# Creating a Cyber Resilient Organization:

## Taking Calculated Risks while Leading Through Emerging Regulatory Change


**Robert D. Brown III**
**Sr. Director of Cyber Resilience**
**Resilience**

# Robert D. Brown III

Senior Director of Cyber Resilience, Resilience

Fifth year contributing to **Risk Awareness Week**.

- 2019 – Value of information on continuous variables
- 2020 – Bayesian method for judging the likely scenario in a defined set that is unfolding
- 2021 – Measuring the value of carbon ($/tonne) and its effect on selecting green initiatives
- 2022 – How to optimize cybersecurity decisions when supporting data is scarce

25+ years of experience serving organizations from startups to government agencies and Fortune 100 companies as a senior strategic planner and decision science advisor.

Author of ***Business Case Analysis with R - Simulation Tutorials to Support Complex Business Decisions*** (Springer-Nature/Apress, 2018).

# What Is The Most Important Thing For CISO Success With…

THE MONEY PEOPLE?

JP Moneyperson III


Shared Objectives

# What Is Your Organization's Security Objective?

# What Is Your Organization's Security Objective?

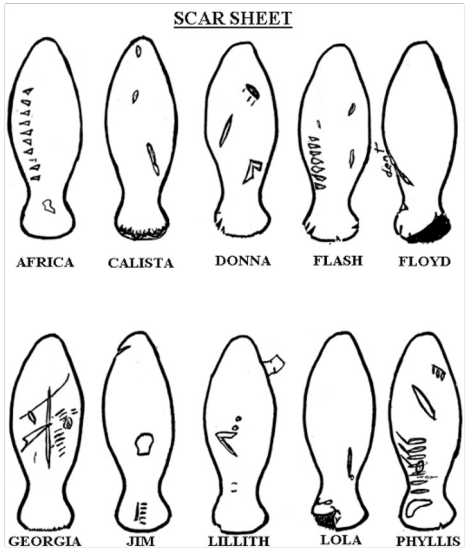
## Are We Resilient

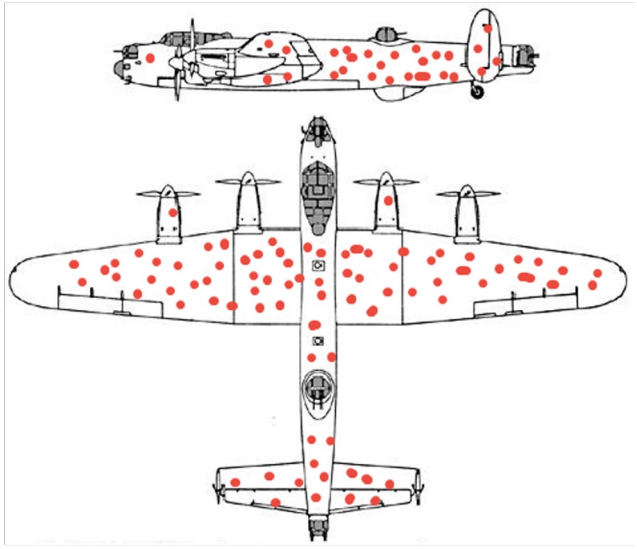
## To Material Losses?

Objectives Matter

# Identifying the Right Objectives

# Avoiding Wrong Objective Measures




**Manatees**

**WWII Bomber**

**Moneyball**

# Having The Right Objectives


**Objective:** Win the world series

**Goal:** In one year with a quarter budget

**Strategy:** Buy undervalued assets

**Tactics:** Maximize walks

# The New Material Objective For Security

Emerging Material Requirements

# Resilient To MATERIAL LOSSES

CyberResilience.com

# Emerging Requirements SEC Cyber Rules

# 355

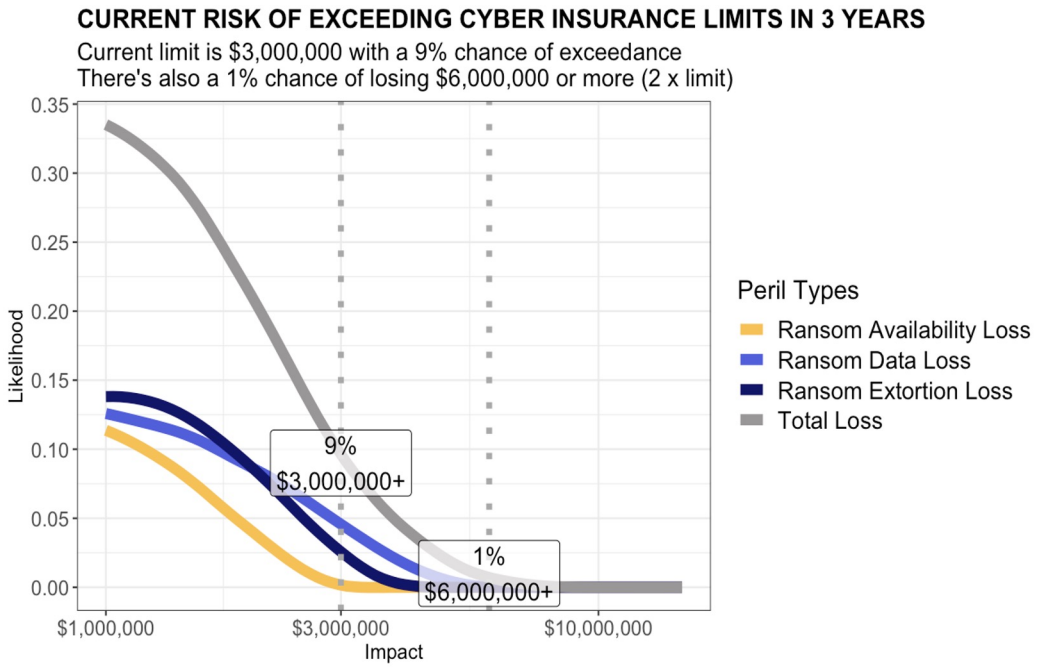
The number of times “**material**” is mentioned in the new SEC Cyber Rule

# Cyber Risk And The Board: Emerging SEC Requirements

## Risk Management and Strategy

"Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats…

"Describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition."



# Cyber Risk And The Board: Emerging SEC Requirements

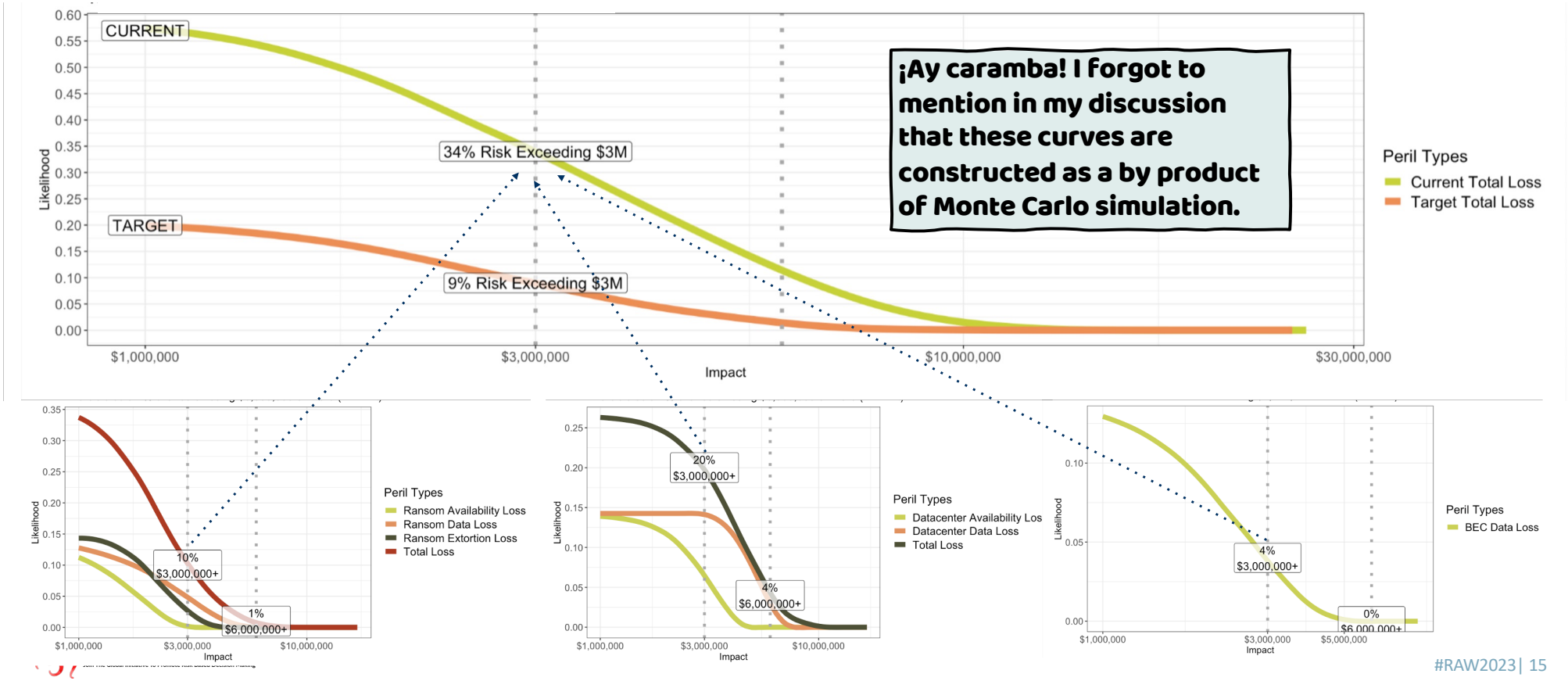
## Identify and manage cybersecurity risks and threats

"Including…

- operational risk;
- intellectual property theft;
- fraud;
- extortion;
- harm to employees or customers;
- violation of privacy laws and other litigation and legal risk; and
- reputational risk."

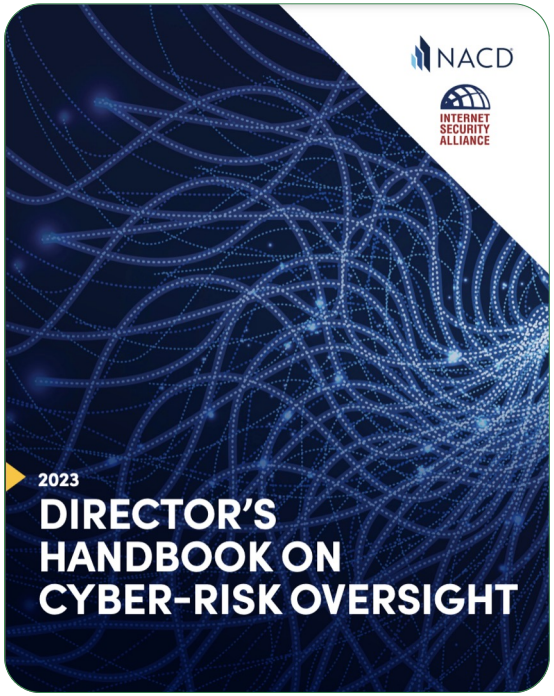
| Threat | Loss |
|---|---|
| Ransomware | Data Breach |
| Ransomware | Business Disruption |
| Ransomware | Extortion |
| Business Email Compromise | Fraud |
| Cloud Compromise | Data Breach |
| Cloud Compromise | Business Disruption |
| SaaS Compromise | Data Breach |
| SaaS Compromise | Business Disruption |
| Insider Threat | Data Breach |
| Insider Threat | Fraud |
| Insider Threat | Business Disruption |
| APT (State Sponsored) | Intellectual Property |
| APT (State Sponsored) | Data Breach |
| APT (State Sponsored) | Business Disruption |
| Software Supply Chain Compromise | Intellectual Property |
| Software Supply Chain Compromise | Data Breach |
| Software Supply Chain Compromise | Business Disruption |

