resilience

Building a Defensible Cybersecurity Budget

From Principles of **C**yber **R**isk **Q**uantification

Robert D. Brown III, Senior Director of Cyber Resilience

January 2025

What do we mean by Cyber Risk Quantification?

CRQ embodies a quantified approach to cybersecurity decision-making

- Evaluating the risk-informed potential losses to an organization through realized perils
- Accounting for costs of control and their reduction of the probability of realized losses
- Prioritizing controls based on net risk adjusted return

Defensible Budget

Thinking Like The Money People

You have to get inside their mind. You have to know what they want, need. You have to think... like a mouse!

How Might The Money People Define A Defensible Security Budget?

A **Defensible Security Budget** is a set of allocated costs that...

...serves the **Strategic Objectives** of the organization...

...based on a choice of controls that maximizes **Capital Efficiency** in an uncertain world.

How To Start Thinking Like The Money People

MAXIMIZE SHAREHOLDER VALUE

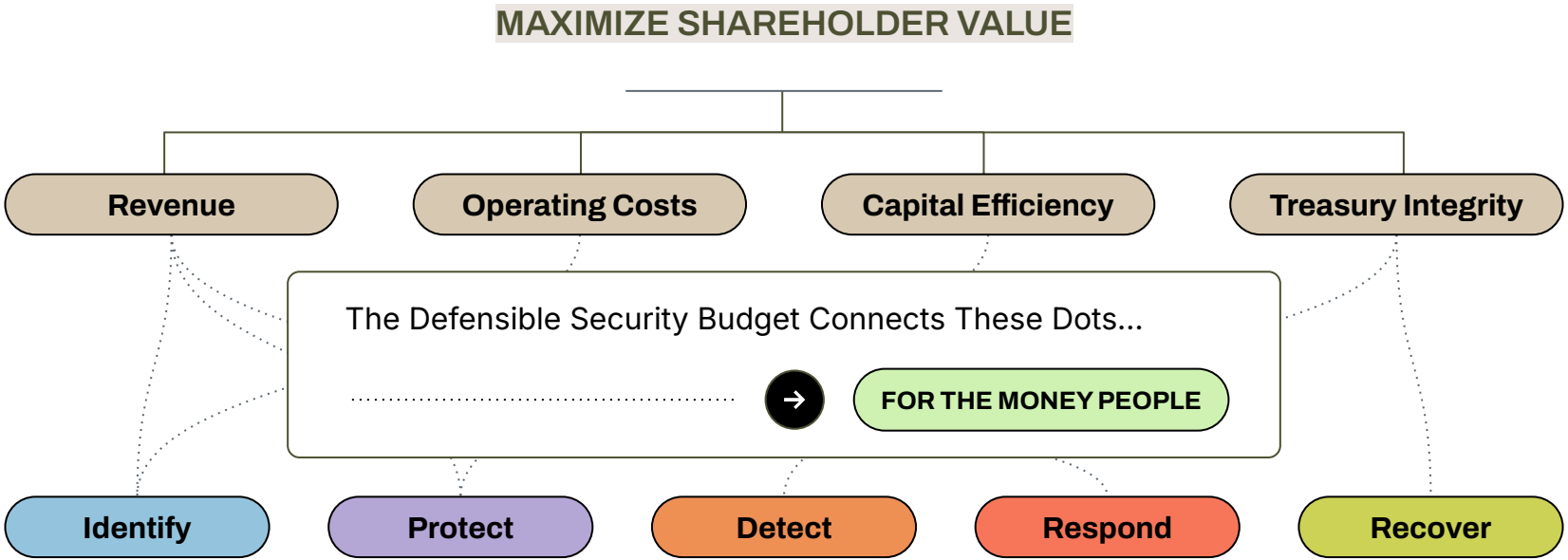
- **Revenue**

- **Operating Costs**

- **Capital Efficiency**

- **Treasury Integrity**

How To Start Thinking Like The Money People



How To Start Thinking Like The Money People

IDENTIFY

Value At Risk

Enable Threat Intelligence

Remediate Vulnerabilities

Segment Systems

Enable IAM

Protect Supply Chain

Maintain Business Continuity

Enable Business

Mitigate Threats

Achieve Compliance

Enable Trust

REVENUE

COSTS

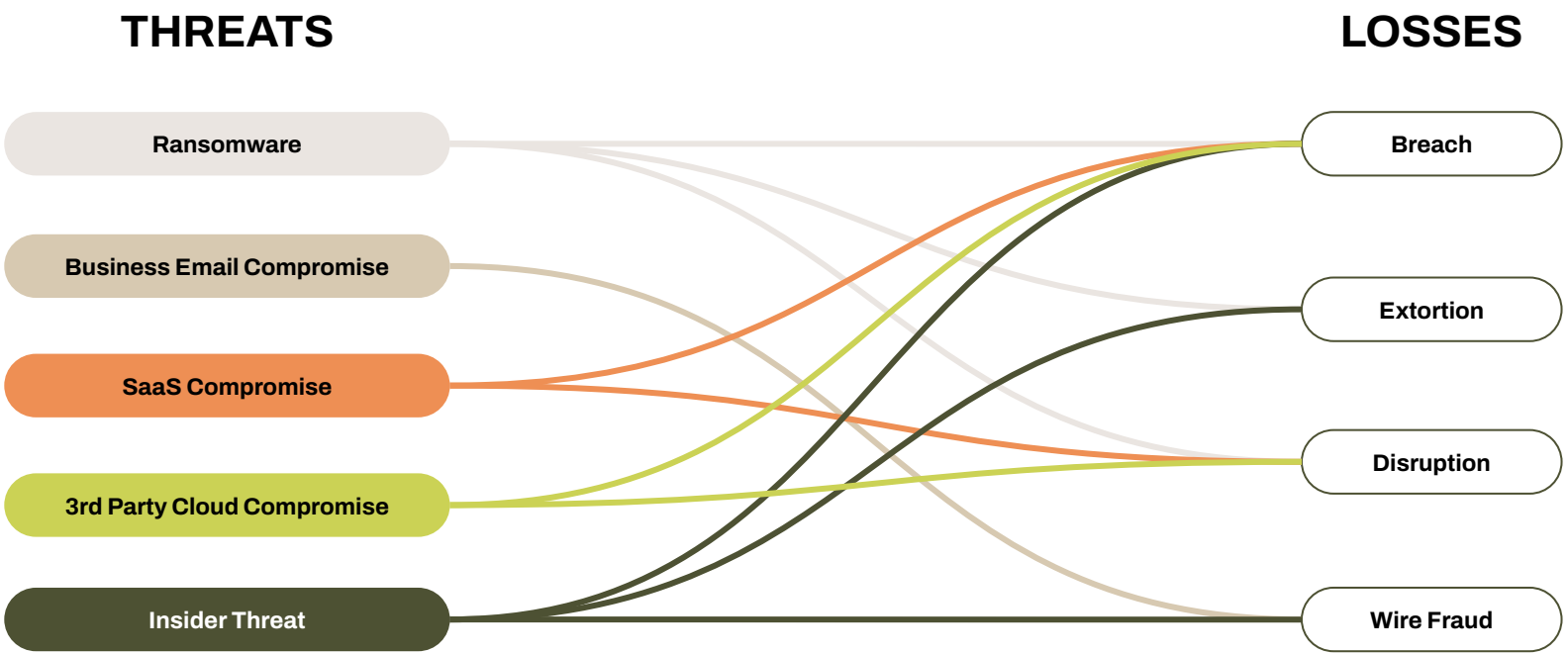
EFFICIENCY

TREASURY

Ok, I see how this connects to revenue and cost....

