

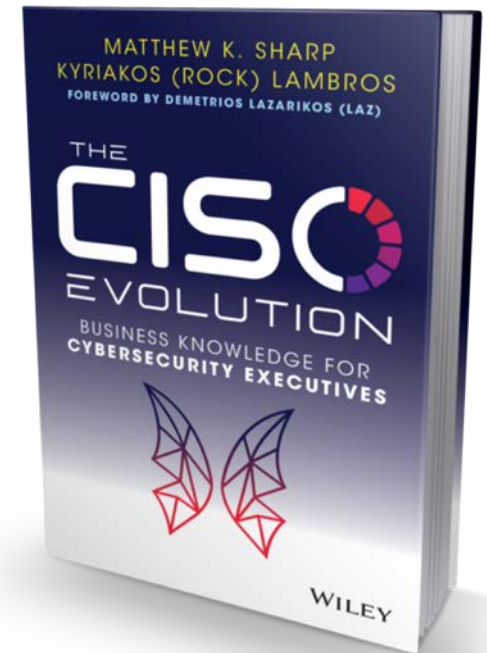



# From defects to \$\$\$

*If you fund it, they disappear...*

## Who am I?

- >17 Years of Experience
- 2x CISO
- Board + Venture Advisor
- Forbes Tech Council Member
- MBA from CSU

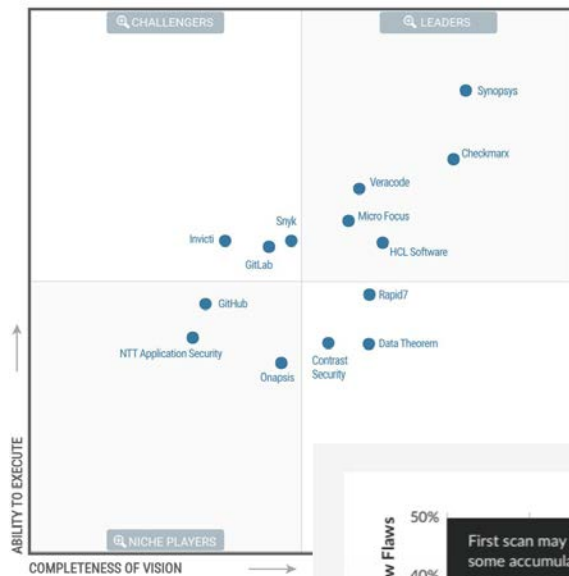




There are actually  
two battlefields

# The external battlefield

2022 Magic Quadrant



Gartner

## FIVE REASONS TO GO WITH THE MARKET LEADER

Checkmarx

## Data Now Driving More Security Decisions

There was growth in security efforts among members of the BSIMM community in "build a capability to combine AST results" (56%), "identify metrics and use them to drive resourcing" (24%), and "publish data about software security internally and drive change" (16%).