# Cyber Risk And The Board: SEC Requirements



# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**29**

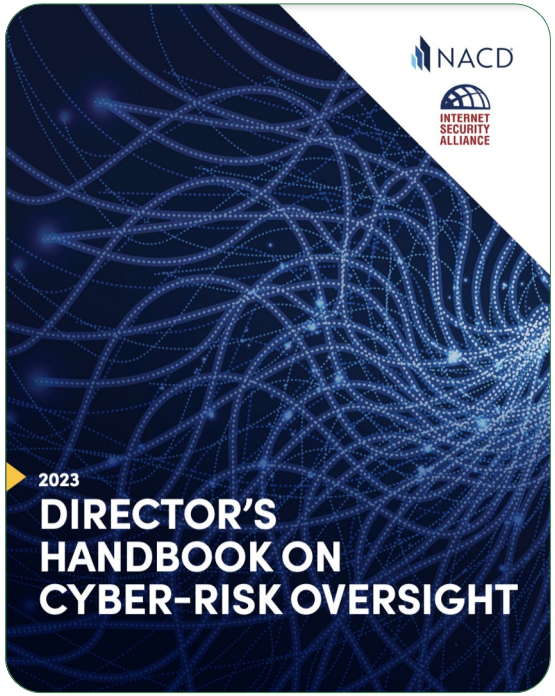



The number of times "**quant**" is mentioned in the new NACD Cyber-Risk Handbook

# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**Board Members are seeing cybersecurity as a strategic risk**

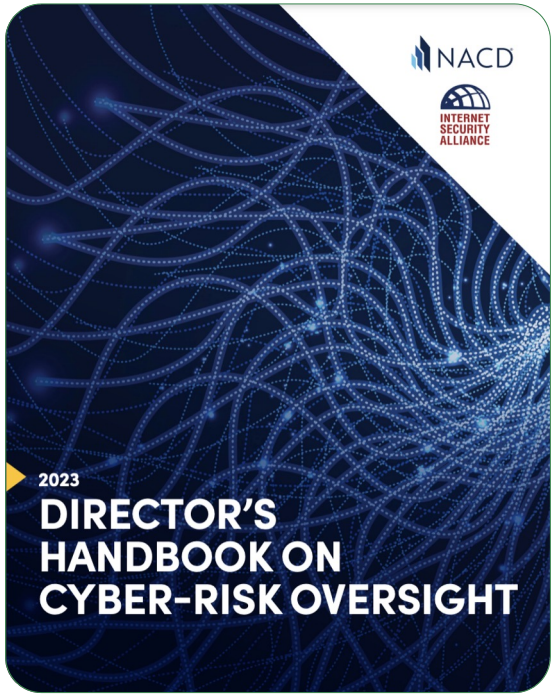
**1** Directors need to understand and approach cybersecurity as a **strategic, enterprise risk… not just an IT risk.**



# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**Board Members are seeing cybersecurity as a strategic risk**

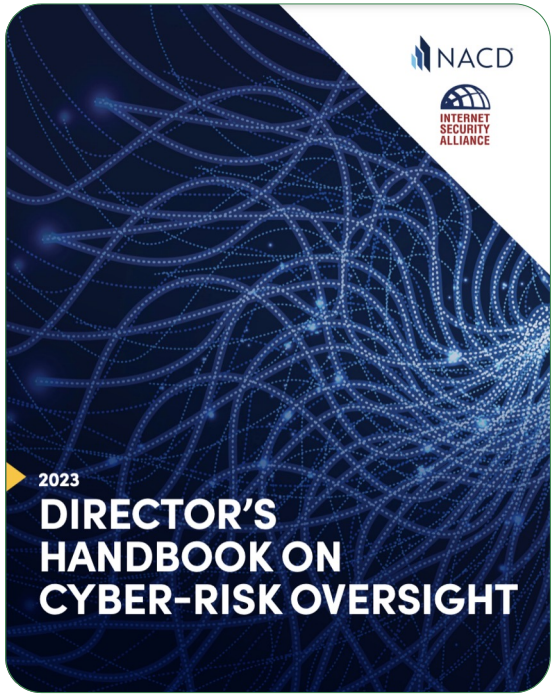
**2** Directors should understand the **legal implications of cyber risks** as they relate to their company's specific circumstances.



# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**Board Members are seeing cybersecurity as a strategic risk**

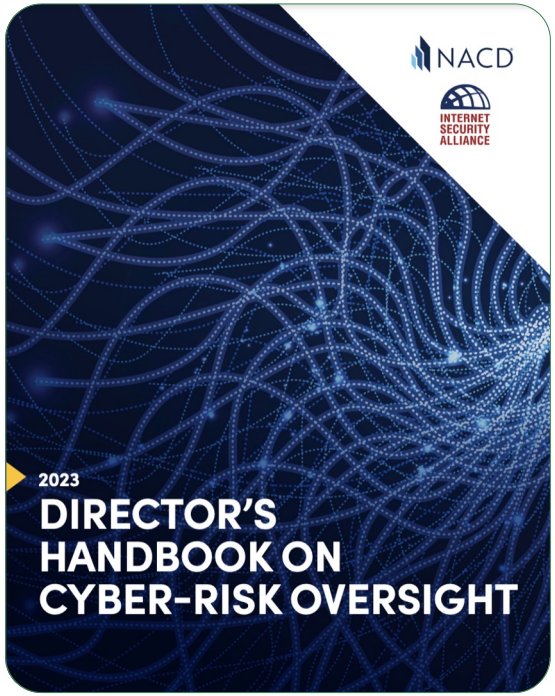
**3** Boards should have adequate access to **cybersecurity expertise**, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.



# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**Board Members are seeing cybersecurity as a strategic risk**

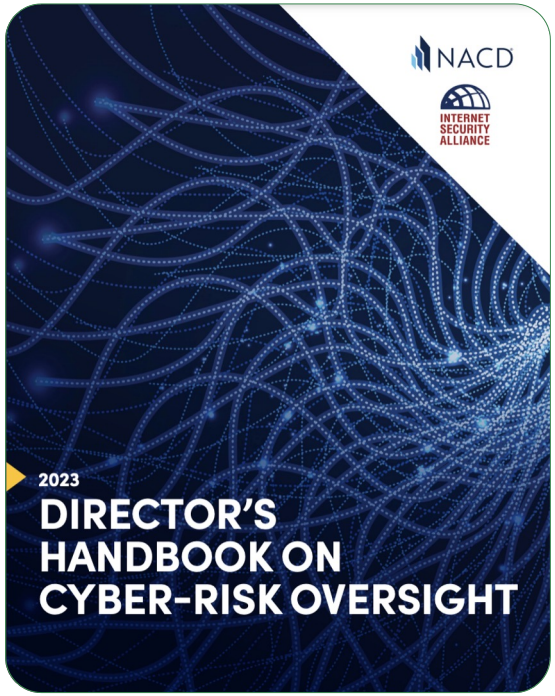
**4** Directors should set the expectation that management will establish an **enterprise-wide, cyber-risk management framework and reporting structure with adequate staffing and budget.**



# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**Board Members are seeing cybersecurity as a strategic risk**

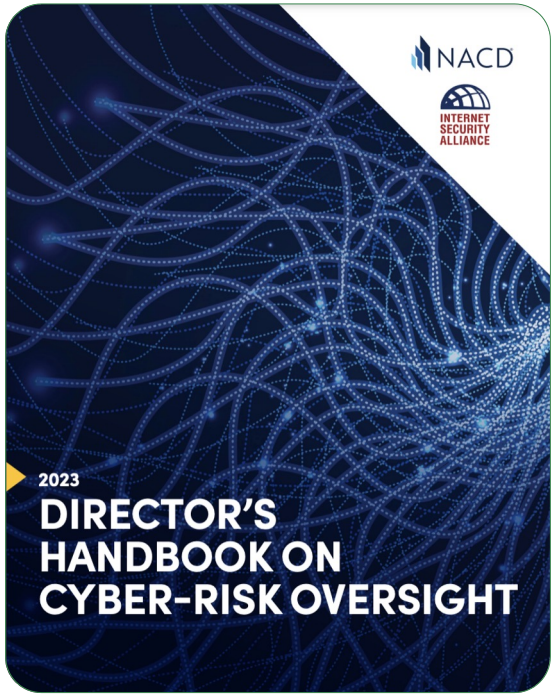
**5** Board-management discussions about cyber risk should include identification and **quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance,** as well as specific plans associated with each approach.



# Cyber Risk And The Board: National Assoc Corporate Directors 2023

**Board Members are seeing cybersecurity as a strategic risk**

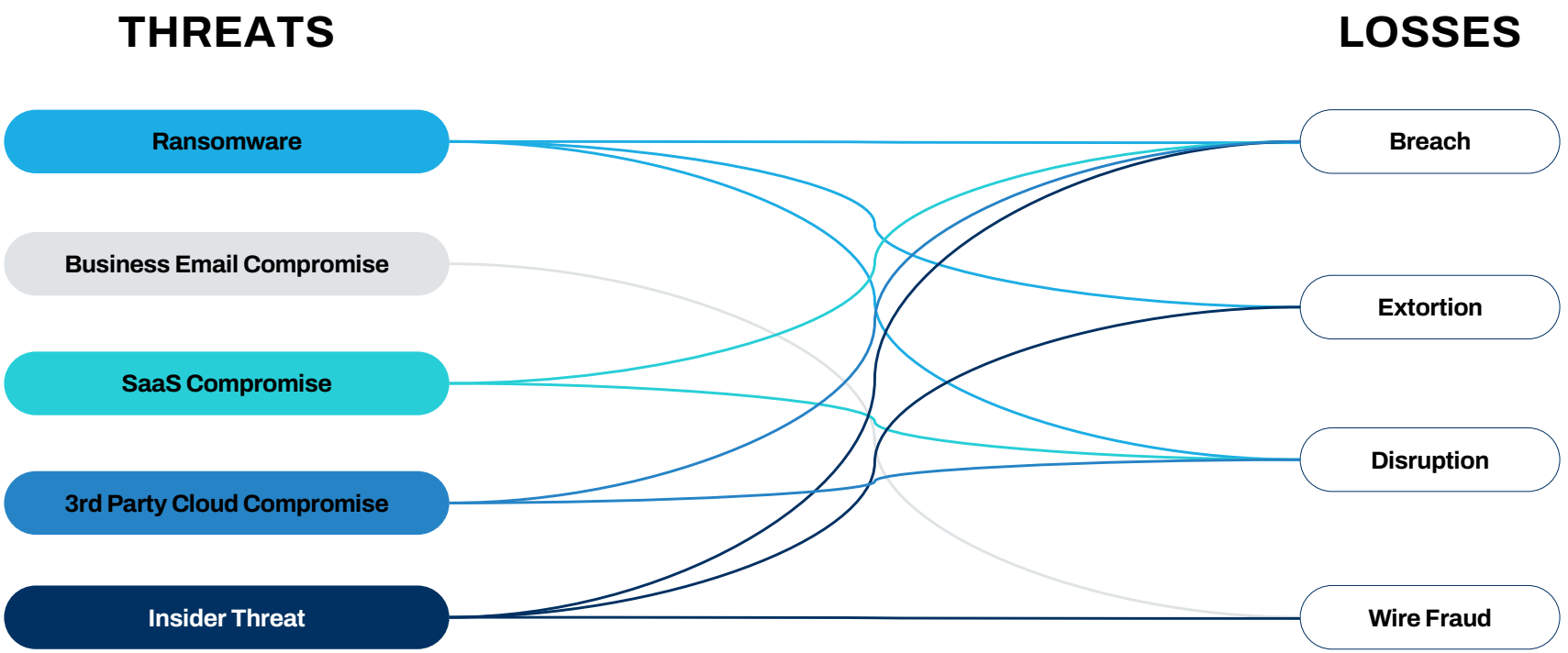
**6** Boards should encourage **systemic resilience** through collaboration with their industry and government peers and encourage the same from their management teams.



