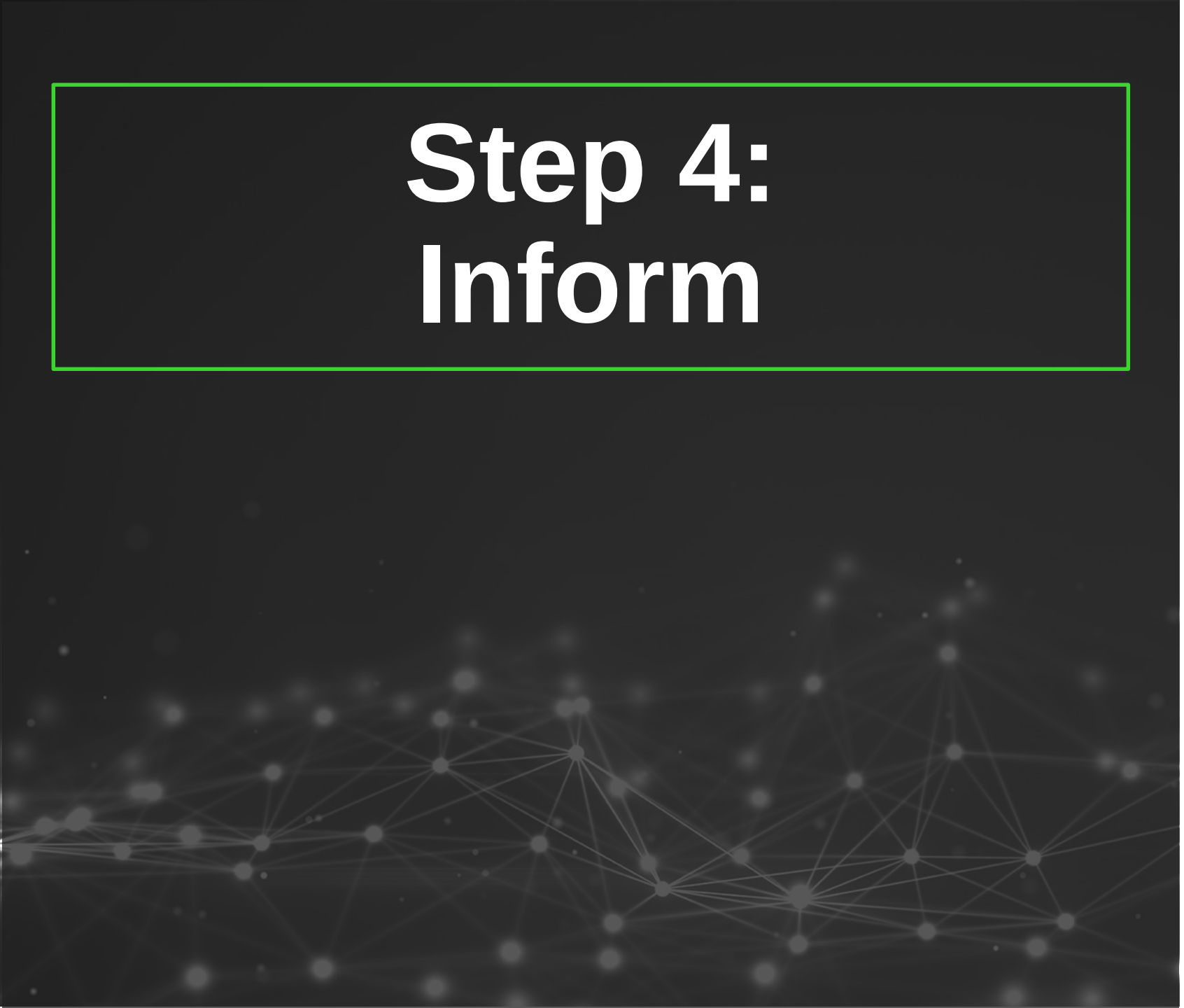


See Appendix For Larger Views

Example

FOCAL POINT DATA RISK

Step 4: Inform



FOCAL POINT

DATA RISK

Final Results Summarized: Informing Strategies And Solutions

What you asked us to do?	How did we proceed?
Focus on the security and privacy exposures of ABC, especially in the light of the first year of XYZ's development and operations	Applied the NIST CSF and scored your cyber risk profile. We reviewed policies, networks, systems, vendors, and interviewed ABC and XYZ management
	We identified and quantified cyber vulnerabilities and calculated potential losses based on the NIST framework
Provide specific recommendations on insurance coverage structure, terms and conditions, and policy wording where appropriate	We developed operational and cyber insurance coverage recommendations using the cyber loss profile results and coordinated with insurance broker to position account for a more strategic insurance placement

What did we find?

1. There is over a 70% chance of a cyber loss
2. With the current $10 m limit, there is a 10% chance of a cyber loss exceeding $38 m including $50k deductible
3. A breach could reduce (or eliminate) future revenue or enrolment due to direct or consequential reputational impacts

What do we recommend?

1. Adopt two-factor authentication to cut likelihood of breach and help lessen reputational impacts of a breach
2. Maintain current deductible, if possible, and increase the limit to $15 m to reduce average losses from $9.8 m to $7.3 m, using a $50 k deductible
3. Improve insurance policy features through alignment with the NIST CSF framework

Example

FOCAL POINT DATA RISK

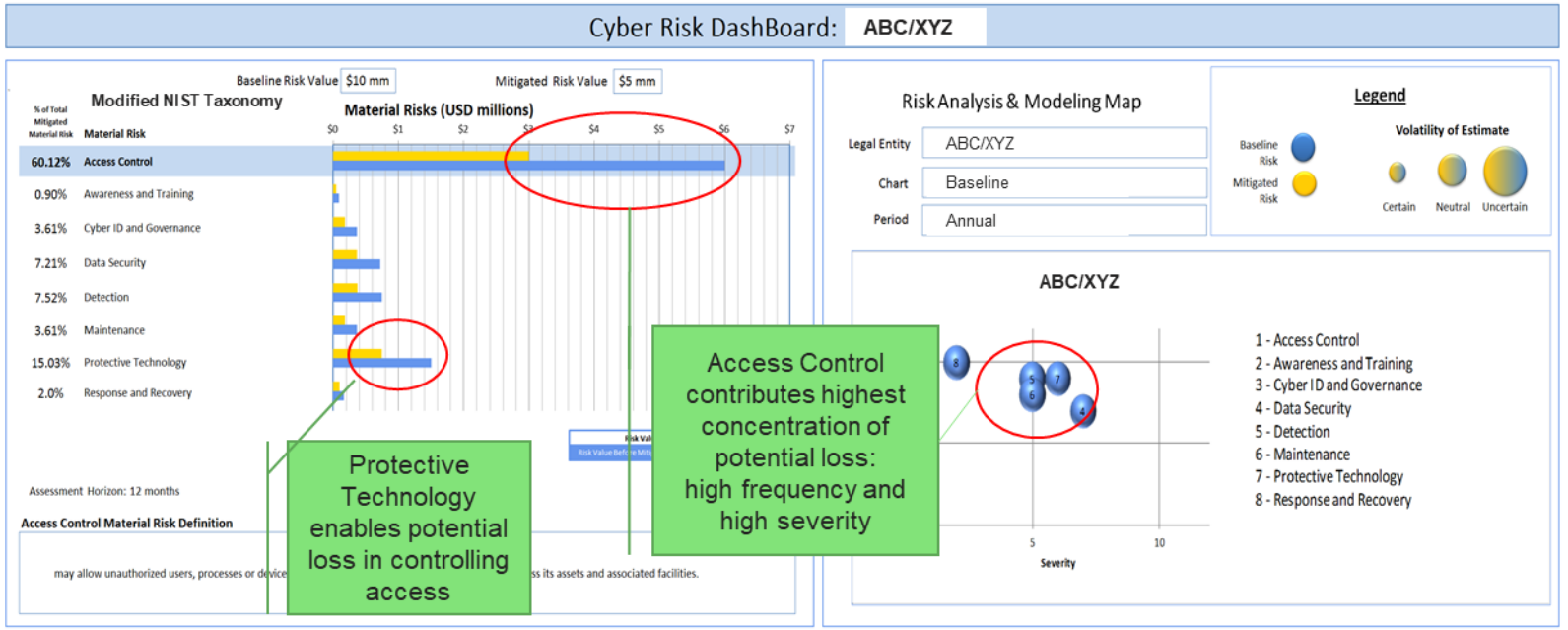
Baseline Risk Measurement:

High concentrations of potential loss in controlling access with protective technology

- **Issue**: How to evaluate Baseline cyber risk exposure without insurance and operational mitigation?

- **Approach**:
  - Use NIST taxonomy to drive review
  - Use risk experts to test and score likelihood and impact of potential cyber risk events associated with each NIST risk driver

- **Findings**: 10% chance of loss greater than $38 million with average losses around $17 million
  1. Over 70% chance that a cyber loss could occur
  2. Loss concentrated around Access Control and Protective Technology: both high frequency and high severity
  3. Either could exceed current insurance limit levels



Example

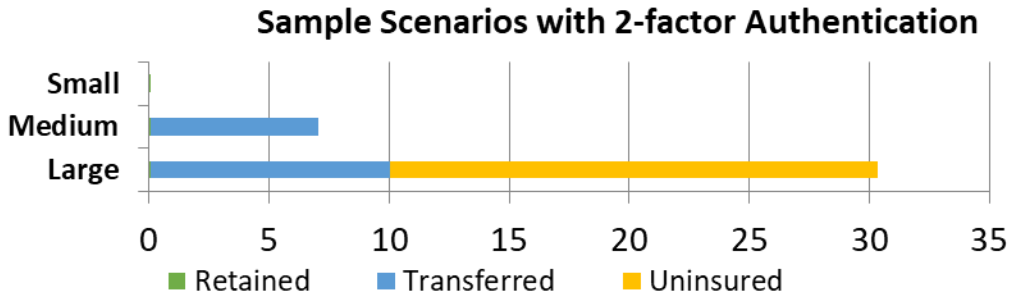
FOCAL POINT DATA RISK

Baseline Risk Measurement: Understanding Operational Risk Impacts and Reduction

Operations	Average Results						
	Unlimited loss (no insurance scenario)		Retained loss (first $.05 M)		Transferred loss (next $10.00 M)		Uninsured loss (beyond $10.05 M)
Before 2-factor	16.54 M	=	0.04 M	+	6.71 M	+	9.79 M
After 2-factor	12.46 M	=	0.04 M	+	5.66 M	+	6.77 M

- Averaging events and non-events, your expected deductible loss is less than the $50 k max
- Averaging events and non-events, the expected insurance payment is less than the $10 M max
- Some events may be so large that most of your expected losses will **not** be covered by insurance

- At right are three sample scenarios.
- Losses come in different sizes, and trigger different amounts of coverage.
- The average of the three sample scenarios gives the result at the top.