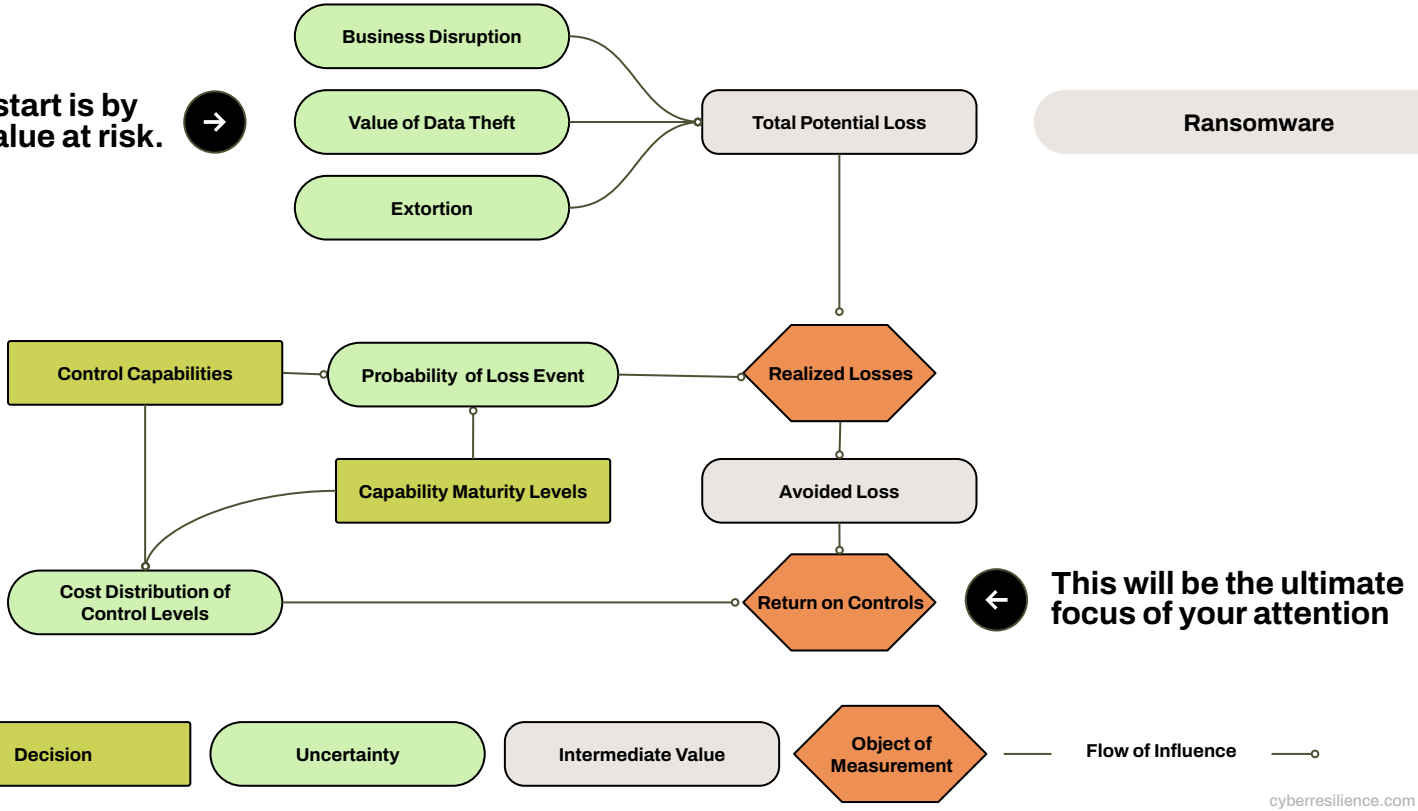
Now show me how this supports **capital efficiency** and **treasury!**

A Qualitative Approach To Quantitative Thinking



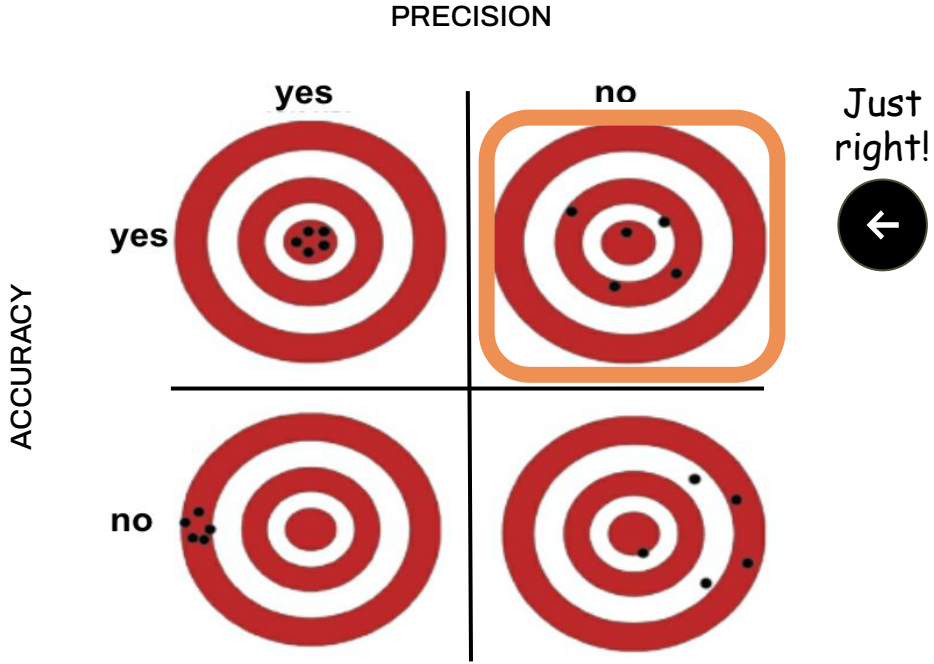
Influence Diagrams Value At Risk

A good place to start is by identifying the value at risk.