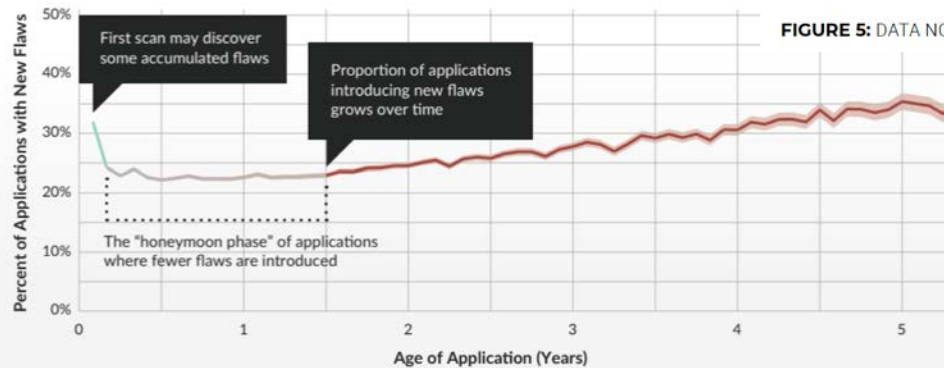
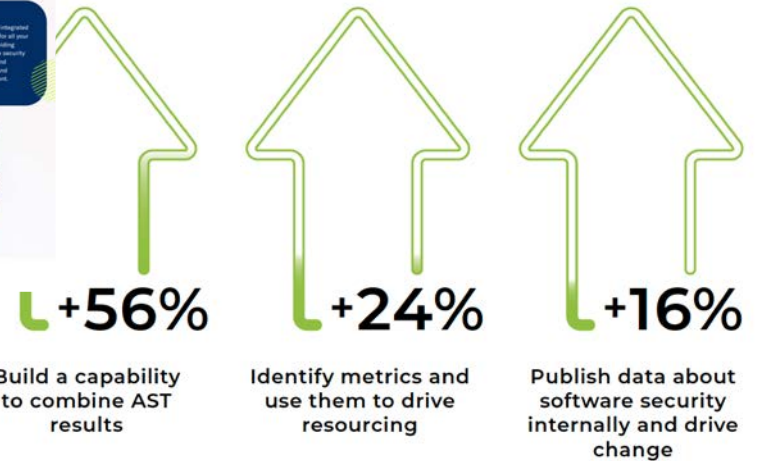
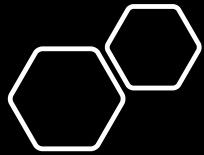