# The Components That Drive Enterprise Cyber Budgets

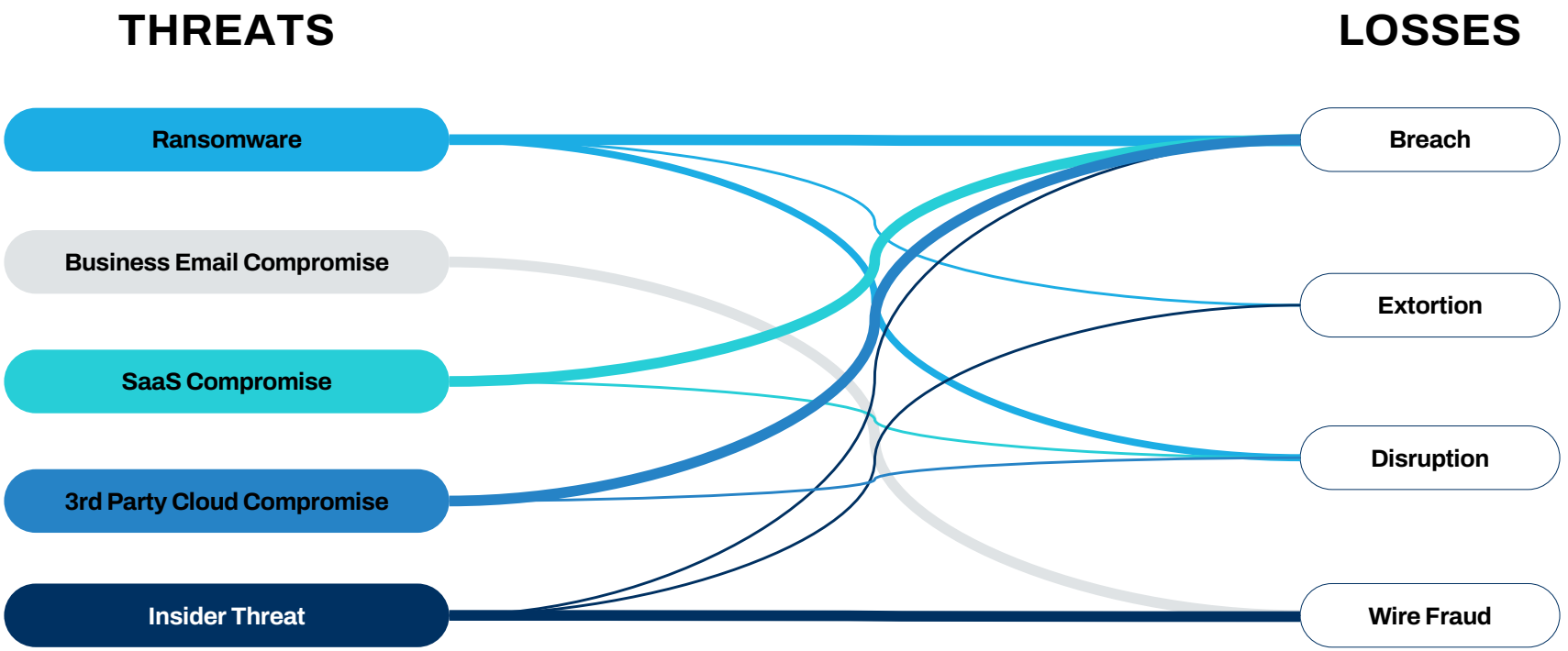
**Quantifying Risk Surface**

# Risk Surface Defined



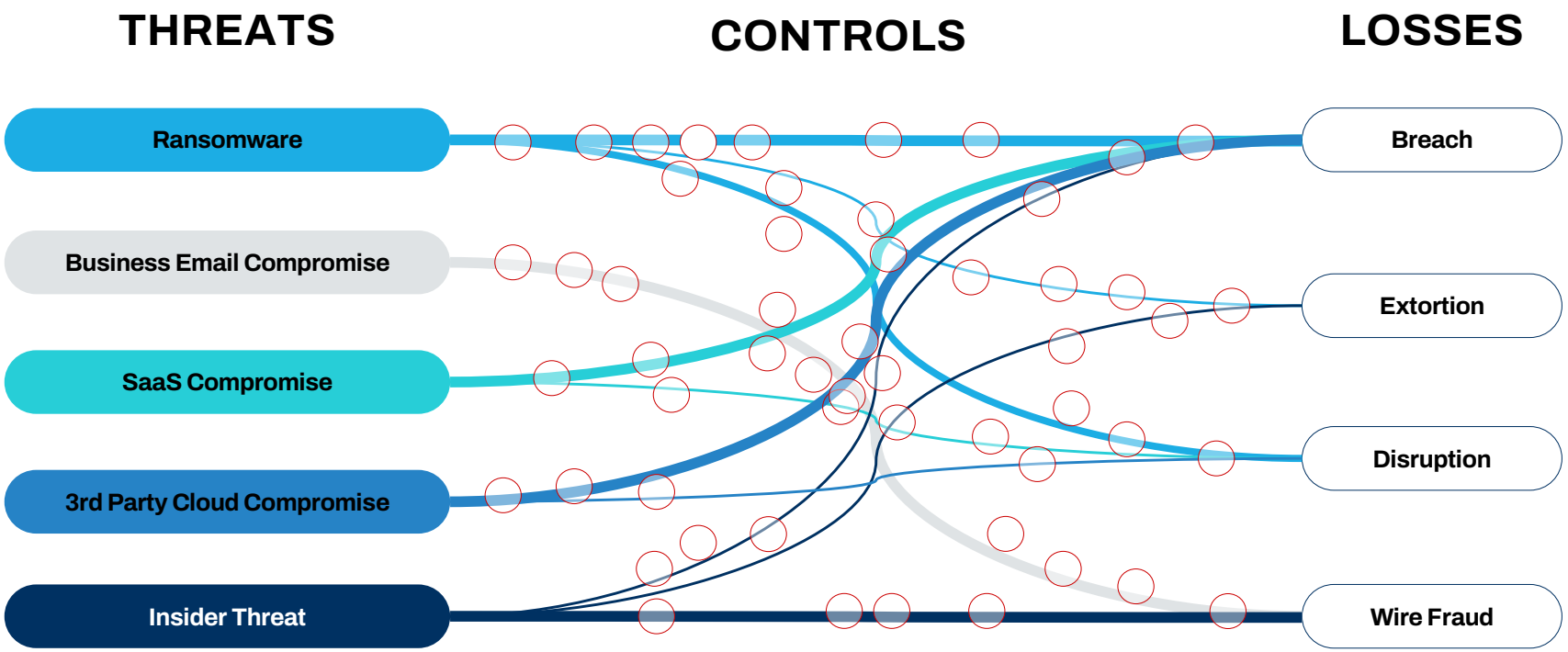
# Risk Surface Defined

## Focusing On What's Most Plausible



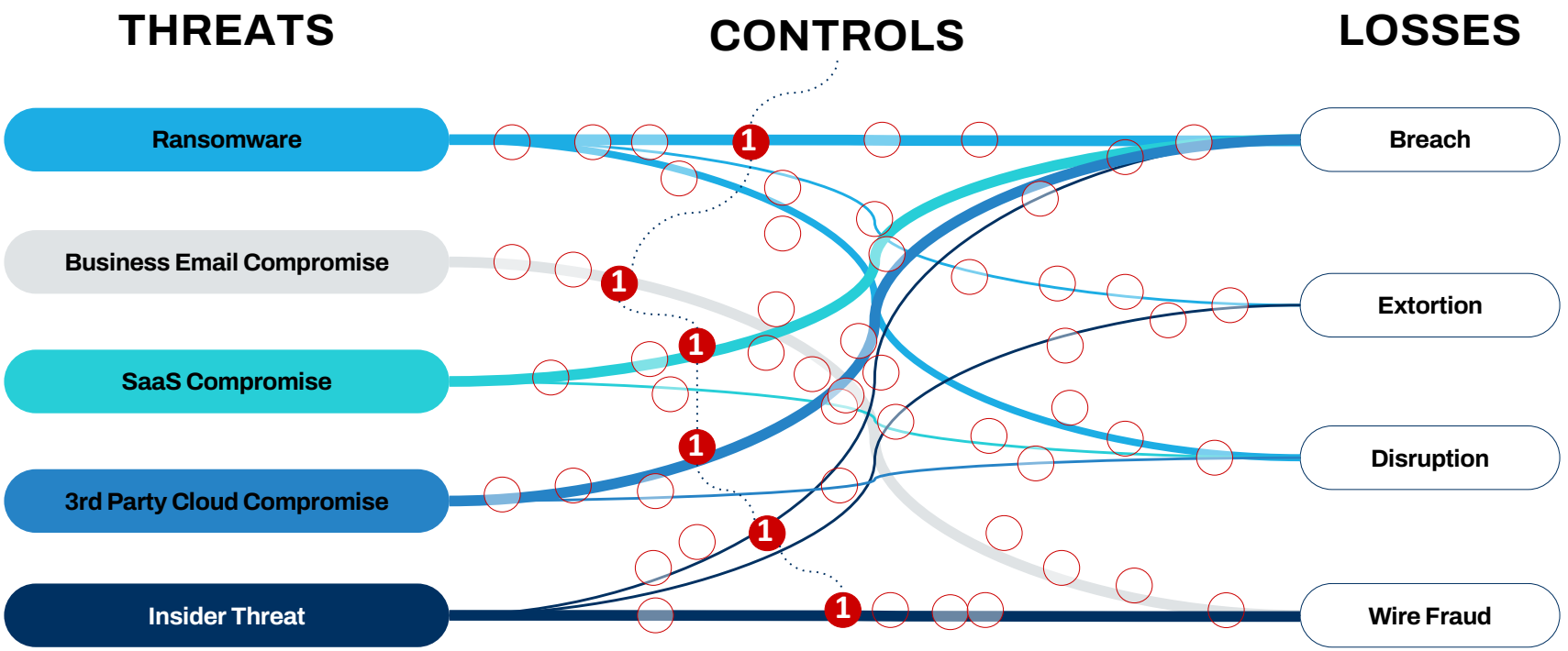
# Risk Surface Defined

## Which Strategic Security Initiatives Come First?



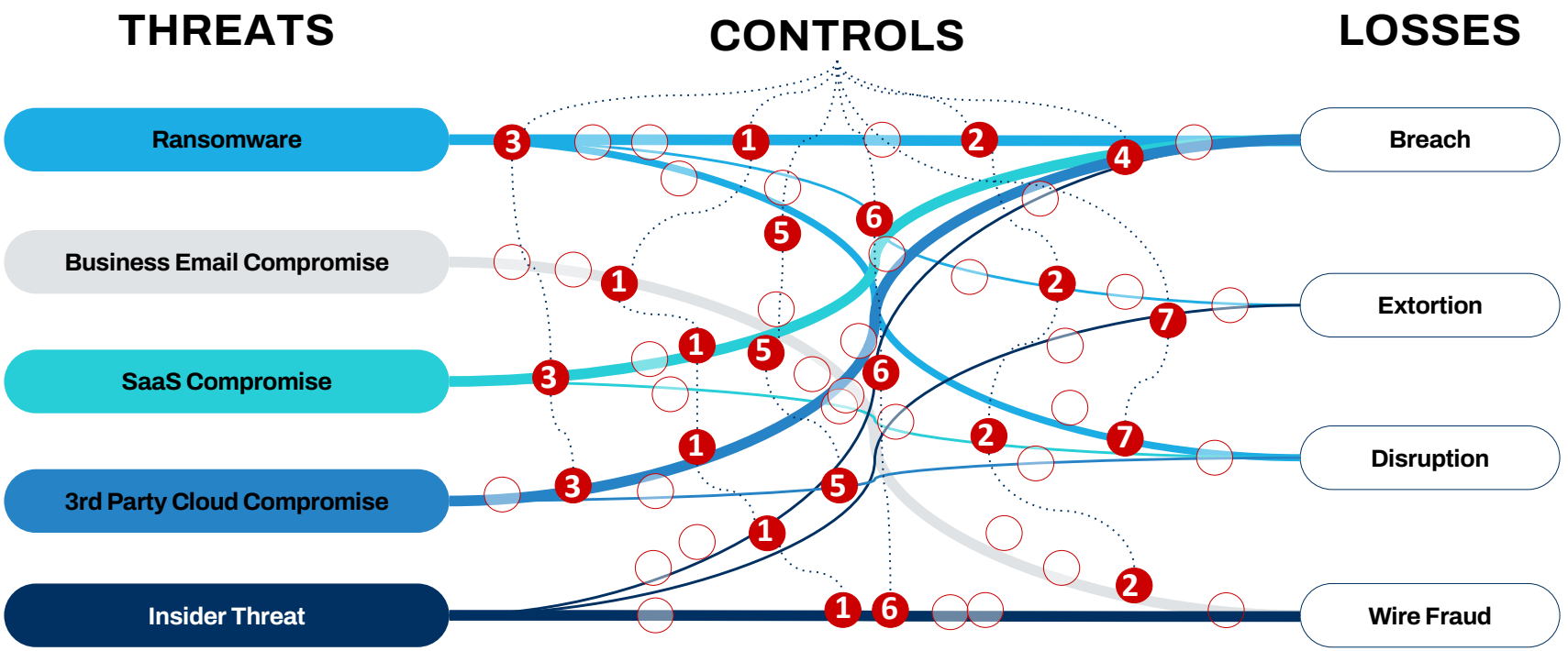
# Risk Surface Defined

## Which Strategic Security Initiatives Come First?



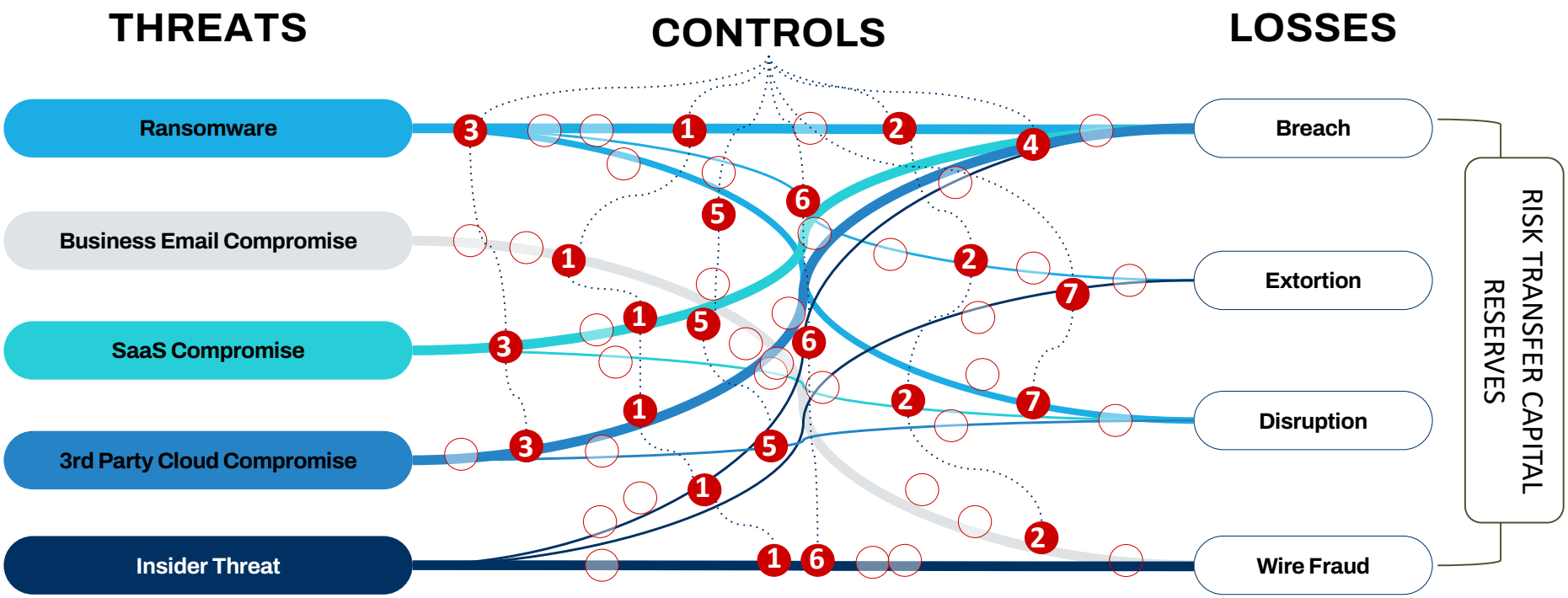
# Risk Surface Defined

## Which Strategic Security Initiatives Come First?



# Risk Surface Defined

## Which Strategic Security Initiatives Come First?



# Quantifying Risk Surface Is Manageable


Records

Time

Revenue

Potential

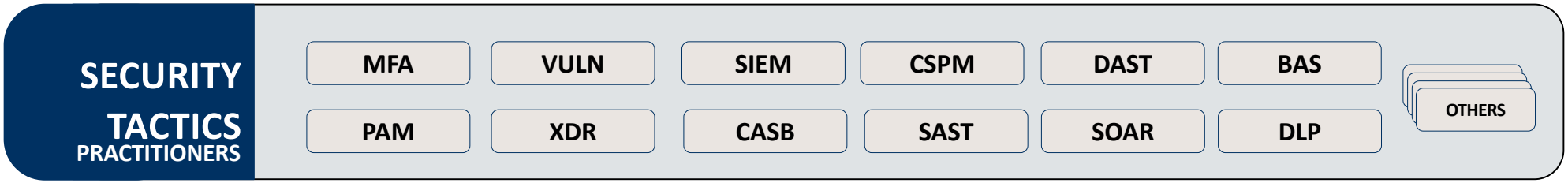
Expected

Example Rapid Risk Assessment Summary

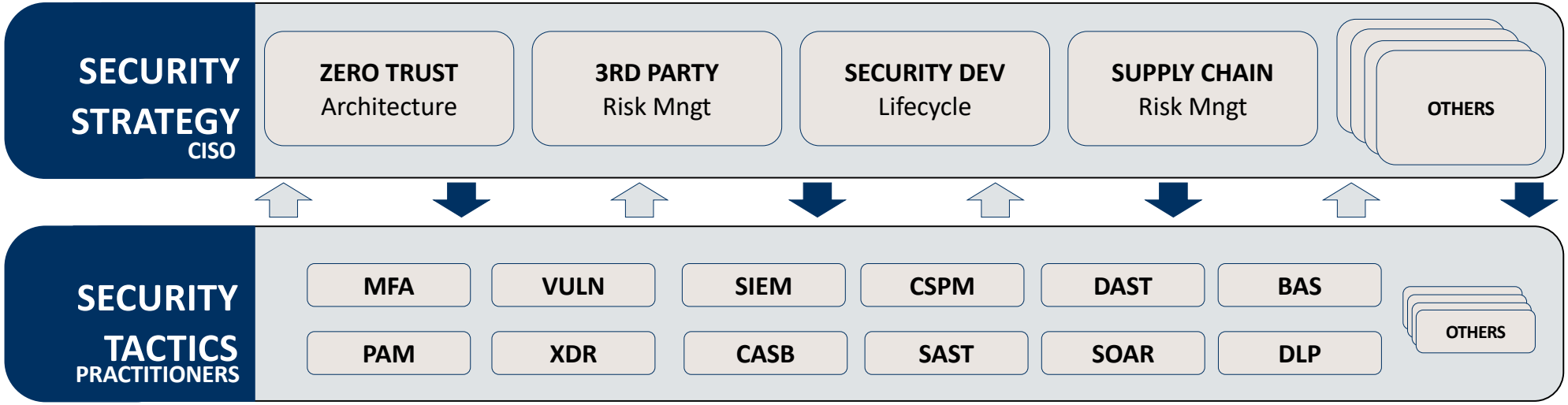
| Peril | Loss Ranges | | | Impact | | Assessed Orgs | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 10% Low | Median | 90% High | Mean Event Loss | Yearly Expected Losses | CIO | CTO | CFO | CMO | CRO | CISO | OTHER |