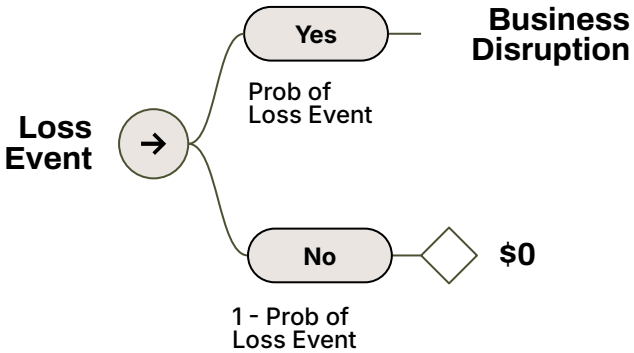
Converting Qualitative Influence Diagrams Into Quantitative Decision Trees

Aim for Goldilocks Level of Precision vs Accuracy



Just right!

Converting Qualitative Influence Diagrams
Into Quantitative Decision Trees



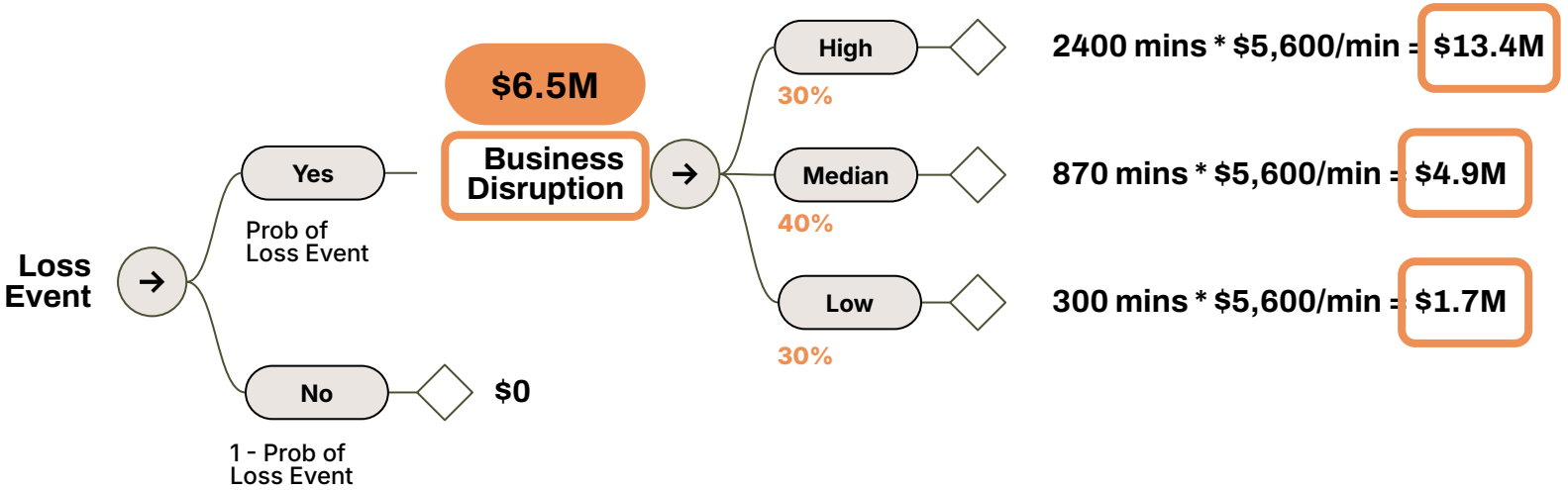
2400 mins * $5,600/min = $13.4M