FIGURE 5: DATA NOW DRIVING MORE SECURITY DECISIONS

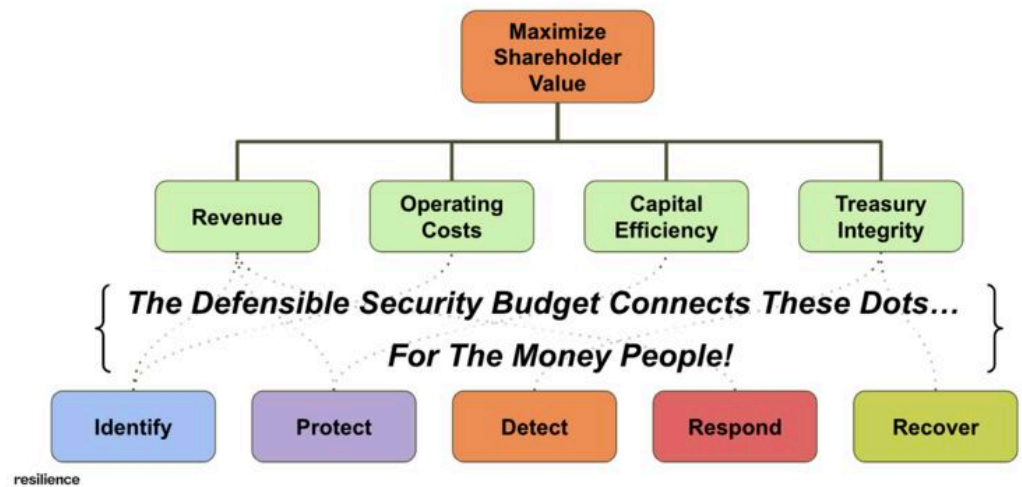
Veracode

Synopsys



# The internal battlefield

## How To Start Thinking Like The Money People





# Two variables drive determine your success

## Economics



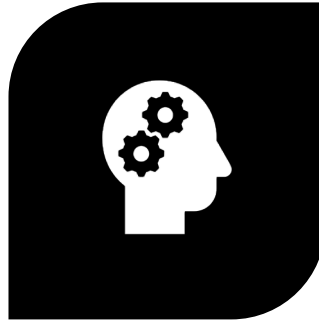
## Psychology



# Our Journey Today



VALUE CREATION



DECISIONS



BUSINESS CASES

# Value Creation







## Primer on Value Creation



# Who determines value?

## Strategic vs. Financial



## Private Equity vs. Hedge Fund



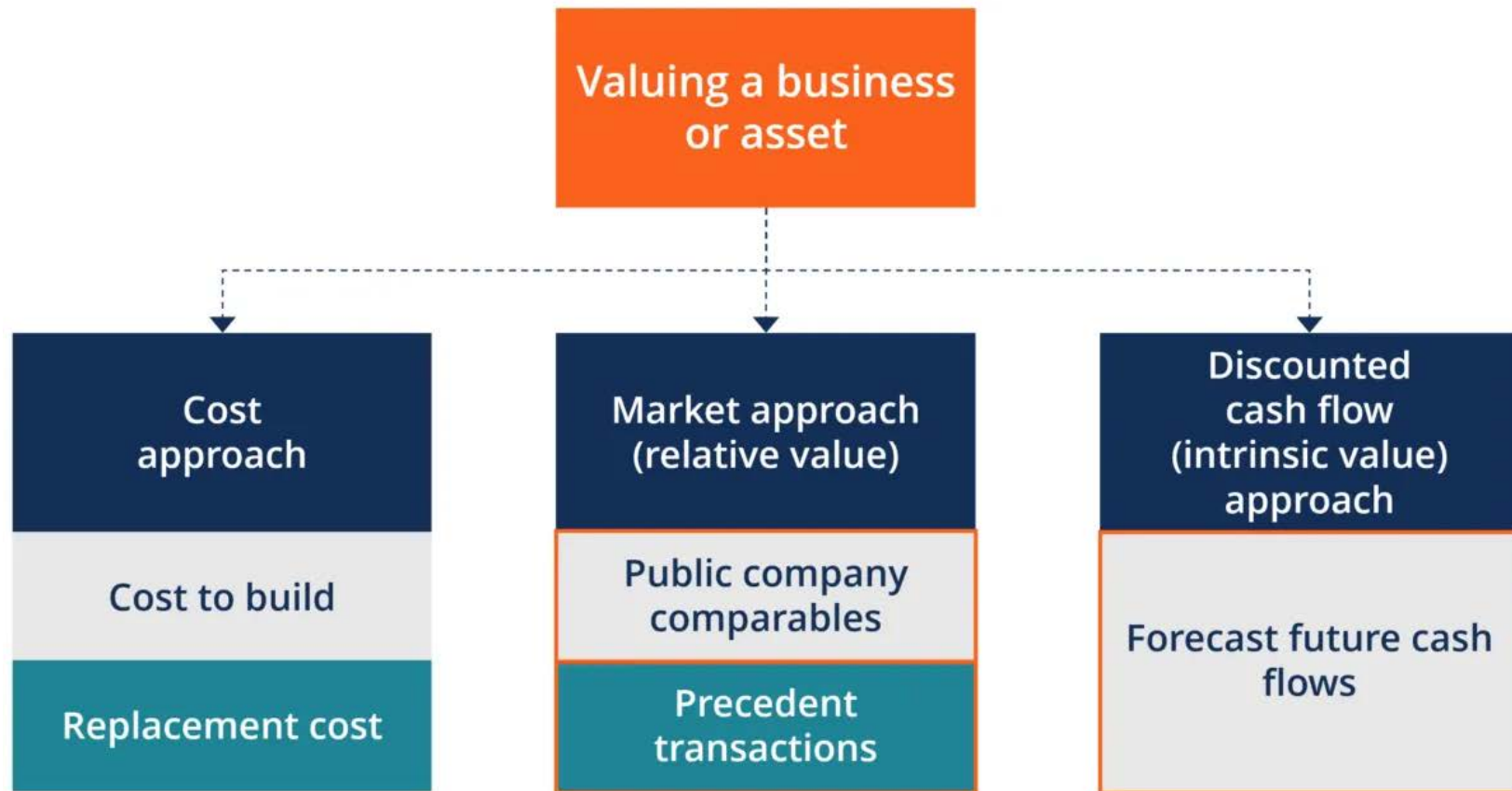
# What delivers value?