| Ransomware Breach | $2.9M | $20.3M | $29M | $17.7M | $443K | ✓ | | | | | ✓ | |
| Ransomware Disruption | $1.7M | $4.9M | $13.4M | $6.5M | $165K | ✓ | | | | | ✓ | |
| Ransomware Extortion | $300K | $1.5M | $5M | $2.2M | $55K | ✓ | | | | | ✓ | |
| BEC Fraud | $200K | $2M | $5M | $2.4M | $60K | ✓ | | ✓ | | | ✓ | |
| Cloud Data Breach | $1.74M | $11.6M | $17.4M | $10M | $250K | ✓ | ✓ | | | | ✓ | |
| Cloud Disruption | $370K | $1.34M | $2.7M | $1.5M | $38K | ✓ | ✓ | | | | ✓ | |
| SaaS Data Breach | $290K | $1.2M | $5.8M | $2.3M | $57K | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| SaaS Disruption | $1M | $4M | $6.5M | $3.9M | $100K | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| **Mean Event Total:** | | | | **$46.5M** | | | | | | | | |
| **Total Expected Yearly Losses:** | | | | | **$1.2M** | | | | | | | |

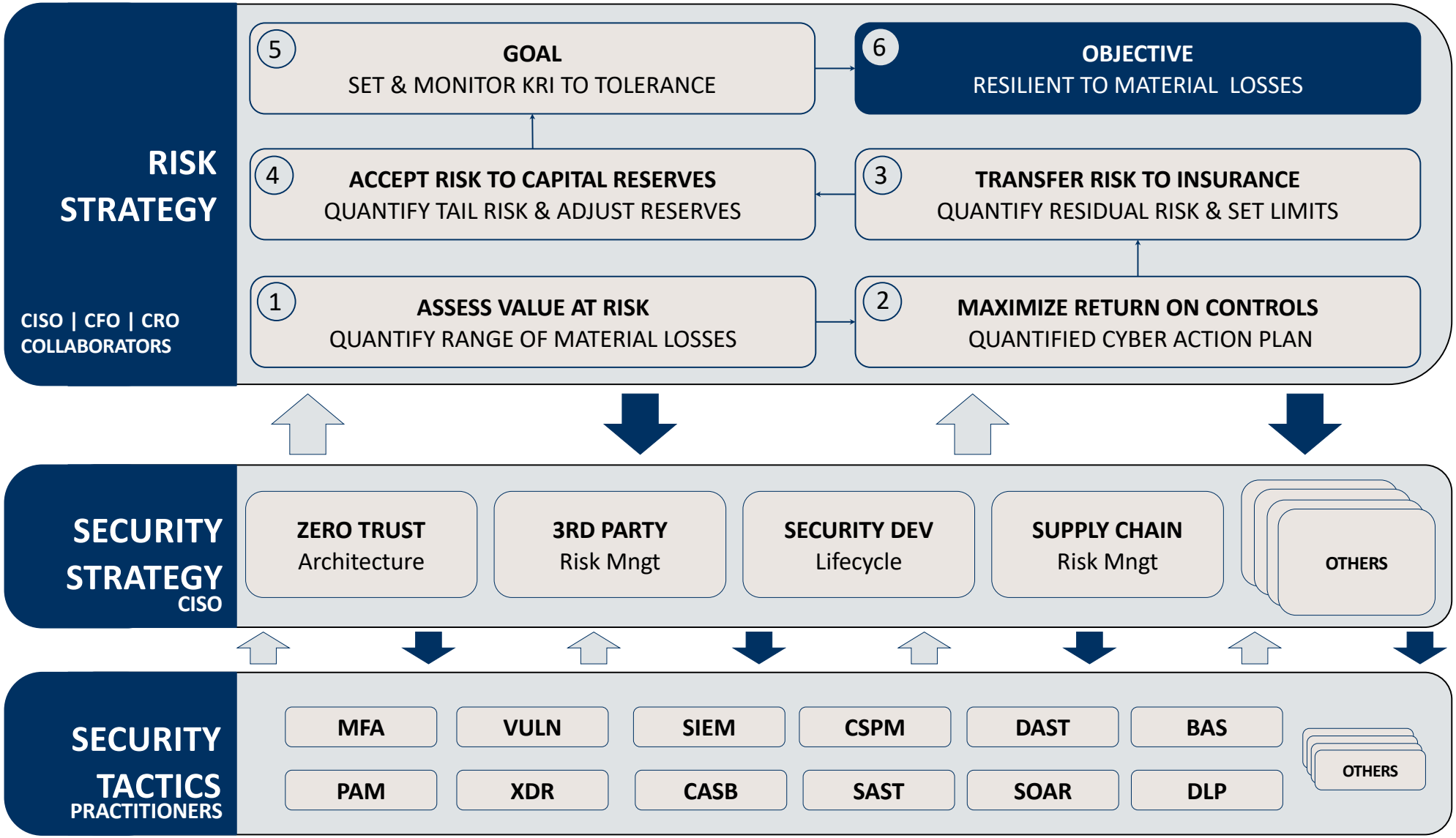
RISK AWARENESS WEEK 2023
Join The Global Initiative To Promote Risk Based Decision Making