870 mins * $5,600/min = $4.9M

300 mins * $5,600/min = $1.7M

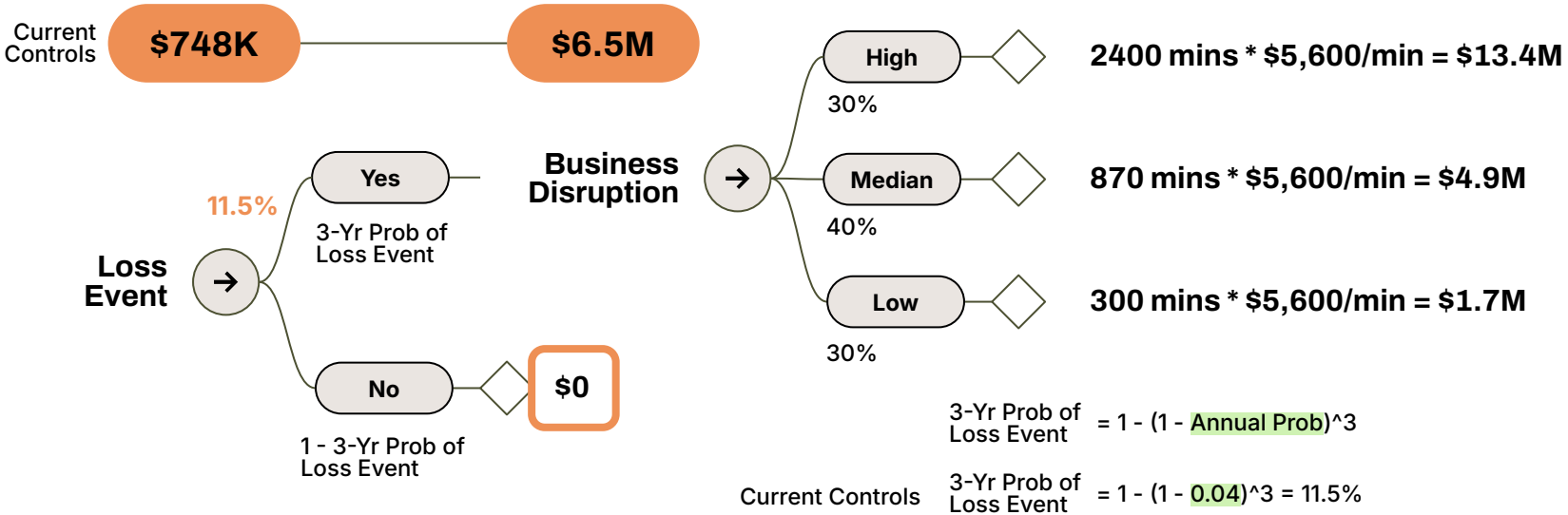
Converting Qualitative Influence Diagrams Into Quantitative Decision Trees

Mean Event Loss Of Business Disruption =



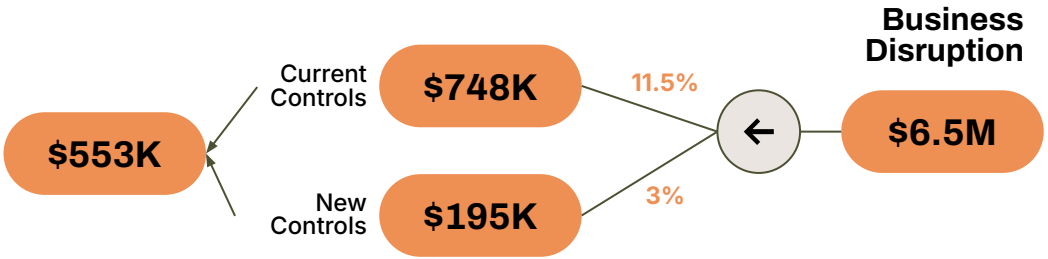
Calculate Current Expected Value of Loss