- Dividends
- Redemptions
- Capital Appreciation

**Table 10. Factors influencing the equity's value (*value drivers*)**

[illegible]

## Where is value created?





# When is value created?

The maximum valuation at a point in time is a function of numerous factors, including:

- Conditions in the stock market
- The level of interest rates and the availability of financing
- Conditions in the relevant economic markets (national, regional, local)
- Industry conditions
- Current interest of competing strategic buyers in similar businesses
- Availability of investment funds in private equity funds focused on similar businesses
- When irrational buyers abound
- **The level of earnings and conditions in the business being sold**



# Why is value so important?

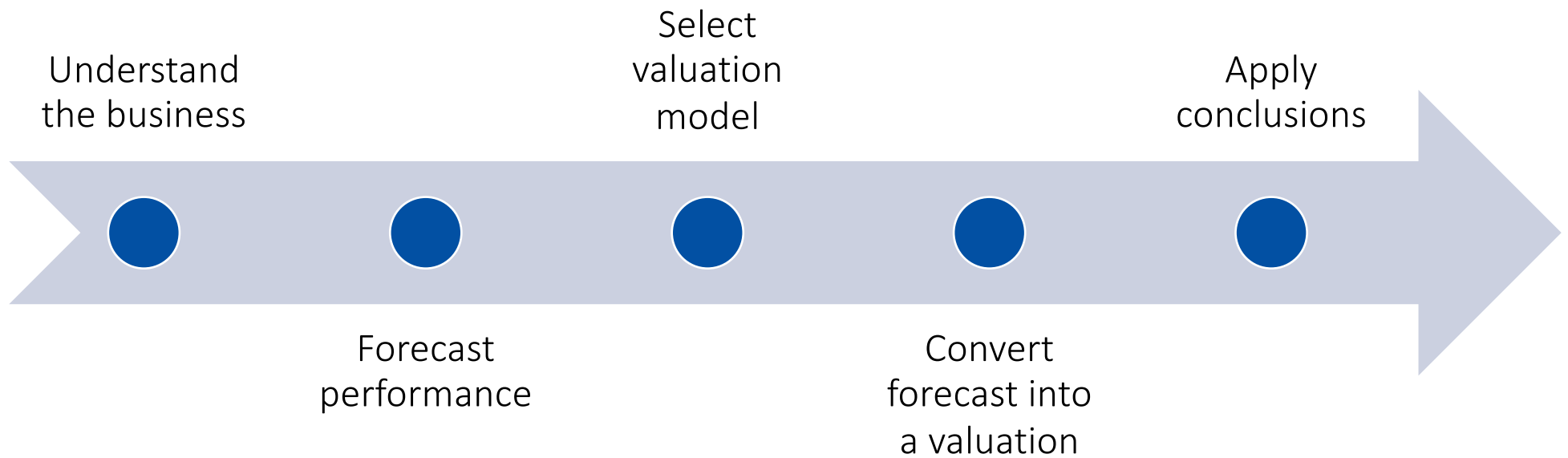
The decisions you make about structuring your team, the controls you implement, the architectures you choose, and the partners you leverage need to be congruent with your company's value agenda. The things you prioritize and protect, the risks you accept, and the stories you tell must also align with the value agenda.


It doesn't matter if the value agenda comprises evolving your business model, streamlining your operating costs, heavy M&A activity, or finding ways to maximize an EBITDA multiple. Cybersecurity leaders need to be aware of the value agenda, and they need to be able to design programs that support and accelerate it. **In short, cybersecurity operations that impede the value agenda are doomed.**

As a side note, understanding how these dynamics affect decisions in your business will make a difference in the executive visibility you are permitted.