# From Risk Surface To Security Strategy



# From Risk Surface To Security Strategy



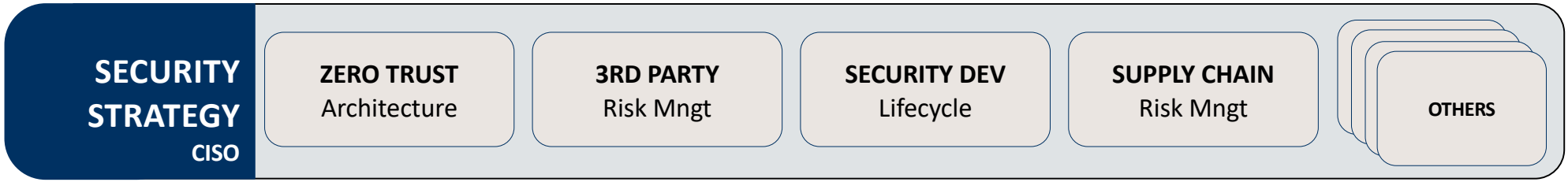

RISK STRATEGY
CISO | CFO | CRO COLLABORATORS
5
GOAL
SET & MONITOR KRI TO TOLERANCE
6
OBJECTIVE
RESILIENT TO MATERIAL LOSSES
4
ACCEPT RISK TO CAPITAL RESERVES
QUANTIFY TAIL RISK & ADJUST RESERVES
3
TRANSFER RISK TO INSURANCE
QUANTIFY RESIDUAL RISK & SET LIMITS
1
ASSESS VALUE AT RISK
QUANTIFY RANGE OF MATERIAL LOSSES
2
MAXIMIZE RETURN ON CONTROLS
QUANTIFIED CYBER ACTION PLAN
SECURITY STRATEGY
CISO
ZERO TRUST
Architecture
3RD PARTY
Risk Mngt
SECURITY DEV
Lifecycle
SUPPLY CHAIN
Risk Mngt
OTHERS
SECURITY TACTICS
PRACTITIONERS
MFA
VULN
SIEM
CSPM
DAST
BAS
PAM
XDR
CASB
SAST
SOAR
DLP
OTHERS

Building The Enterprise Budget

# For A Portfolio Of Strategic Initiatives

CyberResilience.com

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile



# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative |
| --- |
| Zero Trust Architecture |
| 3rd Party Risk Management |
| Supply Chain Risk Management |
| Security Development Lifecycle |
| SaaS Apps Risk Management |

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost |
|---|---|
| Zero Trust Architecture | $ 450,000 |
| 3rd Party Risk Management | $ 150,000 |
| Supply Chain Risk Management | $ 525,000 |
| Security Development Lifecycle | $ 415,000 |
| SaaS Apps Risk Management | $ 145,000 |

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

*Let me check my thesaurus…*

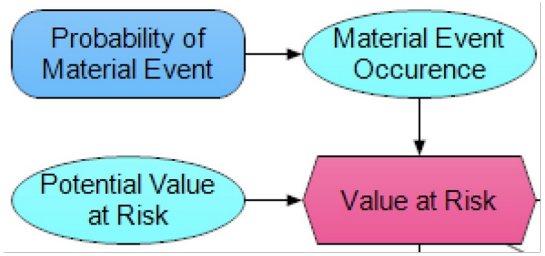
Expected Risk Removal =
Risk Weighted Avoided Loss =
Risk Weighted Net Benefit =
Prior Expected Loss - Targeted Expected Loss

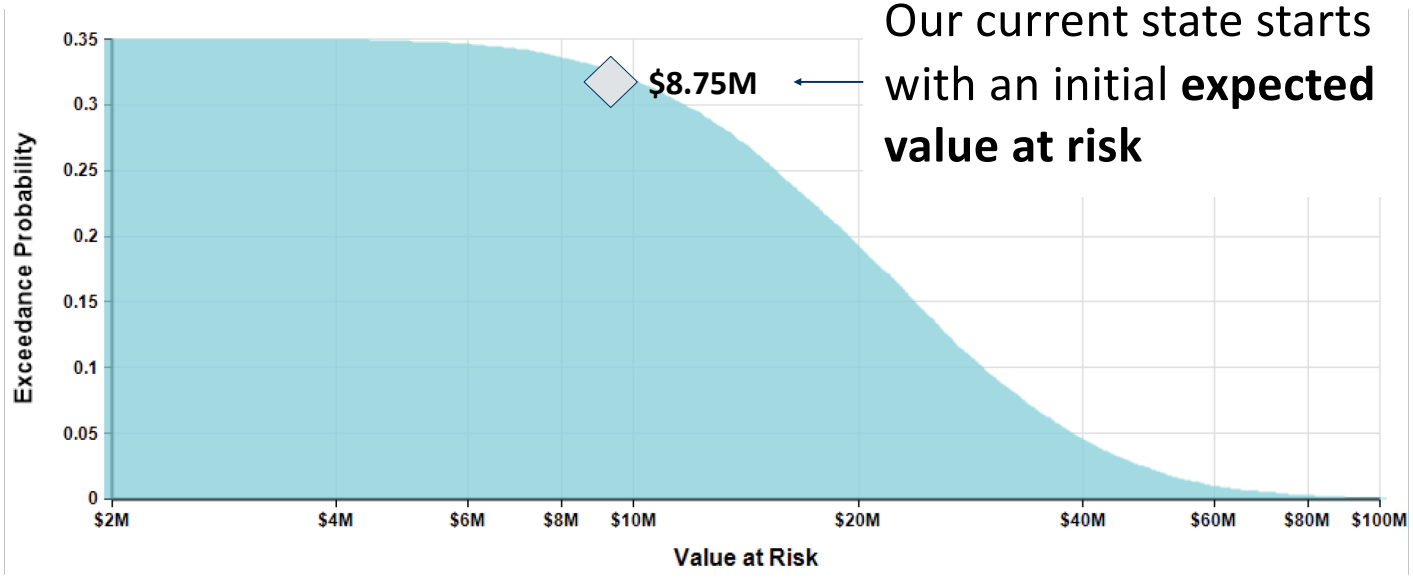
Peter M. Roget

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

Expected Value at Risk = Pr(Material Event) * Avg(Potential Value at Risk)



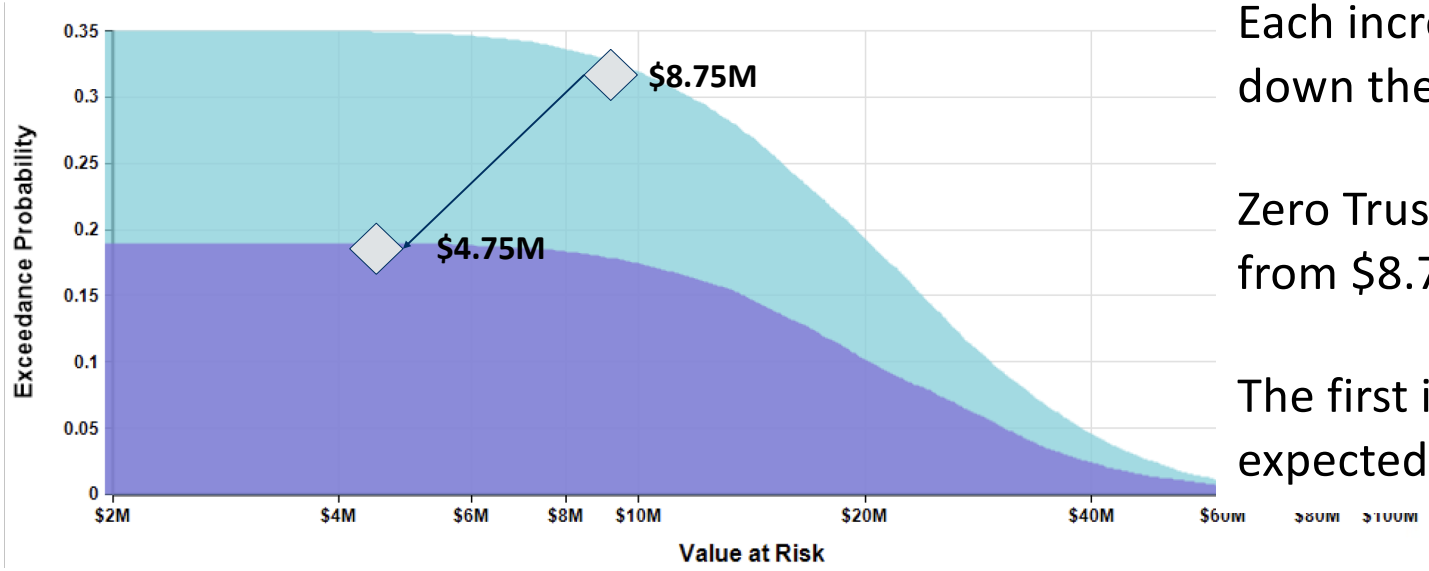




Our current state starts with an initial **expected value at risk**

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

Expected Value at Risk = Pr(Material Event) * Avg(Potential Value at Risk)




Each incremental initiative buys down the expected value at risk.