Expected Value Of Business Disruption =



Calculate Expected Value of Avoided Loss

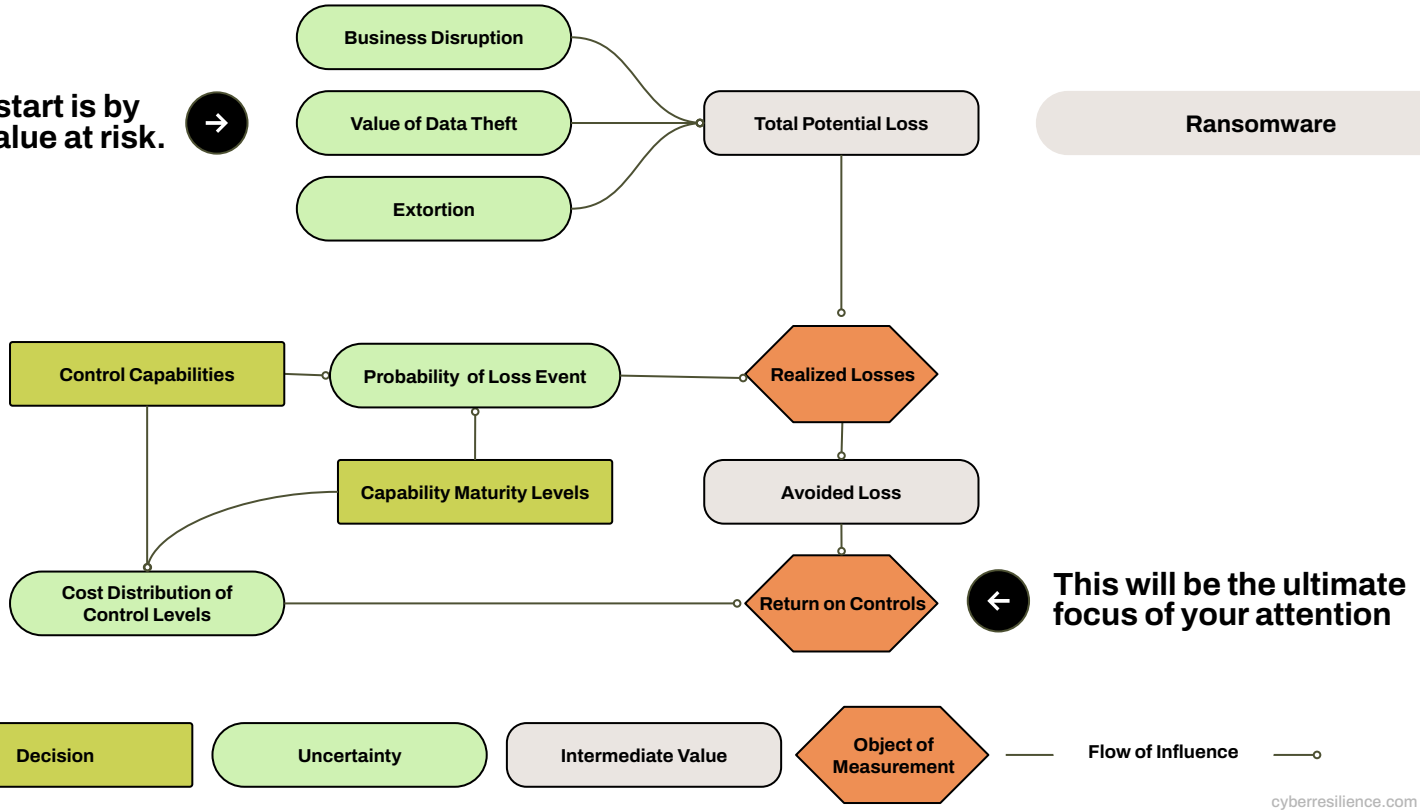
Expected Value Of Avoided Business Disruption = $748K - $195K = $553K



	3-Yr Prob of Loss Event	= 1 - (1 - Annual Prob)^3
Current Controls	3-Yr Prob of Loss Event	= 1 - (1 - 0.04)^3 = 11.5%
New Controls	3-Yr Prob of Loss Event	= 1 - (1 - 0.01)^3 = 3%

Repeat for Data Theft and Extortion

A good place to start is by identifying the value at risk.



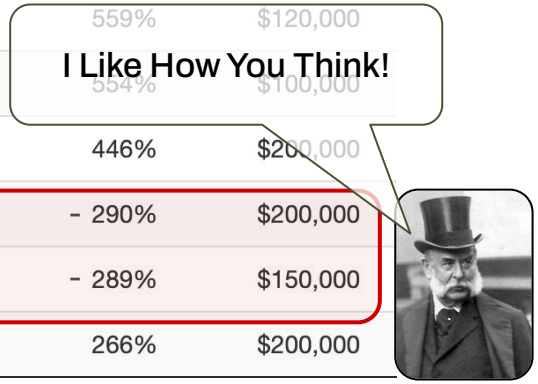
Calculate Return on Controls

ROC = [(Total Avoided Loss for All Perils / Cost of Control_i) - 1] * 100%

	Capability	Level	ROC	Cost
1	Identity Verification	MANAGED:MFA & PAM	658%	$140,000
2	Vulnerability Patch_SLA	MANAGED:30 Days Patch CRITCAL	559%	$120,000
3	Email Security	DEPLOYED:Email Security Gateway & Email Auth	554%	$100,000
4	Endpoint Protection	MANAGED:EPP & EDR	446%	$200,000
5	Network Segmentation	MANAGED:Micro-Segmentation	290%	$200,000
6	Security Training	MANAGED:Attack Simulations	289%	$150,000
7	Backup Security	MANAGED:Tested Backups	266%	$200,000

How To Start Thinking Like The Money People

	Capability	Level	EFFICIENCY ROC	COST Cost
1	Identity Verification	MANAGED:MFA & PAM	658%	$140,000
2	Vulnerability Patch_SLA	MANAGED:30 Days Patch CRITCAL	559%	$120,000
3	Email Security	DEPLOYED:Email Security Gateway & Email Auth	554%	$100,000
4	Endpoint Protection	MANAGED:EPP & EDR	446%	$200,000
5	Network Segmentation	MANAGED:Micro-Segmentation	- 290%	$200,000
6	Security Training	MANAGED:Attack Simulations	- 289%	$150,000
7	Backup Security	MANAGED:Tested Backups	266%	$200,000