Example

FOCAL POINT DATA RISK

How Can You Respond To Cyber Risk?
Recommendation (1 of 3):
Invest In 2FA To Help Reduce A Chance Of A Breach

- **Issue**: How do we evaluate an emergent and insurgent risk and understand *operational* mitigations?

- **Approach:**
  - Use NIST taxonomy to drive comprehensive review
  - Simulate the range of potential losses associated with each NIST risk driver
  - Apply simulation to operational mitigations

- **Insight:** 10% chance of loss greater than $38 million with average losses around $17 million, highly concentrated around Access Control and Protective Technology.

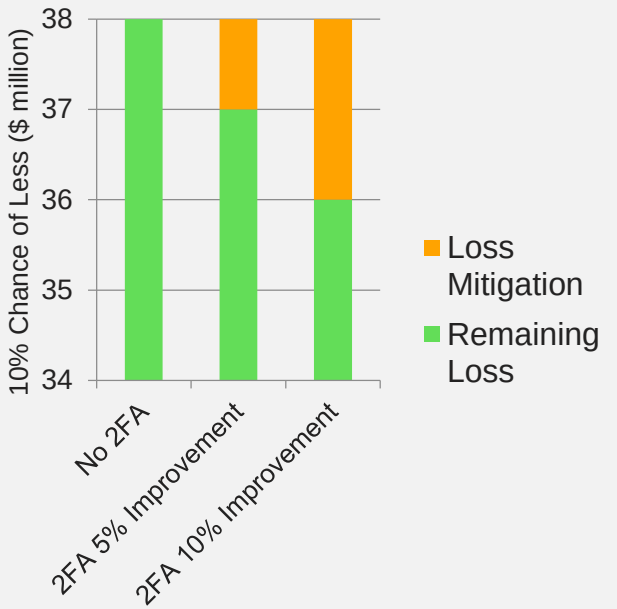
- A failure in Access Control can present a significant reputational risk to the ability to attract and maintain clients, particularly during its early years. An Access Control failure in one part of the business can have a consequential reputational impact on others.

RECOMMENDATION

- **Idea:** Operationally protect core revenues and start-up situations.

Implement Two Factor Authentication (2FA) which reduces by at least 10% the chance of loss impact, by $1 - $2 million
This may also reduce reputational impacts from a breach

2-Factor Authentication May Reduce the Losses from a Breach



Note: 2FA offers a noteworthy reduction in the attack horizon, however the attack surface (as with all networks with any kind of inter web connectivity) still remains high for other types of attacks (phishing, SQL cross-site, etc.) that are not quantifiable as a percentage with any accuracy.

Even **IF** 2FA reduced the exposure by a measurable amount a protected connection is still vulnerable if the connecting system is already infected.

Example

FOCAL POINT DATA RISK

How Can You Respond To Cyber Risk?
Recommendation (2 of 3):
Optimize Insurance Coverage Relative To Potential Cyber Losses

- **Issue**: How do we evaluate an emergent and insurgent risk and understand potential mitigations?

- **Approach**:
  - Use NIST taxonomy to drive comprehensive review
  - Simulate a range of losses for each risk driver
  - Apply simulation to *financial* mitigations

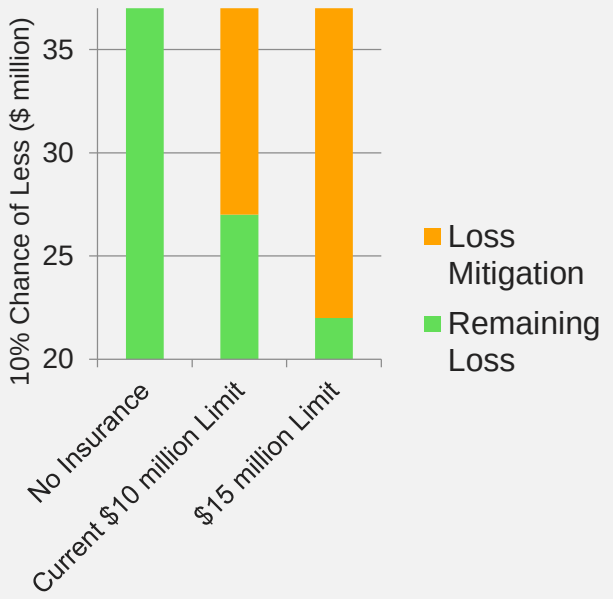
- **Insight**: 10% chance of loss greater than $38 million with average losses around $17 million

RECOMMENDATION

- **Idea**: Financially protect core revenues and new membership enrolment

Increase Cyber Insurance Policy Limit by $5 million
Reduce the estimated loss impact to $23 million
Reduce the average loss to approx. $7.3 million

Use Insurance Coverage to Reduce Potential Cyber Losses



Note: Loss Mitigation estimates include an assumption for a $50,000 insurance deductible.

Example

FOCAL POINT DATA RISK

How Can You Respond To Cyber Risk? Recommendation (3 of 3): *Improve Policy Structure*

- **Issue**: How do we manage policies to mitigate an emerging and insurgent risk like cyber?

- **Approach**:
  - Provide an in-depth policy coverage review
  - Map NIST framework to policy items
  - Discuss potential gaps with broker and determine the market's ability to customize coverage
  - Assist in preparing underwriting documents to educate markets and obtain customized solution
  - Review quotes and coverage against NIST Map when received

- **Insight**: Some NIST-based risks are not covered cleanly in many existing cyber policies (e.g., Reputational impacts)

RECOMMENDATION

- **Idea**: Design and acquire customized cyber coverage better matching to actual risk variables & controls

Working with brokers, provide underwriting markets with clear coverage requirements matching risk exposures to customize coverage to reduce risk of coverage issues in case of a claim.

Example

FOCAL POINT DATA RISK

How Can You Manage Cyber Risk? Recommendation (3 of 3): Align Your Framework To Cyber Insurance Coverages

A FAILURE IN...	WOULD LIKELY TRIGGER COVERAGE UNDER…									
	Security & Privacy Liability	Multimedia & IP Liability	Technology Services	Misc. Prof. Services	Network Interruption & Recovery	Event Support Expense	Privacy Regulatory Defense & Penalties	Network Extortion	Electronic Theft & Computer Fraud	Reputational Damage
Cyber ID and Governance	Y	No Coverage	Y	No Coverage		Y	Y			No Coverage
Access Control	Y	No Coverage	Y	No Coverage	Y	Y	Y	Y	Y	No Coverage
Awareness and Training		No Coverage		No Coverage			Y			No Coverage
Data Security	Y	No Coverage	Y	No Coverage	Y	Y	Y	Y	Y	No Coverage
Maintenance	Y	No Coverage	Y	No Coverage	Y	Y	Y			No Coverage
Protective Technology	Y	No Coverage	Y	No Coverage	Y	Y	Y	Y	Y	No Coverage
Detection	Y	No Coverage	Y	No Coverage	Y	Y	Y	Y		No Coverage
Response & Recovery		No Coverage		No Coverage		Y	Y			No Coverage

Example

FOCAL POINT DATA RISK

For Future Consideration: Updating and Extending Analysis

- Determine an acceptable risk tolerance level
- Select Operating Margin or Net Income (vs Revenue) as a basis for analysis
- Update analysis on an annual basis
- Add new inputs, looking at the effects of other operational changes
- Add new external data about different insurance coverage options available in the market

Example

FOCAL POINT DATA RISK

Appendix

FOCAL POINT

DATA RISK

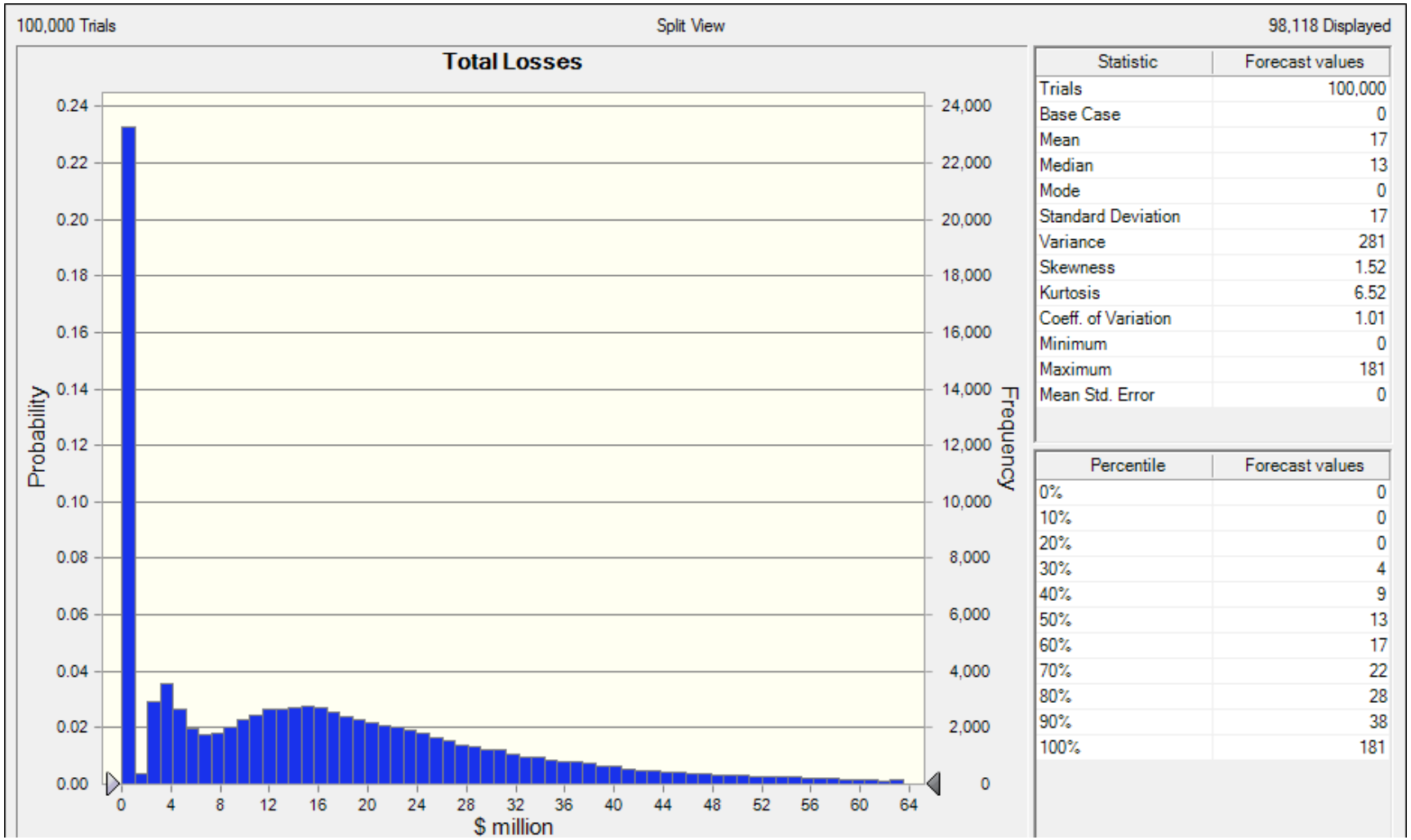
Example Views

FOCAL POINT

DATA RISK

Step 3
MEASURE:
Outputs Inform Model/Scenario Testing to:
Measure Scenario-based Impacts.
Measure Mitigation Options / ROIs.
Measure Overall Cyber Risk Profile.