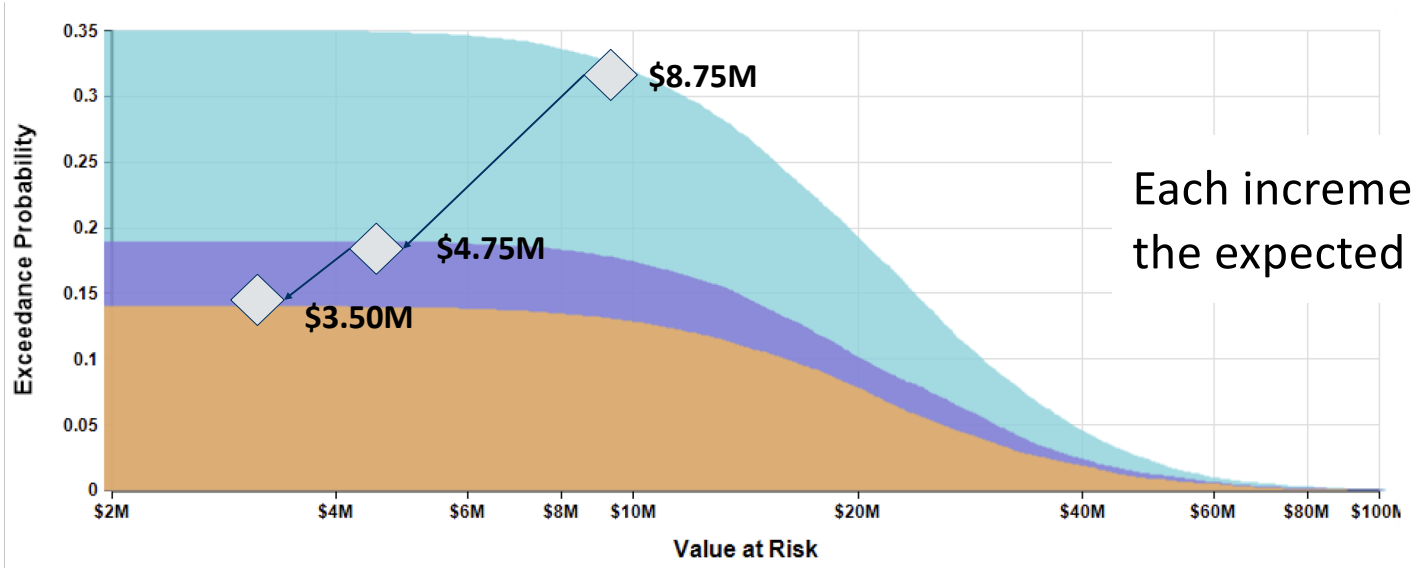
Zero Trust Architecture moves us from $8.75M to $4.75M.

The first initiative yields an expected risk removal of $4.0M

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

Expected Value at Risk = Pr(Material Event) * Avg(Potential Value at Risk)

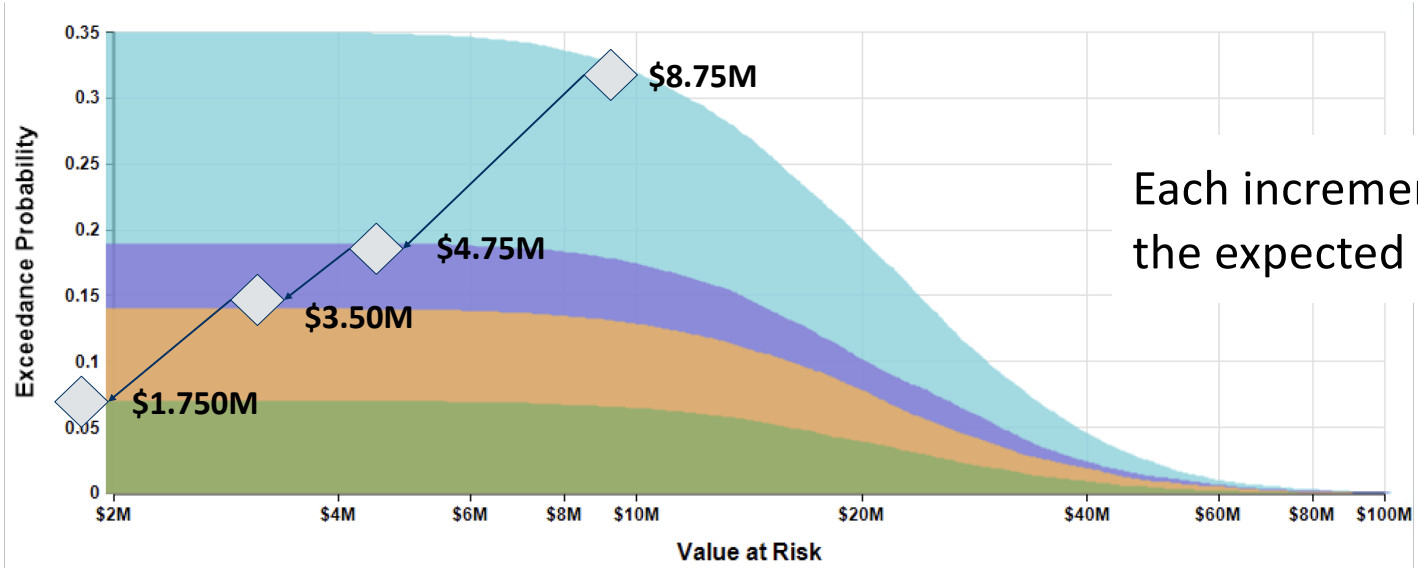



Each incremental initiative buys down the expected value at risk.

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

Expected Value at Risk = Pr(Material Event) * Avg(Potential Value at Risk)

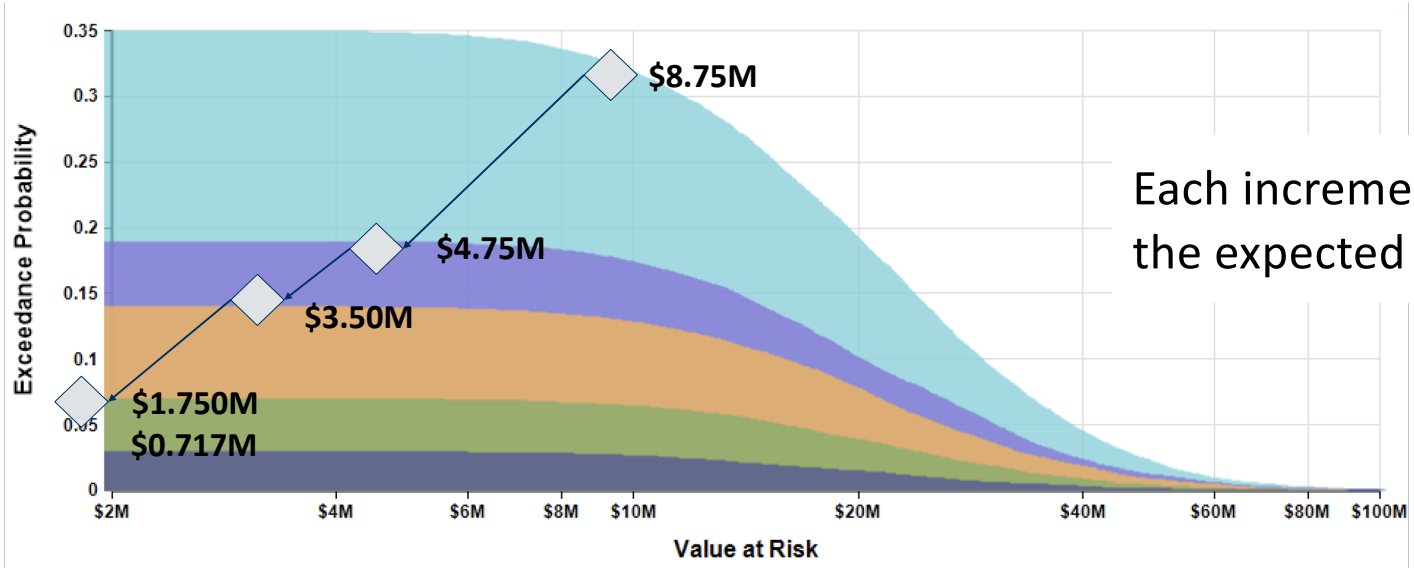



Each incremental initiative buys down the expected value at risk.

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

Expected Value at Risk = Pr(Material Event) * Avg(Potential Value at Risk)

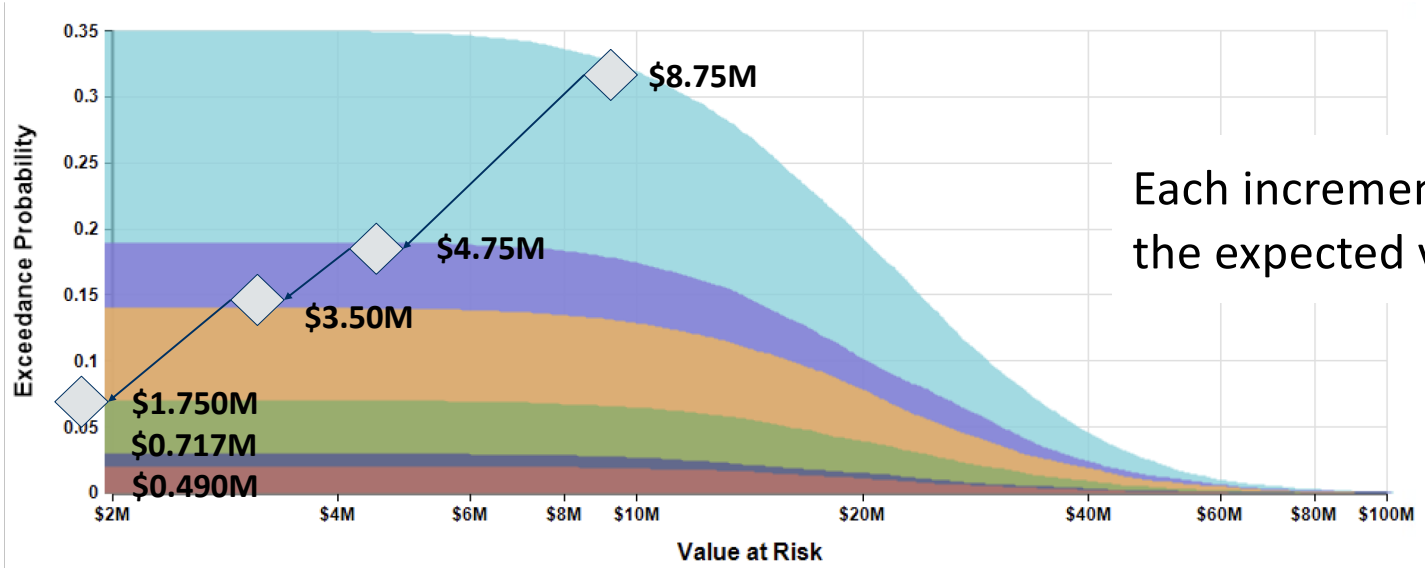



Each incremental initiative buys down the expected value at risk.

# Think about the Security Strategy as a Portfolio of Strategic Initiatives Coordinated to Reduce Risk Profile

| Strategic Initiative | Incremental Cost | Expected Risk Removal |
|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 |

Expected Value at Risk = Pr(Material Event) * Avg(Potential Value at Risk)




Each incremental initiative buys down the expected value at risk.