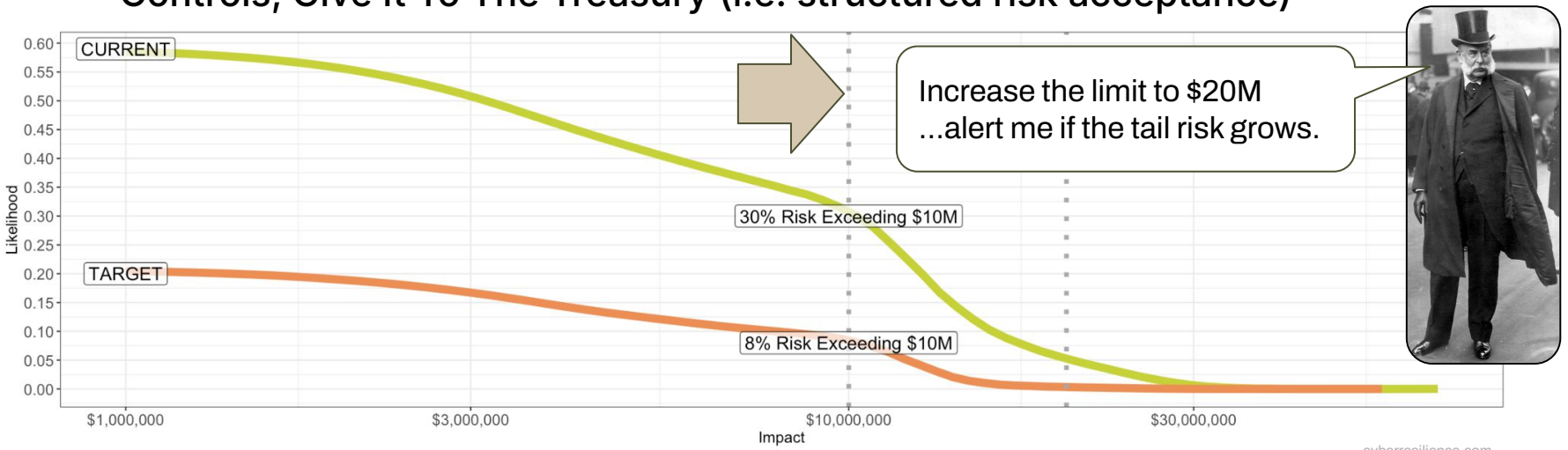


Non-Money People's Budget = $1.11M

Hero's Optimized Budget = $760K

How To Start Thinking Like The Money People

- The CURRENT line is before applying high ROI controls
- The TARGET line is after applying high ROI controls (from optimized budget)
- Losses beyond the LIMIT impact The Money People's TREASURY
- The money people have three STRATEGIC choices: More Limit, More Controls, Give It To The Treasury (i.e. structured risk acceptance)



Additional Resources to Guide Your Way

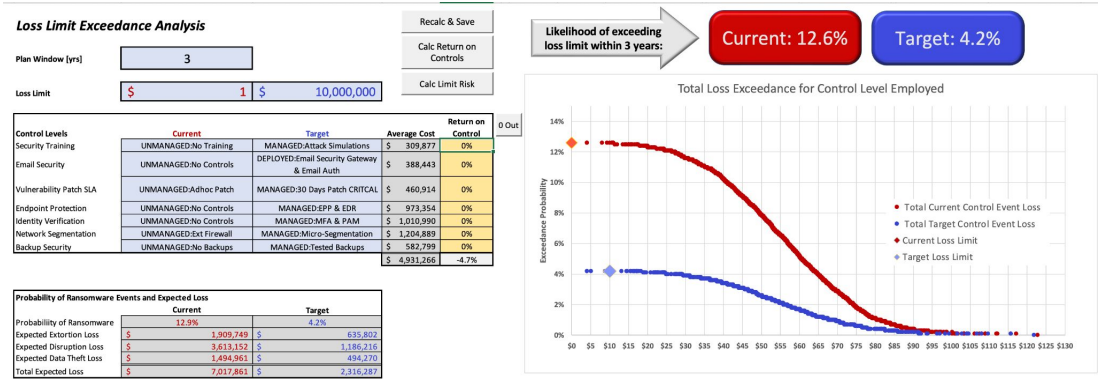
Workbook

→ cyberresilience.com

How To Do Rapid Risk Interviews

Since the publication of How To Measure Anything In Cybersecurity Risk, author and Resilience Chief Risk Officer Richard Seiersen has had the opportunity to consult with dozens of CISOs and their security teams. One thing he hears frequently is, **"how do I get started with the methods found in your book?"** This document written by Seiersen addresses that concern.