Simulated Losses:
Total Potential Cyber Losses – Excluding Insurance



Statistic	Forecast values
Trials	100,000
Base Case	0
Mean	17
Median	13
Mode	0
Standard Deviation	17
Variance	281
Skewness	1.52
Kurtosis	6.52
Coeff. of Variation	1.01
Minimum	0
Maximum	181
Mean Std. Error	0

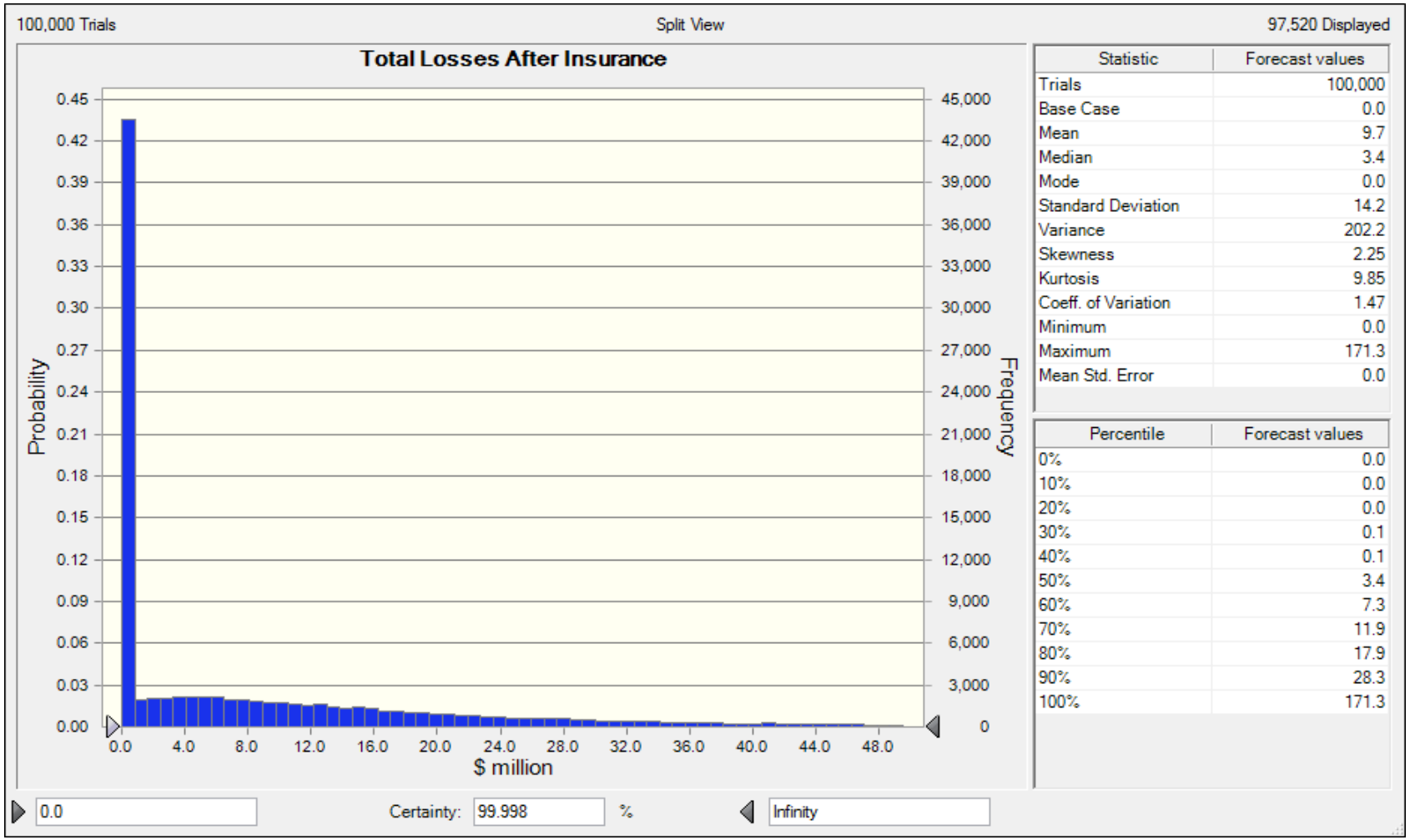
Percentile	Forecast values
0%	0
10%	0
20%	0
30%	4
40%	9
50%	13
60%	17
70%	22
80%	28
90%	38
100%	181

Example

FOCAL POINT DATA RISK

Step 3
MEASURE:
Outputs Inform Model/Scenario Testing to:
Measure Scenario-based Impacts.
Measure Mitigation Options / ROIs.
Measure Overall Cyber Risk Profile.

Simulated Losses After Insurance: Total Cyber Losses After Current Insurance



Statistic	Forecast values
Trials	100,000
Base Case	0.0
Mean	9.7
Median	3.4
Mode	0.0
Standard Deviation	14.2
Variance	202.2
Skewness	2.25
Kurtosis	9.85
Coeff. of Variation	1.47
Minimum	0.0
Maximum	171.3
Mean Std. Error	0.0

Percentile	Forecast values
0%	0.0
10%	0.0
20%	0.0
30%	0.1
40%	0.1
50%	3.4
60%	7.3
70%	11.9
80%	17.9
90%	28.3
100%	171.3

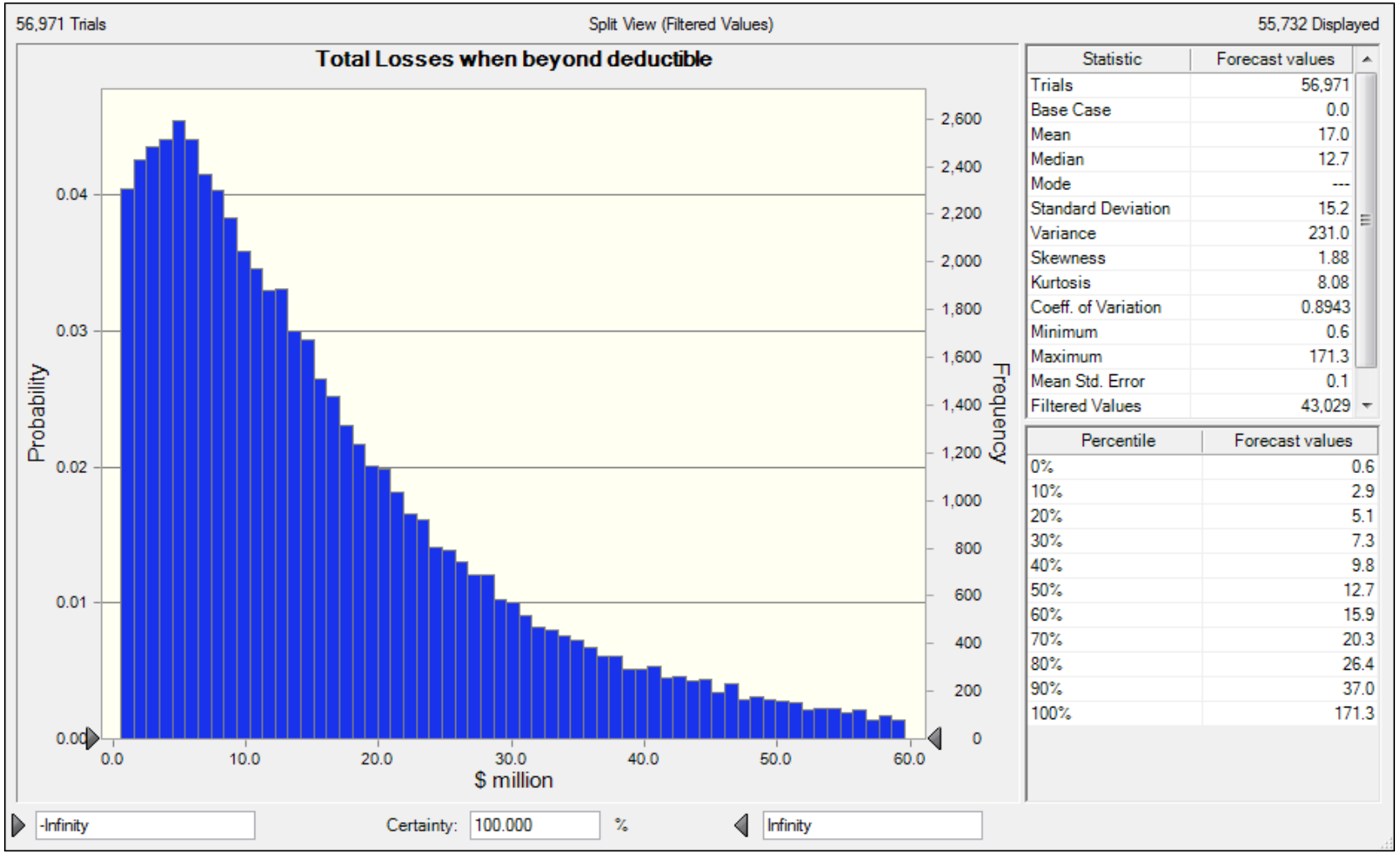
Shows $9.7m average net residual loss exposure (uninsured losses)

Example

FOCAL POINT DATA RISK

Step 3
MEASURE:
Outputs Inform Model/Scenario Testing to:
Measure Scenario-based Impacts.
Measure Mitigation Options / ROIs.
Measure Overall Cyber Risk Profile.