Calculate the **Bang For Your Buck** of each initiative

| Strategic Initiative | Incremental Cost | Expected Risk Removal | Return on Strategic Initiative |
|---|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 | 789% |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 | 733% |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 | 233% |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 | 141% |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 | 59% |

Sort

Return on Initiative = (Expected Risk Removal - Incremental Cost) / Incremental Cost

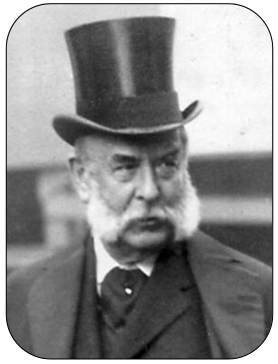
= (Expected Risk Removal / Incremental Cost) - 1

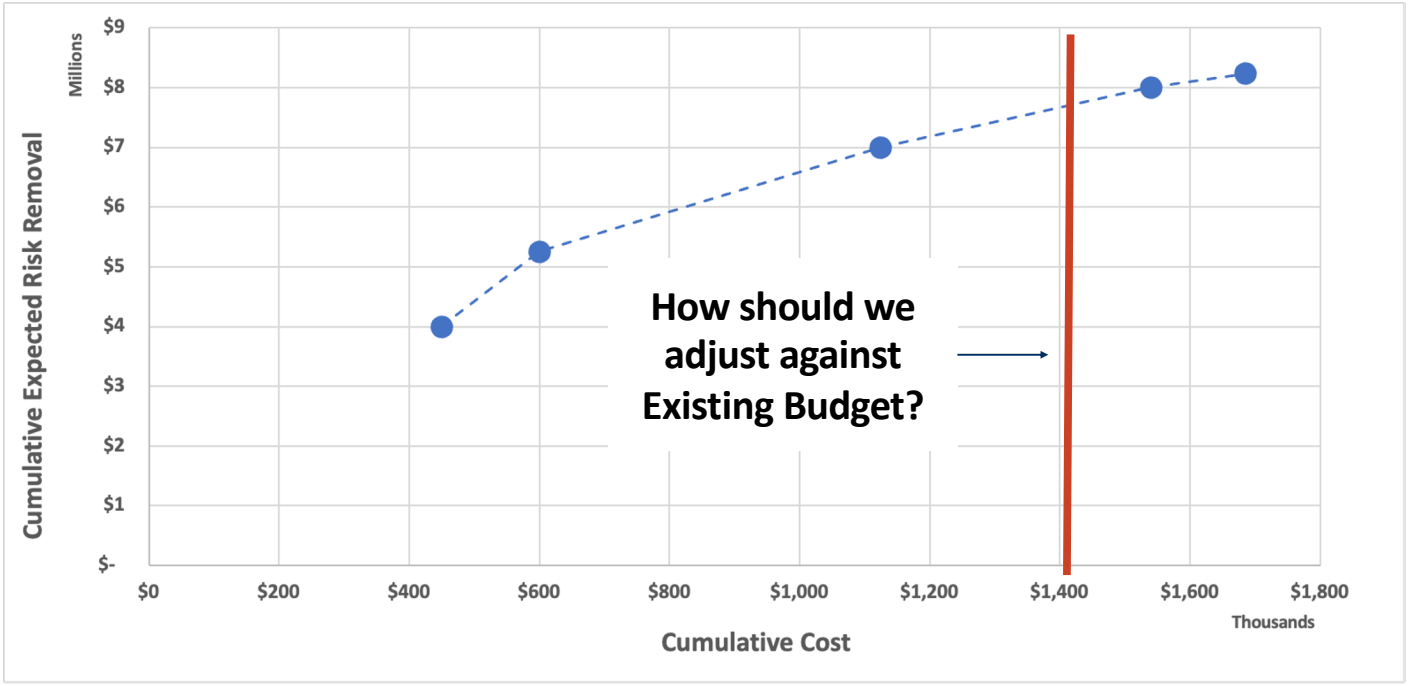
Bang For Your Buck is a measure of capital efficiency, an essential metric to establish the defensible security budget.

# A CFO Chart tells us where our cumulative #BFYB slows down

| Strategic Initiative | Incremental Cost | Expected Risk Removal | Return on Strategic Initiative | Cumulative Cost | Cumulative Expected Risk Removal |
|---|---|---|---|---|---|
| Zero Trust Architecture | $ 450,000 | $ 4,000,000 | 789% | $ 450,000 | $ 4,000,000 |
| 3rd Party Risk Management | $ 150,000 | $ 1,250,000 | 733% | $ 600,000 | $ 5,250,000 |
| Supply Chain Risk Management | $ 525,000 | $ 1,750,000 | 233% | $ 1,125,000 | $ 7,000,000 |
| Security Development Lifecycle | $ 415,000 | $ 1,000,000 | 141% | $ 1,540,000 | $ 8,000,000 |
| SaaS Apps Risk Management | $ 145,000 | $ 230,000 | 59% | $ 1,685,000 | $ 8,230,000 |

I love this chart. But I bet you're going to ask for more budget…

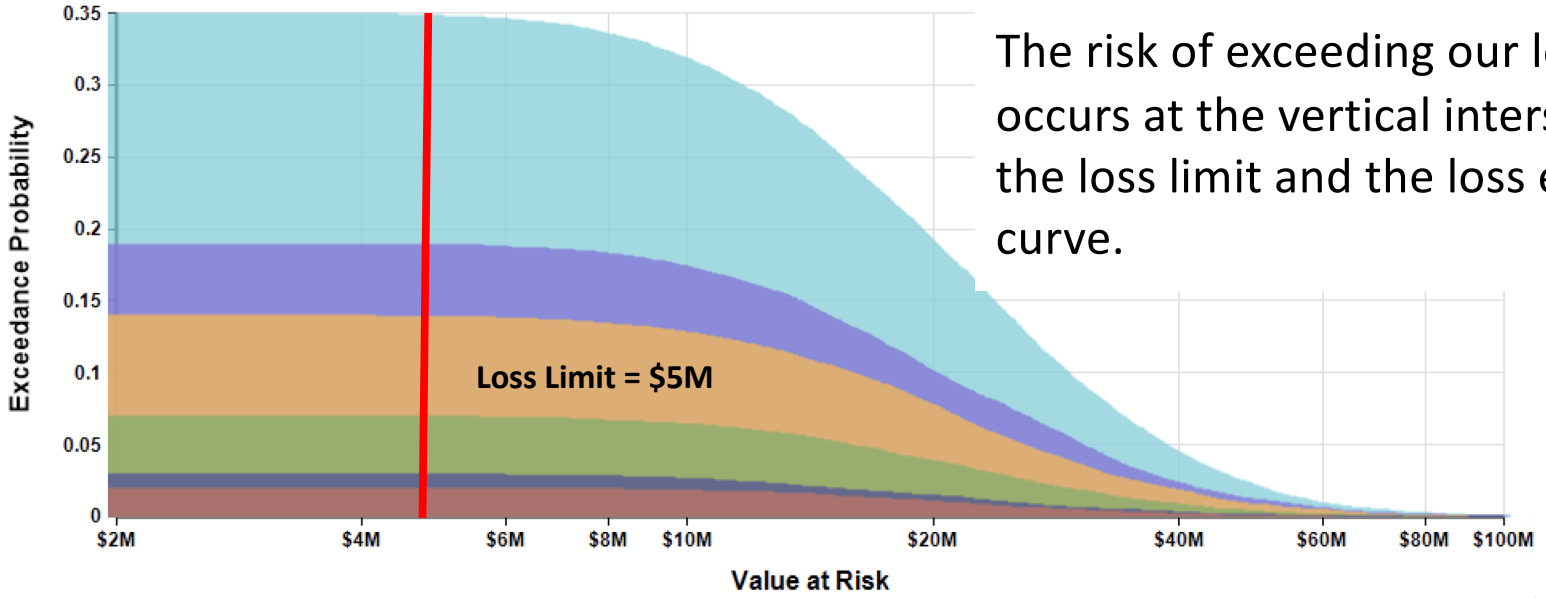





RISK AWARENESS WEEK 2023
Join The Global Initiative To Promote Risk Based Decision Making

# We should observe how each initiative buys down threat to our capital reserves as we plan to achieve them

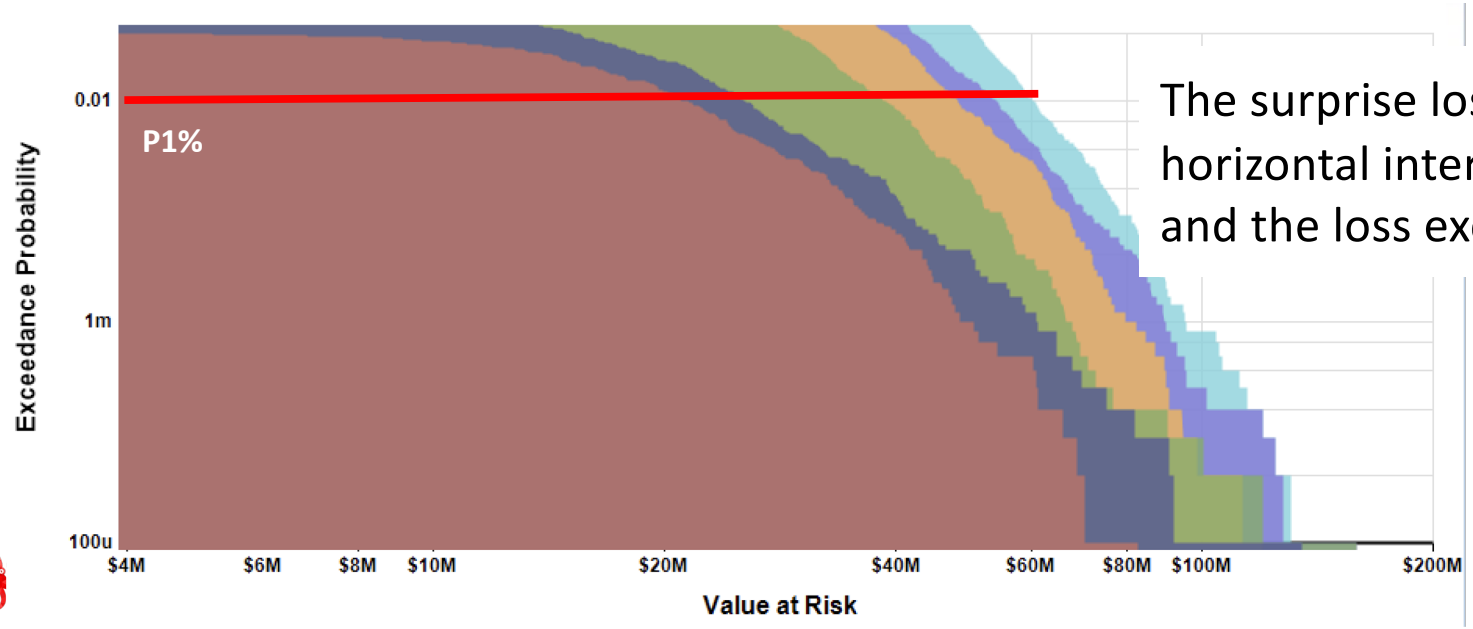
| Strategic Initiative | Planned Start Date | Duration [months] | Planned End Date | Risk of Exceeding Loss Limit |
|---|---|---|---|---|
| Zero Trust Architecture | 8/16/24 | 6 | 2/12/25 | 19% |
| 3rd Party Risk Management | 9/17/24 | 6 | 3/16/25 | 14% |
| Supply Chain Risk Management | 11/18/24 | 6 | 5/17/25 | 7% |
| Security Development Lifecycle | 12/19/24 | 6 | 6/17/25 | 3% |
| SaaS Apps Risk Management | 2/20/25 | 6 | 8/19/25 | 2% |




The risk of exceeding our loss limit occurs at the vertical intersection of the loss limit and the loss exceedance curve.