Ransomware Spreadsheet



Loss Limit Exceedance Analysis

Recalc & Save | Calc Return on Controls | Calc Limit Risk

Likelihood of exceeding loss limit within 3 years: Current: 12.6% | Target: 4.2%

Plan Window [yrs]	3	
Loss Limit	$ 1	$ 10,000,000

Control Levels	Current	Target	Average Cost	Return on Control
Security Training	UNMANAGED:No Training	MANAGED:Attack Simulations	$ 309,877	0%
Email Security	UNMANAGED:No Controls	DEPLOYED:Email Security Gateway & Email Auth	$ 388,443	0%
Vulnerability Patch SLA	UNMANAGED:Adhoc Patch	MANAGED:30 Days Patch CRITCAL	$ 460,914	0%
Endpoint Protection	UNMANAGED:No Controls	MANAGED:EPP & EDR	$ 973,354	0%
Identity Verification	UNMANAGED:No Controls	MANAGED:MFA & PAM	$ 1,010,990	0%
Network Segmentation	UNMANAGED:Ext Firewall	MANAGED:Micro-Segmentation	$ 1,204,889	0%
Backup Security	UNMANAGED:No Backups	MANAGED:Tested Backups	$ 582,799	0%
			$ 4,931,266	-4.7%

0 Out

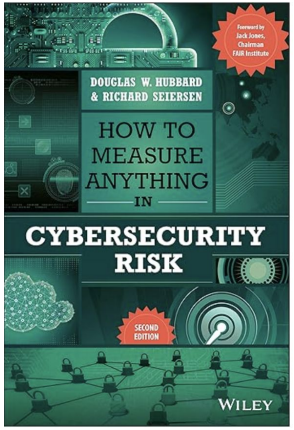
Probability of Ransomware Events and Expected Loss	Current	Target
Probability of Ransomware	12.9%	4.2%
Expected Extortion Loss	$ 1,909,749	$ 635,802
Expected Disruption Loss	$ 3,613,152	$ 1,186,216
Expected Data Theft Loss	$ 1,494,961	$ 494,270
Total Expected Loss	$ 7,017,861	$ 2,316,287

Total Loss Exceedance for Control Level Employed

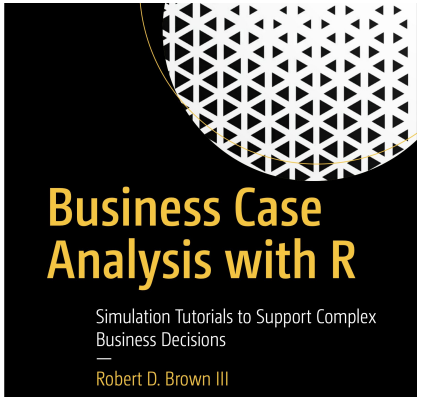
Exceedance Probability

Total Current Control Event Loss
Total Target Control Event Loss
Current Loss Limit
Target Loss Limit

The objects and means of measurement



Monte Carlo simulation tutorial in R



How To Start Thinking Like The Money People

Control	Planned Start Dat	Duration to Full Implementation [months	Planned End Dat	Risk of Exceeding Lim	Planned Cost
MANAGED:MFA & PAM	19-Nov-24	10	15-Sep-25	4.3%	$ 1,013,721
MANAGED:Micro-Segmentation	20-Sep-24	11	16-Aug-25	6.3%	$ 1,197,358
MANAGED:EPP & EDR	18-Oct-24	9.6	2-Aug-25	7.3%	$ 974,006
MANAGED:Tested Backups	21-Jun-24	5.7	9-Dec-24	9.2%	$ 587,245
MANAGED:30 Days Patch CRITCAL	17-Jun-24	4.6	2-Nov-24	10.2%	$ 463,895
DEPLOYED:Email Security Gateway & Email Auth	16-Aug-24	2.5	30-Oct-24	11.3%	$ 388,902
MANAGED:Attack Simulations	15-Jul-24	2.5	28-Sep-24	12.5%	$ 310,493

A defensible budget should include a schedule for deployment and the incremental benefit achieved at each milestone