Simulated Losses Beyond Deductible: Total Cyber Losses Beyond $50k Deductible



Statistic	Forecast values
Trials	56,971
Base Case	0.0
Mean	17.0
Median	12.7
Mode	---
Standard Deviation	15.2
Variance	231.0
Skewness	1.88
Kurtosis	8.08
Coeff. of Variation	0.8943
Minimum	0.6
Maximum	171.3
Mean Std. Error	0.1
Filtered Values	43,029

Percentile	Forecast values
0%	0.6
10%	2.9
20%	5.1
30%	7.3
40%	9.8
50%	12.7
60%	15.9
70%	20.3
80%	26.4
90%	37.0
100%	171.3

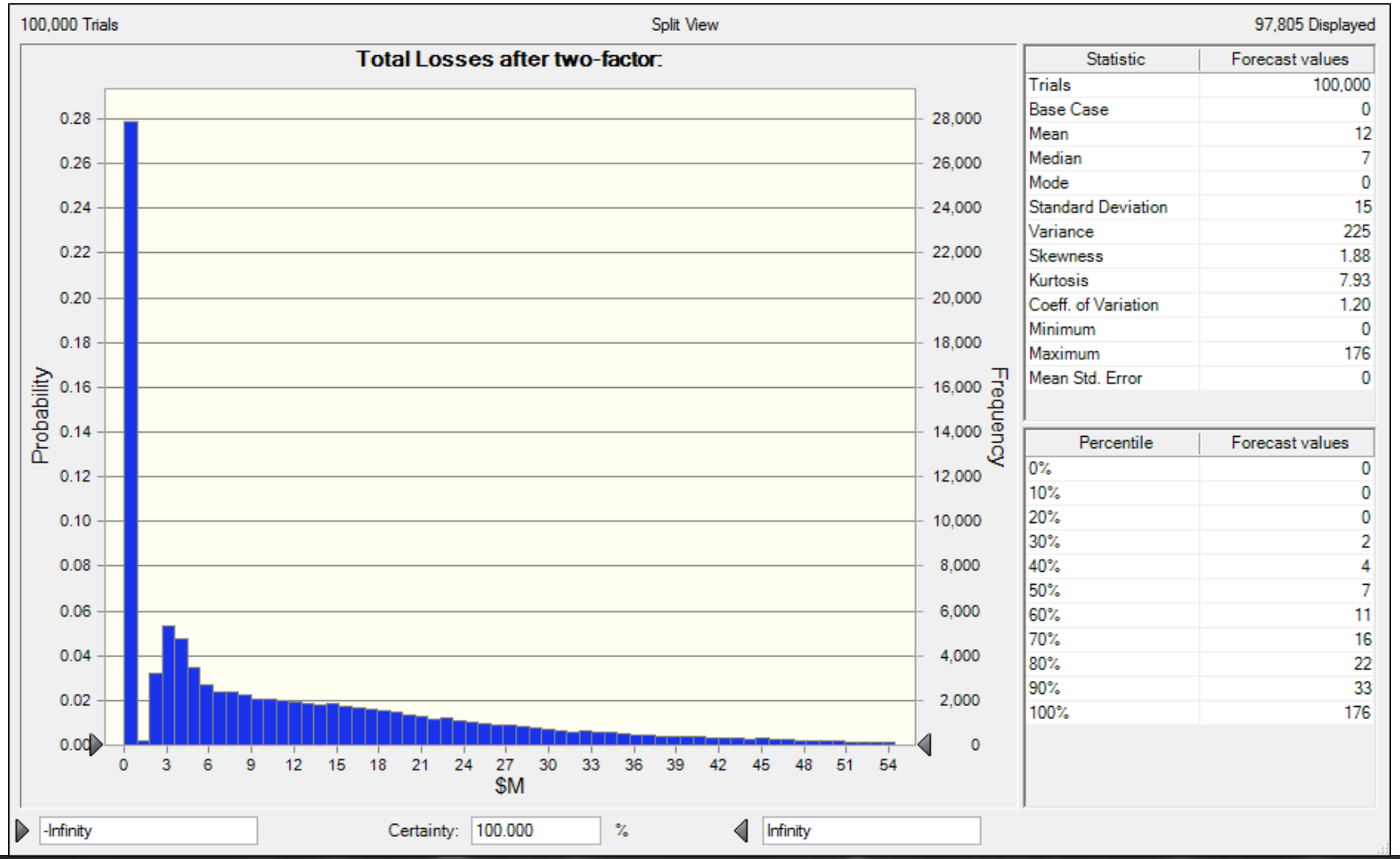
Shows $17m of exposure remaining which can be mitigated through higher insurance limits

Example

FOCAL POINT DATA RISK

Step 3
MEASURE:
Outputs Inform Model/Scenario Testing to:
Measure Scenario-based Impacts.
Measure Mitigation Options / ROIs.
Measure Overall Cyber Risk Profile.

Simulated Losses Under Two-Factor Authentication: Total Losses Using 2FA



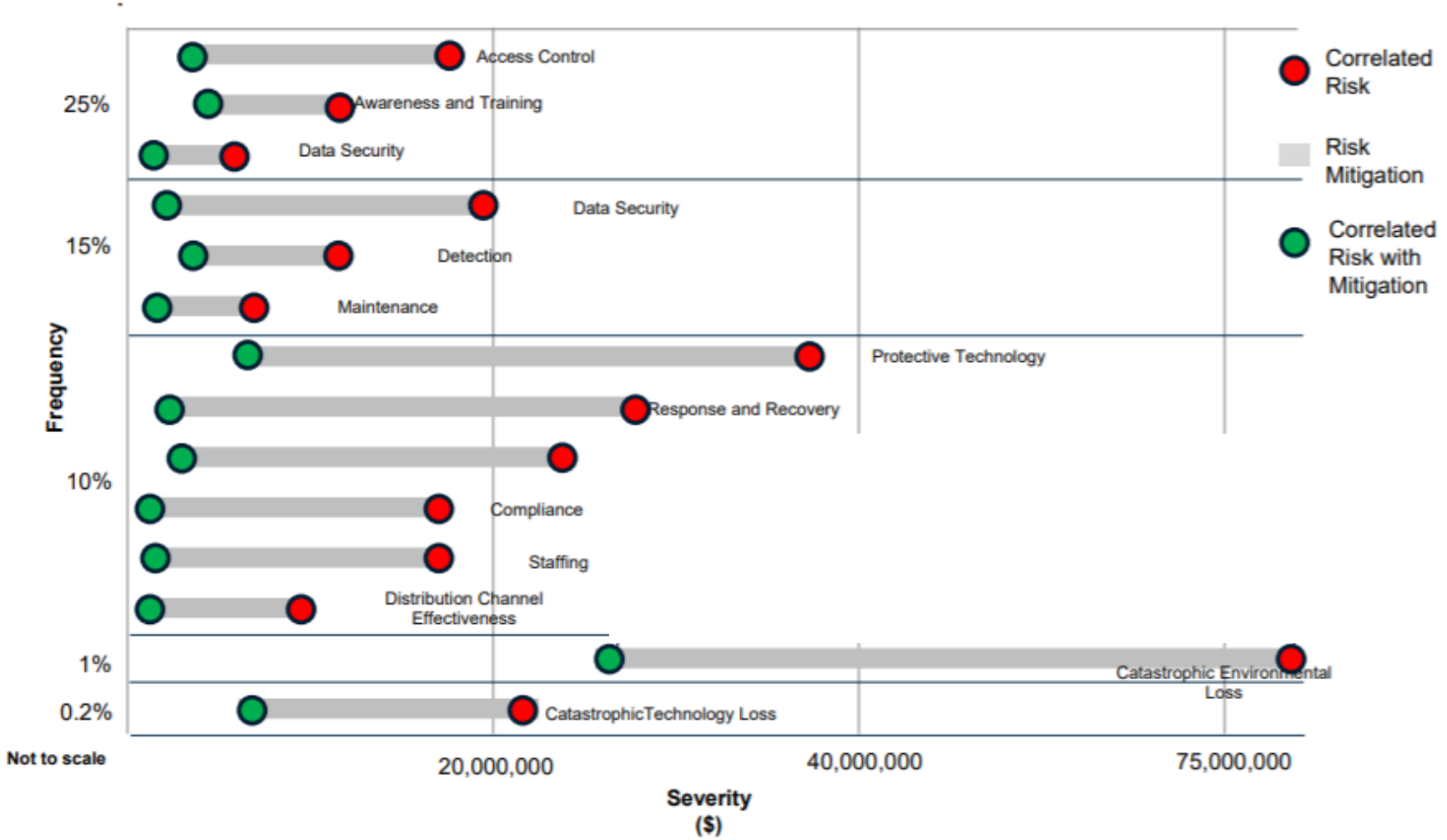
Statistic	Forecast values
Trials	100,000
Base Case	0
Mean	12
Median	7
Mode	0
Standard Deviation	15
Variance	225
Skewness	1.88
Kurtosis	7.93
Coeff. of Variation	1.20
Minimum	0
Maximum	176
Mean Std. Error	0

Percentile	Forecast values
0%	0
10%	0
20%	0
30%	2
40%	4
50%	7
60%	11
70%	16
80%	22
90%	33
100%	176

Shows improvement in the value of cyber losses (less) post implementation of two-factor authentication (2FA) technology (mitigation solution)

FOCAL POINT DATA RISK

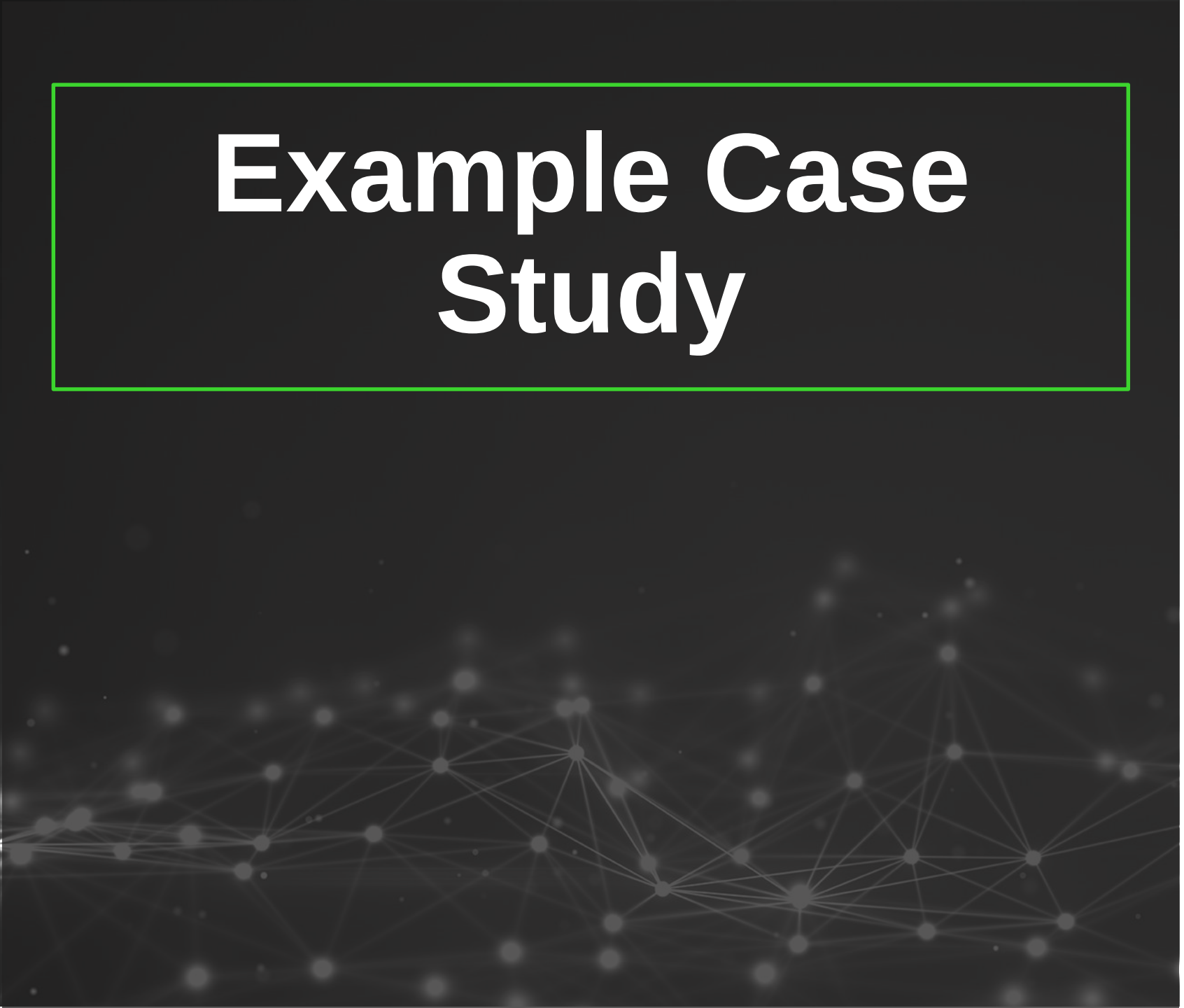
Enterprise Risk Impacts:
Correlated Cyber Risk Impact Views