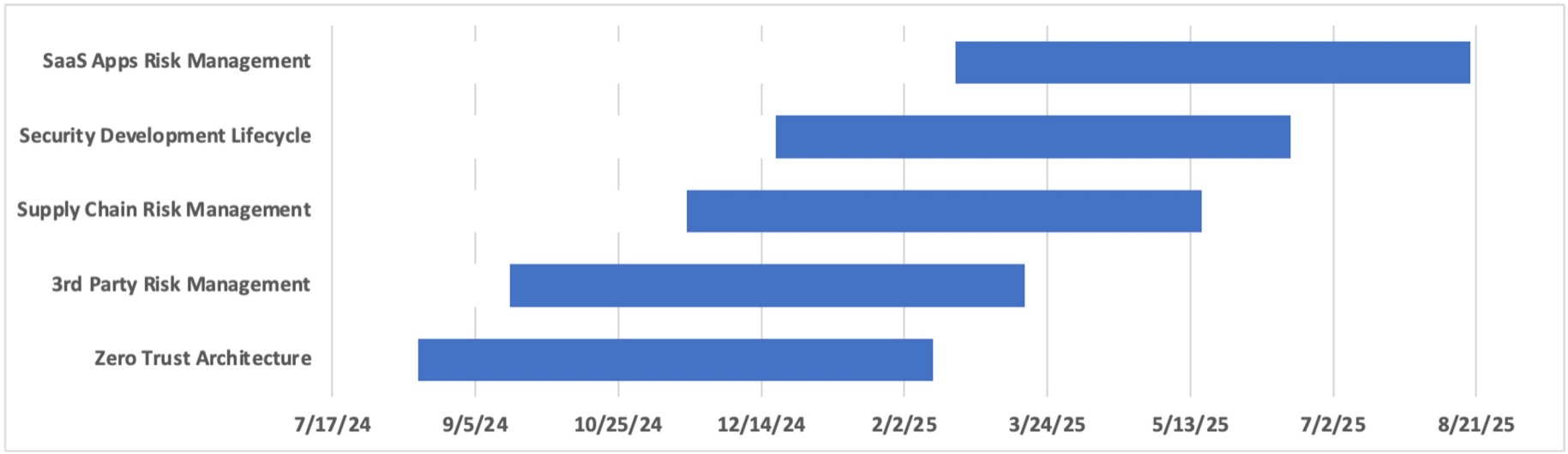
# We should observe how each initiative buys down threat to our capital reserves as we plan to achieve them

| Strategic Initiative | Planned Start Date | Duration [months] | Planned End Date | Risk of Exceeding Loss Limit | Surprise Loss |
|---|---|---|---|---|---|
| Zero Trust Architecture | 8/16/24 | 6 | 2/12/25 | 19% | $ 54,000,000 |
| 3rd Party Risk Management | 9/17/24 | 6 | 3/16/25 | 14% | $ 48,000,000 |
| Supply Chain Risk Management | 11/18/24 | 6 | 5/17/25 | 7% | $ 39,000,000 |
| Security Development Lifecycle | 12/19/24 | 6 | 6/17/25 | 3% | $ 25,000,000 |
| SaaS Apps Risk Management | 2/20/25 | 6 | 8/19/25 | 2% | $ 21,000,000 |

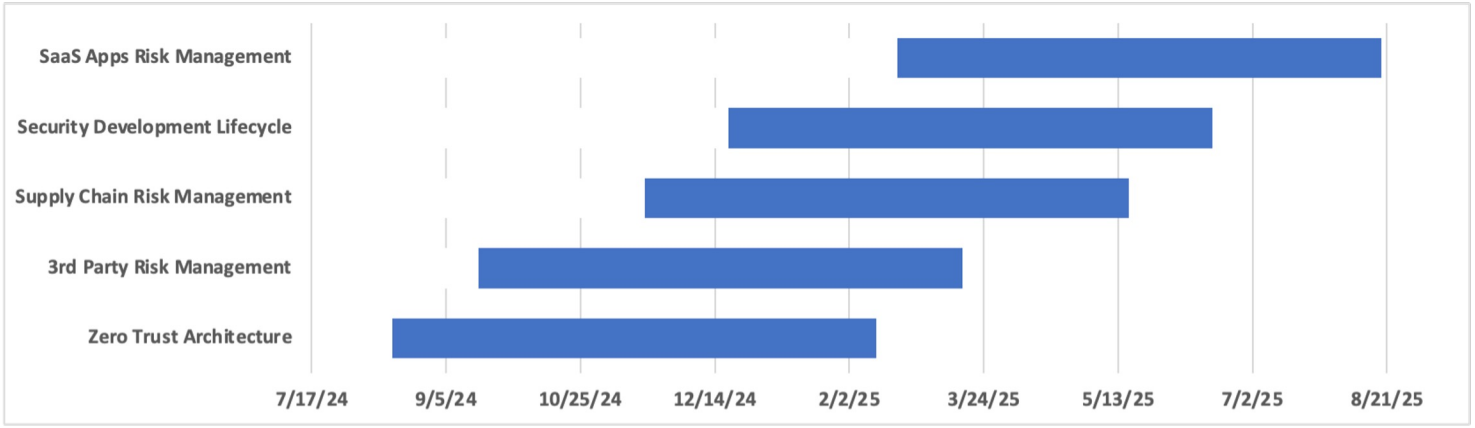


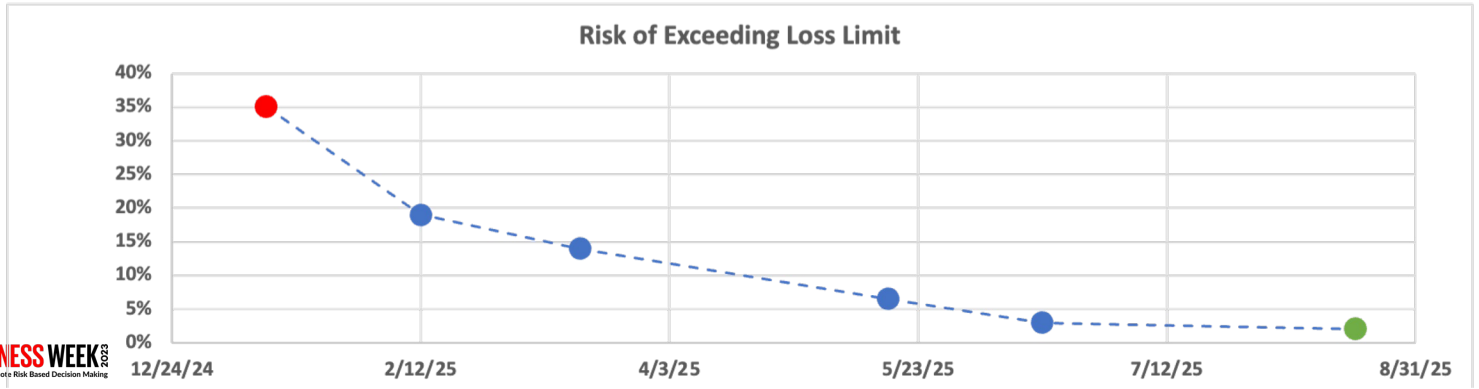

The surprise loss occurs at the horizontal intersection of the P1% and the loss exceedance curve.

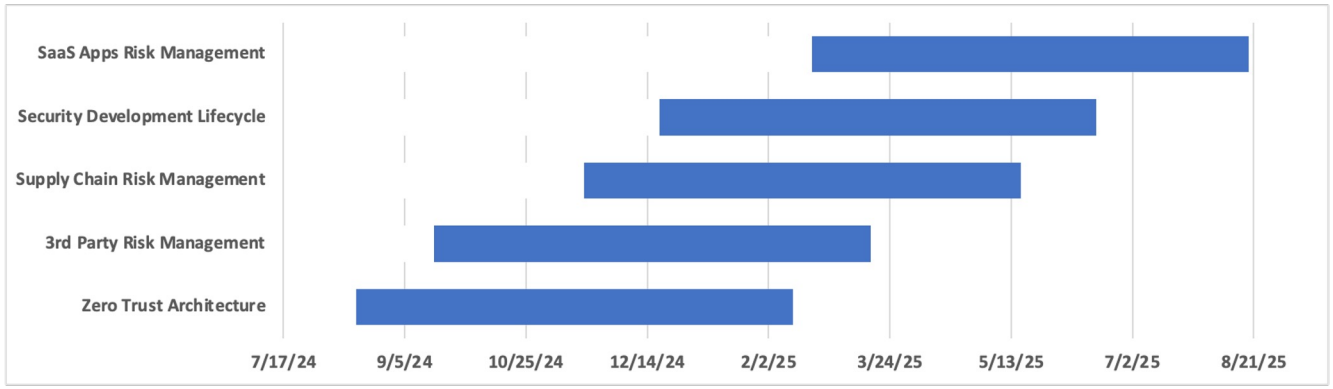
# We roll out capabilities based on how each buys down threat to our capital reserves as we plan to achieve them

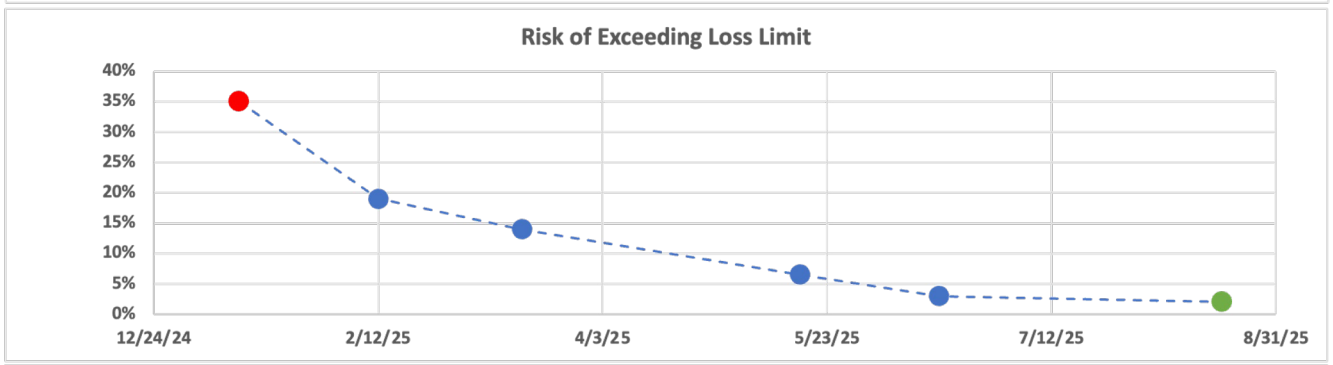


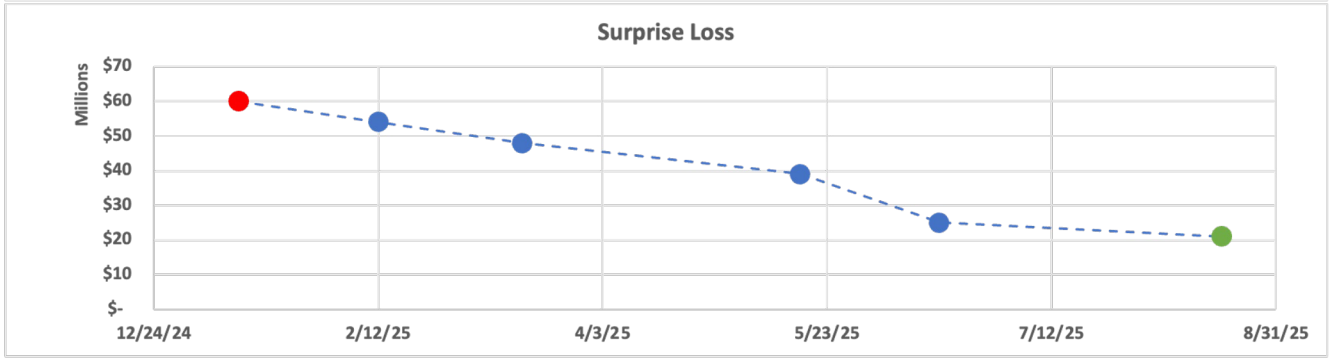
# We roll out capabilities based on how each buys down threat to our capital reserves as we plan to achieve them



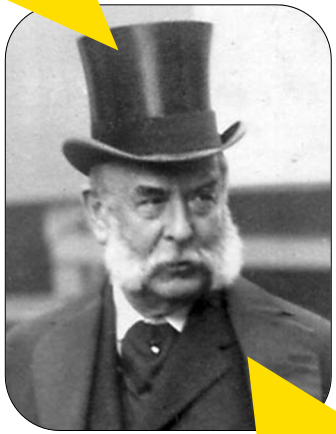






You're implementing initiatives in order of capital efficiency…



And showing me how we're buying down risk in the process!

# Thank you!

Questions or further dialogue? robbrown@cyberresilience.com