Example

FOCAL POINT DATA RISK

Example Case Study



FOCAL POINT

DATA RISK

Case Study Example:
Solving For An Enterprise-wide Cyber Loss Profile

- Assisted a prominent global healthcare research organization with qualifying and quantifying operational risks, and doing so with a key focus on identifying emerging cyber risk related loss exposures.
- The operational risk assessment involved estimating and quantifying the value of a vast amount of longitudinal research studies (a key organizational product sold into the marketplace) that were critical to annual revenue.
- The product was largely warehoused in a proprietary IT system that was undergoing operational changes. Worked with internal client teams to assess the cyber risk profile and apply NIST/COBIT/ISO27K control and risk frameworks and develop a gap analysis'.
- Proposed appropriate risk mitigation strategies involving personnel, enhanced processes and additional technology. Specific insurance solutions were also examined.

Case Study Example:
Solving For An Enterprise-wide Cyber Loss Profile

- This organization then asked to:
  - deeply test its cyber security environment across multiple IT networks and across both mature and immature technology environments;
  - categorize, quantify, and model its operational cyber risks; and
  - understand how its cyber risk profile impacts its enterprise wide risk mitigation strategies and insurance (limits and coverage).
- Responses and solutions included:
  - performing numerous ERM and operational cyber risk assessments (e.g., vulnerability & compromise assessments, external network scans, ERM risk maturity assessments and reports.) to produce qualitative and quantitative reporting of operational risks;
  - developing a risk taxonomy that is useful for operational risk assessment; more fully aligned with the NIST framework. Developed a unique approach to a cyber risk scoring methodology; and
  - using operational risk modeling results to help inform various operational risk and financial risk hedging strategies the organization can undertake as part of its overall ERM and risk management strategies.

Team Bios

FOCAL POINT

DATA RISK

Background

Yvette Connor

Chief Risk Officer & Lead Engagement Partner
Enterprise Risk Consulting

Yvette Connor joined Focal Point in 2017 as its Chief Risk Officer and head of the Enterprise Risk Consulting practice. Ms. Connor has more than 20 years of experience building, and implementing and testing enterprise risk frameworks. She is a thought leader on emerging risk and efficient ways to effectively manage and link enterprise risk frameworks with regulatory, InfoSec, compliance, and audit platforms. Ms. Connor focuses on identifying opportunities for value creation, including building decision-driven models informed by risk awareness and organizational behavior.

Immediately prior to joining Focal Point, Yvette Connor was a Managing Director with Alvarez & Marsal Insurance and Risk Advisory Services in Chicago, where she focused on global Enterprise Risk Management engagements and developed an approach for Enterprise-wide cybersecurity risk valuation.

Ms. Connor's research is focused on ways companies identify risk priorities broadly throughout an organization or more narrowly, by going deeper into a specific risk topic. Her master's thesis,: "Does Risk Management Matter to Shareholders," describes a methodology to financially assess the impacts of "sophisticated" risk management on both profitability and growth.

Prior to A&M, Ms. Connor served as the Director of Client Engagement for Marsh,, Inc. where she lead a proprietary global servicing model designed to define clients' business needs and risk priorities, design optimal risk management responses, and deliver value-add solutions (Marsh 3D). Ms. Connor is the lead designer of the Dynamic Risk Mapping tool utilized by Marsh, Inc, within their global iMap analytics offering.

Prior to joining Marsh in 2010, Ms. Connor was the Director of Risk Management at Vulcan Inc., a privately held company, with a diverse portfolio of over 200 operating companies. While at Vulcan, Ms. Connor led the development of a multi-disciplinary risk management department and rolled out an enterprise-wide risk management framework across a portfolio of stakeholders and companies..

Ms. Connor was the Vice President of Risk Management at Roll International (now, the Wonderful Company), a global food producer, distributor and product manufacturer, as well as Director of Insurance and Risk Financing at Sutter Health.

Ms. Connor earned a master's of science degree in risk management at NYU and an MBA in finance at University of California, Davis., graduating Beta Gamma Sigma (highest honors). In 2013, *Business Insurance* magazine named Ms. Connor as one of the "Women to Watch" in Risk Management and Insurance, confirming her talents as a leader and innovator for risk management excellence. In 2008, *Treasury and Risk* magazine named her as one of the up and coming key leaders in treasury risk, as part of their "40 under 40 list."

FOCAL POINT DATA RISK

Background

Bill Foote

Senior Director
Enterprise Risk Consulting

Bill Foote joined Focal Point in 2017 as a Senior Director/Strategic Advisor in its Enterprise Risk Consulting practice in New York City and is focused on supporting and delivering ERM solutions to Focal Point clients. Dr. Foote has over 40 years of risk and performance modeling and consulting experience in private and public sector organizations. Dr. Foote has led several public and sector enterprise risk quantification and management initiatives, and he has specialized expertise across several functional domains including quantitative and qualitative modeling of market, credit, and operational risk.

Immediately prior to joining Focal Point, Mr. Foote was a Director with Alvarez & Marsal's Insurance and Risk Advisory Services in New York. While at A&M, Dr. Foote has designed, developed and built an enterprise risk management process, governance, quantification, and reporting capability for impending ORSA and existing business decision making requirements. He also built enterprise risk measurement and reporting for mitigation decisions and regulatory disclosure by senior management of a major U.S. asset manager.

Dr. Foote has built market, credit, and operational risk functionality for financial services, energy, manufacturing, and public sector firms. Specifically for credit, he implemented credit risk governance, risk factor identification and quantification, transaction structuring, collateral and counterparty management, and the production of reviews, reports, presentations for regulators, investors, management, and public disclosure. He also provided expert testimony in legal and regulatory proceedings regarding credit risk practices, transactions and risk management systems, collateral valuation, analysis of credit events and their impact on asset portfolios. Dr. Foote has participated in the structuring of transactions to mitigate credit risk and provided specialist valuation services for management and external auditors.

On other projects at Paraclete, Dr. Foote advised a major pharmaceutical to improve margins and reduce treasury, marketing, and sales process costs on an operating annual budget by designing integrated valuation, risk control assessment and assurance, value chain, decision, real options pricing, and KPI taxonomies to deliver enterprise risk and performance strategy for CFO business planning and budgeting function; constructed business simulation, scenario analysis, stress testing, capital modeling and review to support project management based on integrated taxonomies.

Prior to working with Alvarez & Marsal, Dr. Foote started his career, and was credit trained, at Manufacturers Hanover, and was more recently a Senior Manager with Ernst & Young, a Firm Director with Deloitte & Touche, a Vice President with Charles River Associates, and most recently a Principal at Paraclete Risk Solutions. Dr. Foote holds his M.A. and Ph.D. in Economics from Fordham University, and also has a B.A. in Classical Languages and Philosophy from Fordham.

FOCAL POINT DATA RISK

Background

Daniel Barwick

Director,
Enterprise Risk Consulting

Daniel Barwick is a Director with Focal Point's Enterprise Risk Consulting practice. He specializes in market, credit and operational risk analysis and mitigation. With more than 14 years of Risk Management experience, Mr. Barwick's primary areas of concentration are with the analytics/models for risk metrics and valuations and the associated systems and methods to gather the data to drive these models.

Prior to joining Focal Point, Mr. Barwick was a Director in Alvarez & Marsal (A&M)'s Enterprise Risk Management practice where he worked on complex risk quantification projects related to Technology risk, among others.

Prior to A&M, Mr. Barwick served as a subject matter expert for bulge bracket banks working on their CCAR (Capital adequacy reviews) reviews of their market risk models for CVA, trade and derivative models. Along with the review of these models Mr. Barwick also added insight and opined on the system layouts and governance processes currently in place, suggesting new measures where applicable to mitigate procedural and operational risk to the companies.

Mr. Barwick has experience in the auto leasing industry where serving as an analyst he helped to model the residual values for autos. He also performed analysis on the potential resale values and impacts of tax benefits such as like kind exchange on the pricing and value of the portfolio at large.

Before his transition to consulting, Mr. Barwick served as a financial engineer for Fannie Mae in Washington DC, where he helped to specify the design of and roll out new risk system updates to the models and systems responsible for various market risk, credit default, prepayment and trade analytics across the company.

Additionally, prior to his service at Fannie Mae, Mr. Barwick gained valuable counterparty risk experience at Ditech mortgage in Fort Washington PA, where functioning as a risk manager assessing the companies aggregate market exposure to third parties and ensuring these assessed risk were within established tolerances. While at Ditech, Mr. Barwick helped to redesign their counterparty risk system during the company's divestiture from Ally Bank form scratch into a more cost effective form to meet the needs of the new formed small business.

Mr. Barwick earned a bachelor's degree in finance from Virginia Polytechnic and State University and a master's degree in Finance from George Washington University.

FOCAL POINT DATA RISK

Background

Damon Levine

Director
Enterprise Risk Consulting

Damon Levine is a published enterprise risk management thought leader, industry speaker, and practitioner, serving as a Director in Focal Point's Enterprise Risk Management practice. Mr. Levine has more than 20 years' experience in enterprise risk management, asset management, quantitative modeling, consulting, and insurance. His specialties include risk-reward optimization, risk appetite and limit systems, risk modeling, risk training, and linking ERM to strategy and company value. Mr. Levine emphasizes a business-enabling approach to risk management that reflects a company's culture, business goals, and resources.

Mr. Levine has researched and developed approaches to improve risk culture, embed ERM in operating companies, and optimize both return on capital and earnings as a function of product allocation. He is the winner of the Actuarial Foundation's ERM Research Excellence Award for his whitepaper "Enterprise Risk-Reward Optimization: Two Critical Approaches" and the Joint CAS/CIA/SOA Award for Practical Risk Management Applications for "Growth in Stock Price as the ERM Linchpin".

Prior to joining Focal Point, Mr. Levine served as Vice President, Enterprise Risk Management for Assurant Inc., where he developed and implemented its risk framework and risk governance infrastructure while serving on the ERM, Information Security, and Benefit Plan Investment Committees of this global Fortune 300 insurer. In that role, he partnered with all business lines and functional areas to manage risk exposures and mitigations for financial, credit, market, operational, and insurance risks.

He is a frequent speaker at RIMS, the Enterprise Risk Management Symposium, Insurance Nexus, the Actuarial Society of NY, and Marcus Evans conferences. He has taught actuarial mathematics at Columbia University, was published in The Actuary, and has been included in Society of Actuaries' exam syllabus. He authored the March 2017 cover article for the CAS/CIA/SOA Joint Risk Management Section.

Mr. Levine holds a Masters in Mathematics from the University of Maryland at College Park and a BA in Statistics/Mathematics from the State University of New York at Buffalo, where he graduated Summa cum Laude, Phi Beta Kappa, and received the Best Undergraduate in Mathematics award. He is a Chartered Financial Analyst (CFA) and Certified Risk and Compliance Management Professional (CRCMP) with over 20 years' experience in ERM, cyber risk management, COSO, ORSA, insurance, quantitative modeling, asset management, and consulting.

FOCAL POINT
DATA RISK

Background

Doug Richter

Manager
Enterprise Risk Consulting

Doug Richter joined Focal Point in 2017 as a Manager in its Enterprise Risk Consulting practice in New York City. Mr. Richter brings extensive experience in the areas of ERM, corporate risk management, insurance, and project management (PMO) in the staffing, insurance, manufacturing, oil & gas, technology, pharmaceutical, and construction industries. Immediately prior to joining Focal Point, Mr. Richter was a Manager with Alvarez & Marsal Insurance and Risk Advisory Services (A&M) in New York and a member of its ERM team. While at A&M, Mr. Richter has helped lead multiple engagements that has included project work with a large healthcare insurer, state governments, and a staffing company, working across multidisciplinary teams on a variety of projects.

Mr. Richter also served as Director of M&A Transaction Services at The Hauser Group based in New York. Mr. Richter was responsible for performing and managing the Risk Management and Insurance due diligence process and developing the go-forward recommendations for Hauser's Private Equity partners and related portfolio companies.

Prior to joining Hauser, Mr. Richter was a Management Consultant with Deloitte Consulting LLP's Actuarial, Risk and Analytics (ARA) practice in New York City for over four years where he regularly served some of Deloitte's largest clients. Amongst his risk management and insurance work, Mr. Richter led two major PMO insurance & risk management work streams on Coca-Cola's acquisition of Coca-Cola Enterprises and Pfizer's merger with Wyeth. Mr. Richter also managed the day-to-day PMO of Deloitte's Audit engagement of MetLife, covering its global operations.

Prior to joining Deloitte in January 2008, Mr. Richter was a risk manager with Volt Information Sciences, Inc., a Fortune 1000 multi-services company. He was responsible for managing, monitoring, and responding to various risks and losses at several thousand domestic and international company and client-worksite locations of a contingent workforce of nearly 55,000 and an annual workers' compensation program in excess of $30 million.

Mr. Richter also worked for Allstate Insurance Company where he served as Associate, servicing personal and commercial lines of insurance coverage. Among his responsibilities included field-level underwriting of new business risks as well as performing initial loss assessments in processing policyholder's property and casualty claims.

Mr. Richter has co-authored numerous thought leadership articles on a variety of risk management and insurance topics including product recall, safety analytics, directors & officers liability, and sustainability. Mr. Richter earned a bachelor's degree in Economics with a concentration in Business from Indiana University, Bloomington. Mr. Richter also holds the Associate in Risk Management (ARM) designation.

FOCAL POINT
DATA RISK

Background

Soraya Wright

Consultant
Enterprise Risk Consulting

Soraya Wright, is a Consultant in Focal Point's Enterprise Risk Consulting practice and has over 30 years of experience managing complex risks for global businesses. She leverages her experience to identify and evaluate enterprise risks and determine appropriate mitigation and risk finance strategies.

Soraya previously held executive positions, including VP-Global Risk Management & Crisis Management at The Clorox Company where she was responsible for leading Clorox's enterprise risk management program, the Company's global insurance strategy, crisis management and business continuity for worldwide operations, and President-Board of Directors of the Company's captive insurance subsidiary which she formed; and, VP-Enterprise Risk Management at Target where she was recruited to launch the strategy and centralized oversight of Target's post-breach enterprise risk management program.

Soraya is committed to community service and has served in a leadership capacity at over a dozen community and professional organizations, including the Board of Trustees at Holy Names University, Oakland's Children's Hospital Foundation, and the East Oakland Youth Development Center's Board of Directors. In recognition for her community service, The United Way honored Soraya with the Adele K. Corvin Outstanding Agency Board Volunteer Award.

Sought out for her expertise, Soraya has served on the Client Advisory Board of several insurance companies and commercial insurance brokerage firms including ACE (Chubb), FM Global, and MARSH. She is a frequent speaker at Risk and Insurance Management Society (RIMS), Advisen, and Hawaiian Captive Insurance Forum conferences, covering a broad range of risk management topics including Enterprise Risk Management (ERM) strategies, managing executive risks, forming captive insurance companies and managing complex claims.

Soraya received her BA in Business Administration & Economics from Holy Names University. She is a member of the Executive Leadership Council (ELC) and Delta Sigma Theta Sorority, Inc. In December 2015, Soraya was named by Business Insurance as a "Woman to Watch".

FOCAL POINT
DATA RISK

Contact Us

Yvette Connor

CRO | Enterprise Risk Consulting Leader

yconnor@focal-point.com

206.669.7440

Headquarters

201 E. Kennedy Blvd.

Suite 1750

Tampa, FL 33602

Focal-point.com

Focal Point Data Risk

@focalpointdr

PARKING LOT

FOCAL POINT

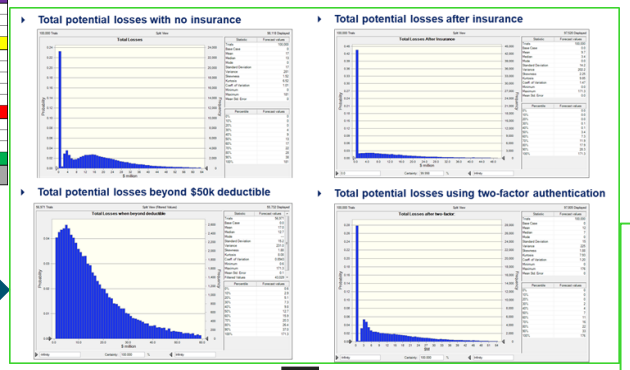
DATA RISK

Our Integrated Cyber Risk Measurement Process

Identify Risks Through A NIST-CSF and/or CRE Evaluation

CORE	SUBCATEGORY	Risk Score
IDENTIFY	Asset Management	2.35
	Business Environment	2.15
	Governance	1.75
	Risk Assessment	1.25
	Risk Management Strategy	2.25
	IDENTIFY CORE - TOTAL SCORE	1.95
PROTECT	Access Control	1.50
	Awareness and Training	2.00
	Data Security	2.50
	Information Protection and Procedures	1.75
	Maintenance	2.75
	Protective Technology	2.50
	PROTECT CORE - TOTAL SCORE	2.17
DETECT	Anomalies and Events	2.35
	Security Continuous Monitoring	1.85
	Detection Processes	2.25
	DETECT CORE - TOTAL SCORE	2.15
RESPOND	Response Planning	1.75
	Communications	2.50
	Analysis	2.85
	Mitigation	1.25
	Improvements	1.75
	RESPOND CORE - TOTAL SCORE	2.02
RECOVER	Recovery Planning	1.25
	Improvements	1.25
	Communications	1.75
	RECOVER CORE - TOTAL SCORE	1.42
	GRAND TOTAL SCORE	1.94

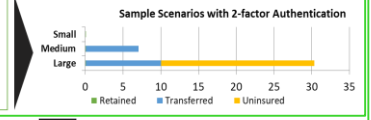
Assess Evaluation Outputs, Perform Modeling, and Measure Cyber Risk Impacts & Profile



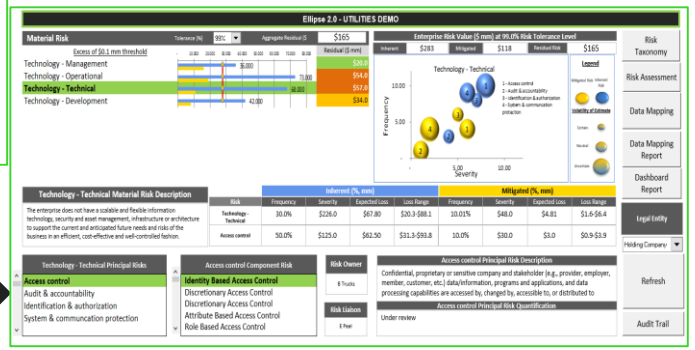
Operations	Average Results							
	Unlimited loss (no insurance scenario)		Retained loss (first $.05 M)		Transferred loss (next $10.00 M)		Uninsured loss (beyond $10.05 M)
Before 2-factor	16.54 M	=	0.04 M	+	6.71 M	+	9.79 M
After 2-factor	12.46 M	=	0.04 M	+	5.66 M	+	6.77 M

- Averaging events and non-events, your expected deductible loss is less than the $50 k max
- Averaging events and non-events, the expected insurance payment is less than the $10 M max
- Some events may be so large that most of your expected losses will **not** be covered by insurance

- At right are three sample scenarios.
- Losses come in different sizes, and trigger different amounts of coverage.
- The average of the three sample scenarios gives the result at the top.

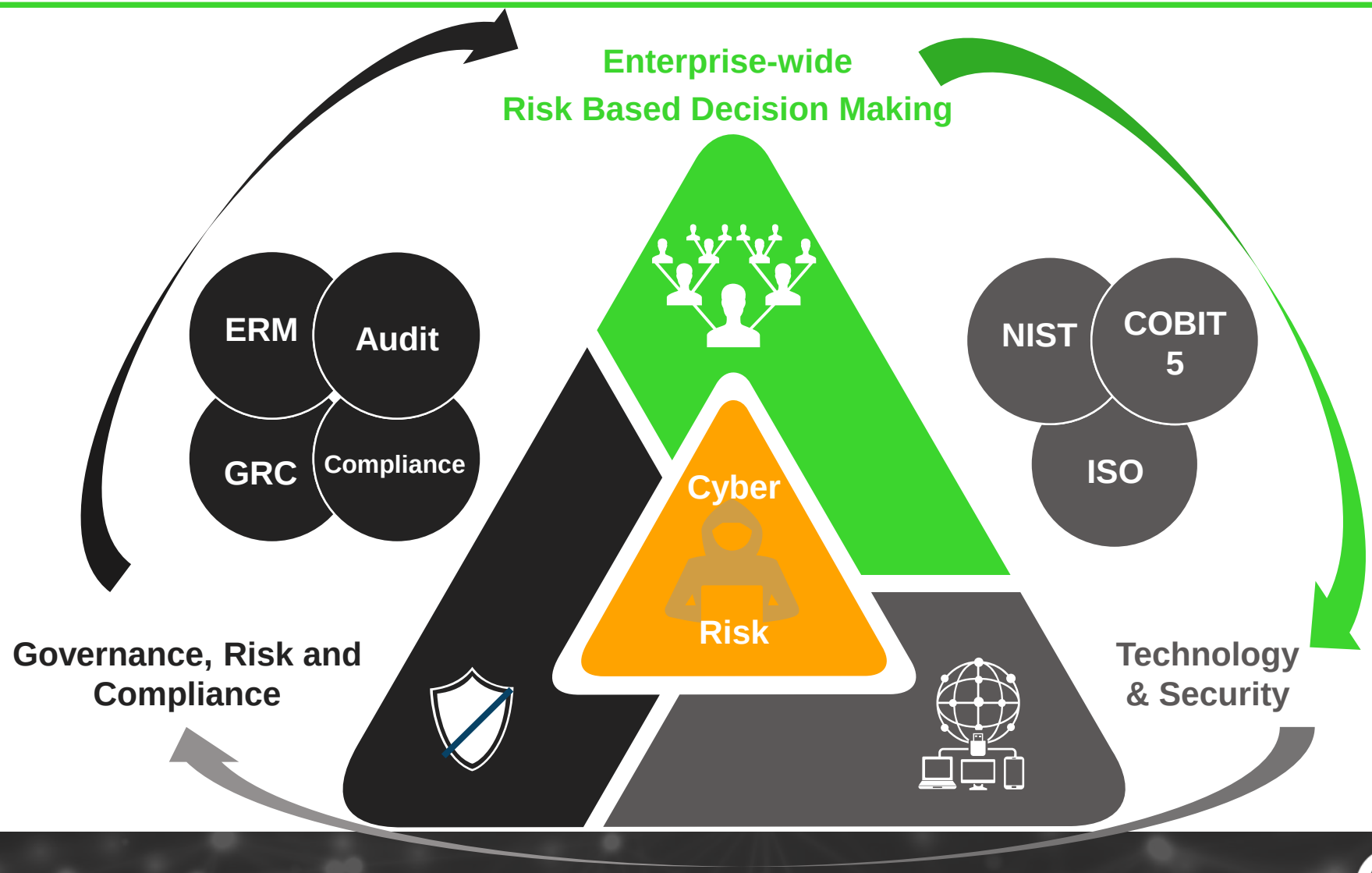


Clear Analysis/Visualizations Inform Risk-based Decisions



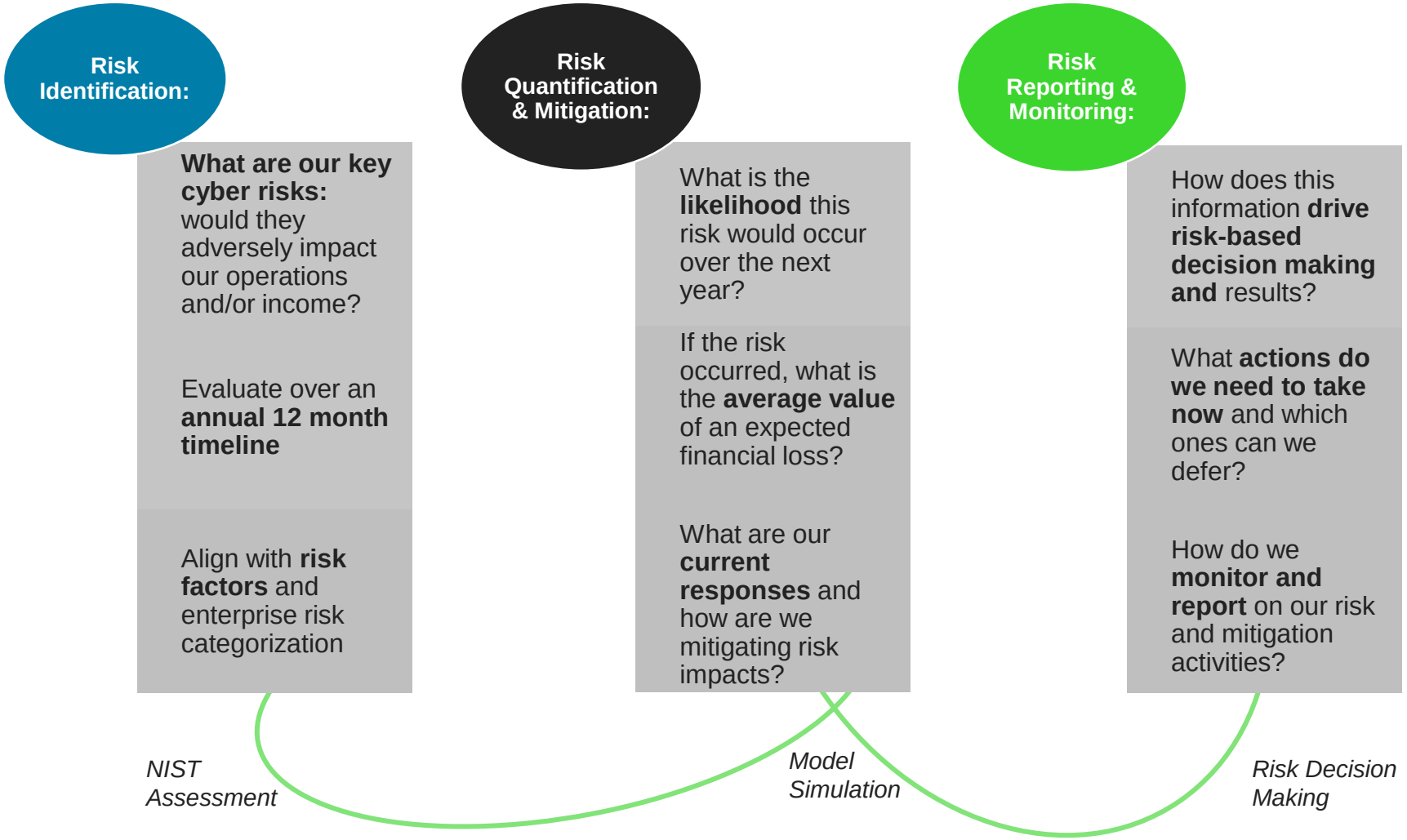
FOCAL POINT DATA RISK

Using An Integrated Approach To Cyber Measure



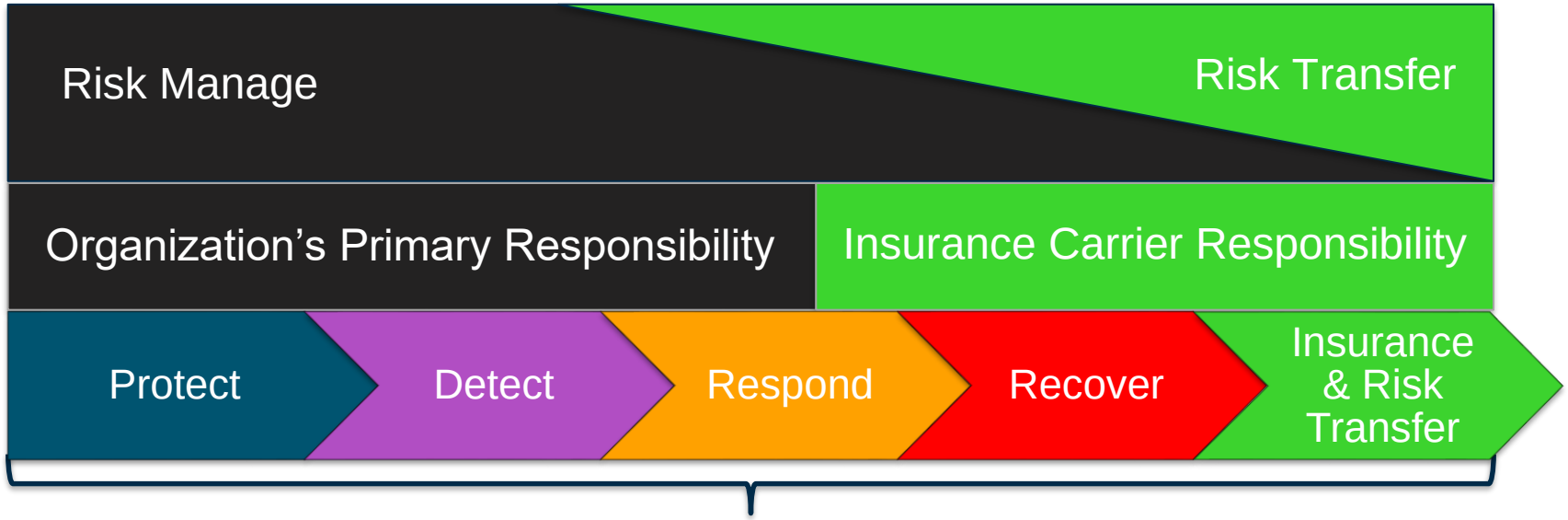
FOCAL POINT DATA RISK

Key Considerations Addressed In Three Steps



FOCAL POINT DATA RISK

Leverage Quantified Results To Drive More Robust Insurance And Operational Risk Decision Making



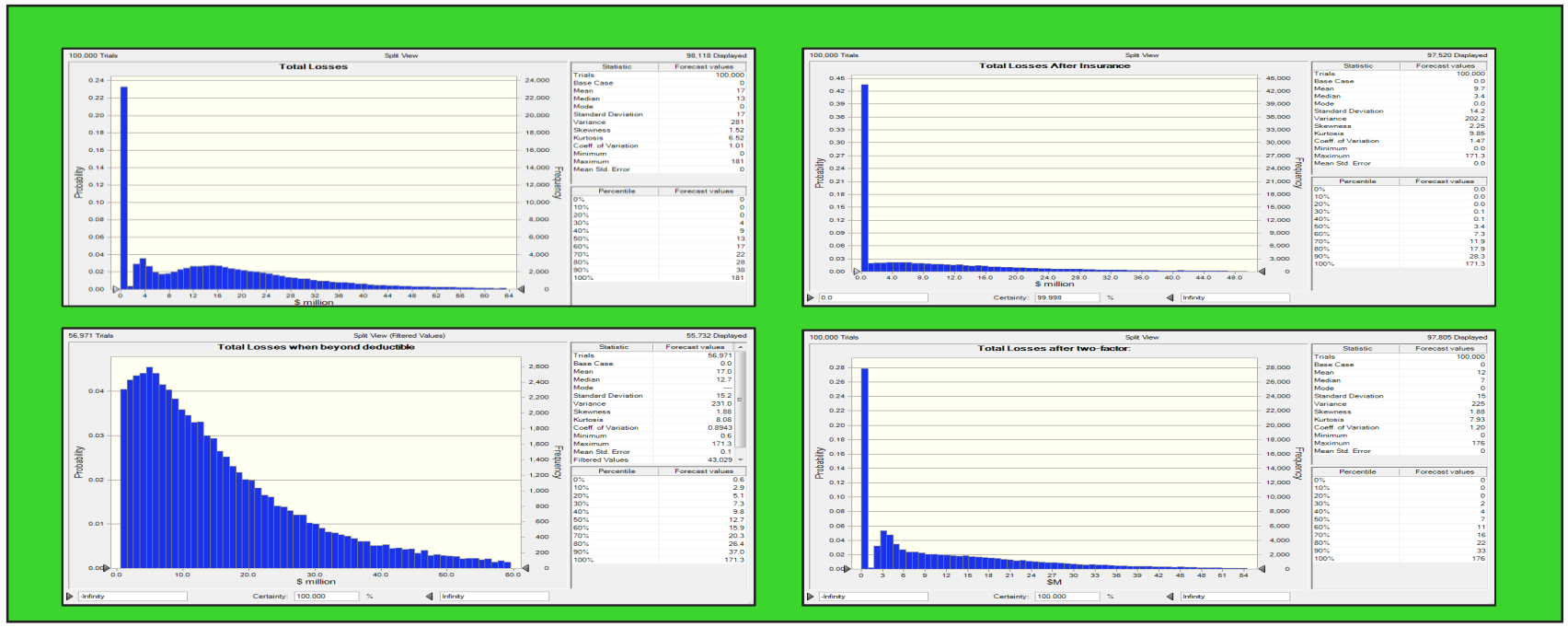
Cyber Risk Management Lifecycle

Many enterprises's primarily focus its traditional cybersecurity spend to develop suitable risk management measures to put in place the right protection, detection, and basic response measures. Cyber insurance, as an example, is typically used to provide response, recovery, and liability management support.

FOCAL POINT DATA RISK

Conduct Modeling and Scenario Testing

- Focal Point applies NIST evaluation outputs and assumptions, estimates, scenarios, and any relevant inputs into our Ellipse quantification and simulation tool to derive cyber risk exposure and loss estimates.
- Each defined cyber risk scenario runs through Ellipse to estimate the potential losses for that scenario. The Ellipse model uses various model inputs within a Monte Carlo simulation, and in combination with other statistical techniques, develops cyber loss estimates. These scenarios will help inform the basis of our Client's cyber risk exposure/profile.
- The cyber loss estimates are estimated at the 95% confidence level, as well as 55% and 75%.

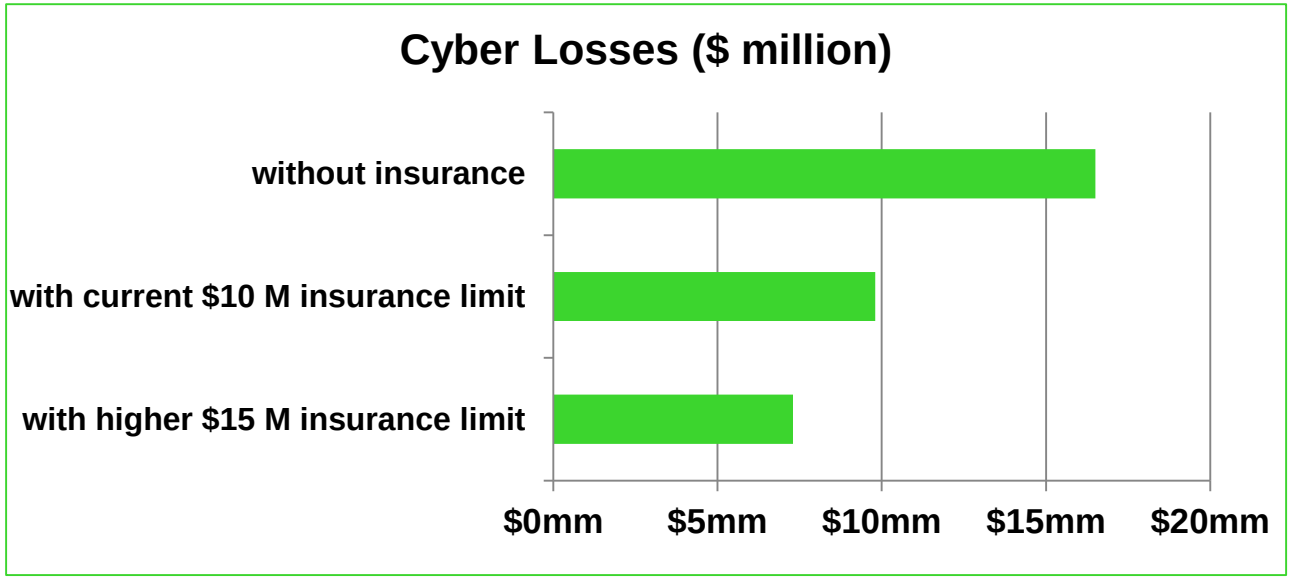


FOCAL POINT DATA RISK

Example Finding:
Value Of Insurance And Risk Transfer

We modeled cyber losses for both organizational entities together, since they will be insured together, and considered implementation of two-factor authentication given this was a likely investment decision:

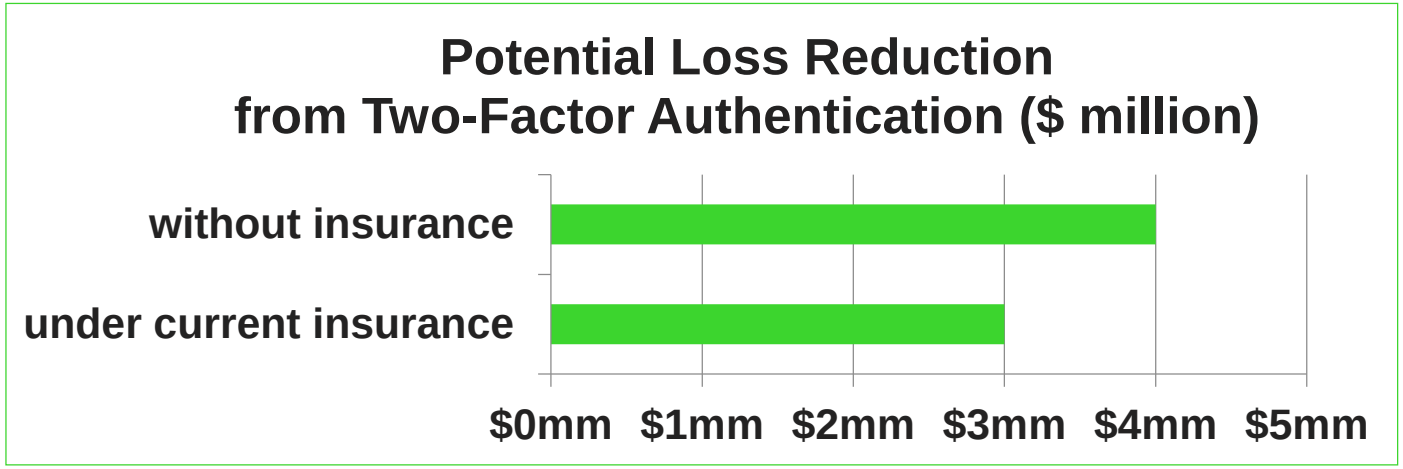
- Our modeling showed average cyber losses of $16.54 M before insurance
- With current insurance, cyber liabilities would be reduced to $9.79 million
- With another $5M of insurance coverage would be reduced to $7.3 million
- On an average basis, this additional coverage would be worth $2.5 million.



FOCAL POINT DATA RISK

Example Recommendation:
Determine Value of Risk Transfer And Insurance

- Our recommendation is to adopt two-factor authentication (2FA):
  - Our modeling estimates that 2FA would **reduce** the frequency of an **Access Control** event by **50%**
  - Without insurance, 2FA would reduce average losses by $4 million
  - With current insurance, 2FA would reduce average losses by $3 million.



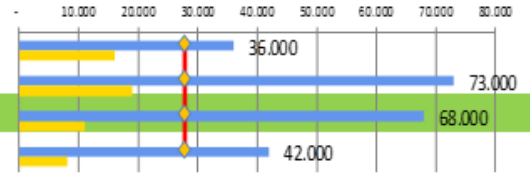
FOCAL POINT DATA RISK

Final Results Visualized (illustrative Access Control example)

Ellipse 2.0 - UTILITIES DEMO

Material Risk | Tolerance (%) 99% | Aggregate Residual ($ $165

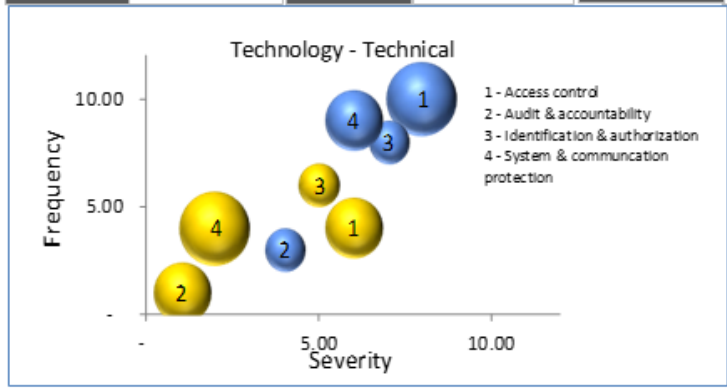
Excess of $0.1 mm threshold



	Residual ($ mm)
Technology - Management	$20.0
Technology - Operational	$54.0
Technology - Technical	$57.0
Technology - Development	$34.0

Enterprise Risk Value ($ mm) at 99.0% Risk Tolerance Level

Inherent	$283	Mitigated	$118	Residual Risk	$165



Risk Taxonomy | Risk Assessment | Data Mapping | Data Mapping Report | Dashboard Report

Technology - Technical Material Risk Description

The enterprise does not have a scalable and flexible information technology, security and asset management, infrastructure or architecture to support the current and anticipated future needs and risks of the business in an efficient, cost-effective and well-controlled fashion.

	Inherent (%, mm)				Mitigated (%, mm)			
Risk	Frequency	Severity	Expected Loss	Loss Range	Frequency	Severity	Expected Loss	Loss Range
Technology - Technical	30.0%	$226.0	$67.80	$20.3-$88.1	10.01%	$48.0	$4.81	$1.6-$6.4
Access control	50.0%	$125.0	$62.50	$31.3-$93.8	10.0%	$30.0	$3.0	$0.9-$3.9

Legal Entity

Holding Company

Technology - Technical Principal Risks

- **Access control**
- Audit & accountability
- Identification & authorization
- System & communcation protection

Access control Component Risk

- **Identity Based Access Control**
- Discretionary Access Control
- Discretionary Access Control
- Attribute Based Access Control
- Role Based Access Control

Risk Owner

B Trucks

Risk Liaison

E Peel

Access control Principal Risk Description

Confidential, proprietary or sensitive company and stakeholder (e.g., provider, employer, member, customer, etc.) data/information, programs and applications, and data processing capabilities are accessed by, changed by, accessible to, or distributed to

Access control Principal Risk Quantification

Under review

Refresh | Audit Trail

FOCAL POINT DATA RISK