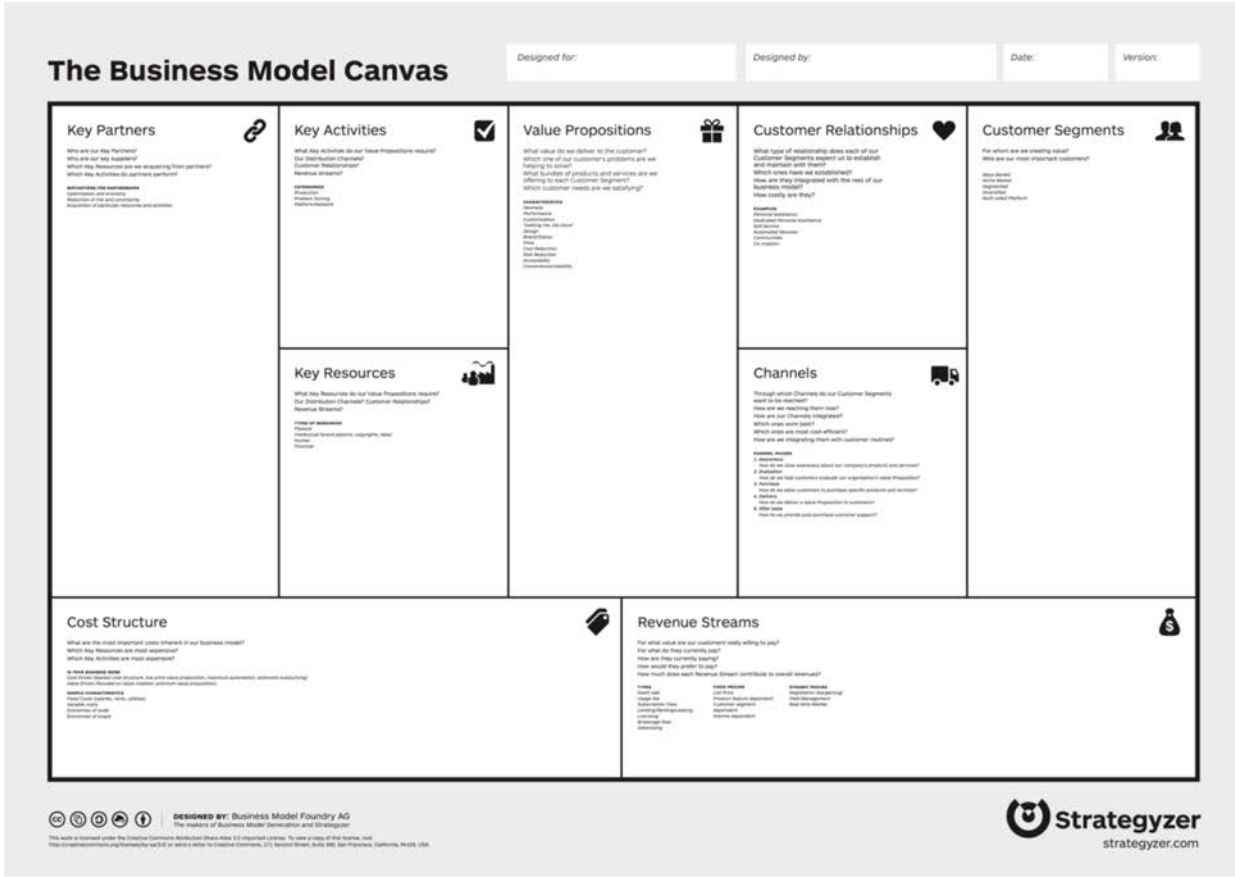


## How is value determined?





# Business Model Canvas



The background is a dark, abstract composition featuring glowing, curved lines in shades of blue, purple, and orange. Scattered throughout are binary digits (0s and 1s) in various sizes and colors, creating a sense of digital data flow and depth.

# Decision Making

# 3 Key Elements

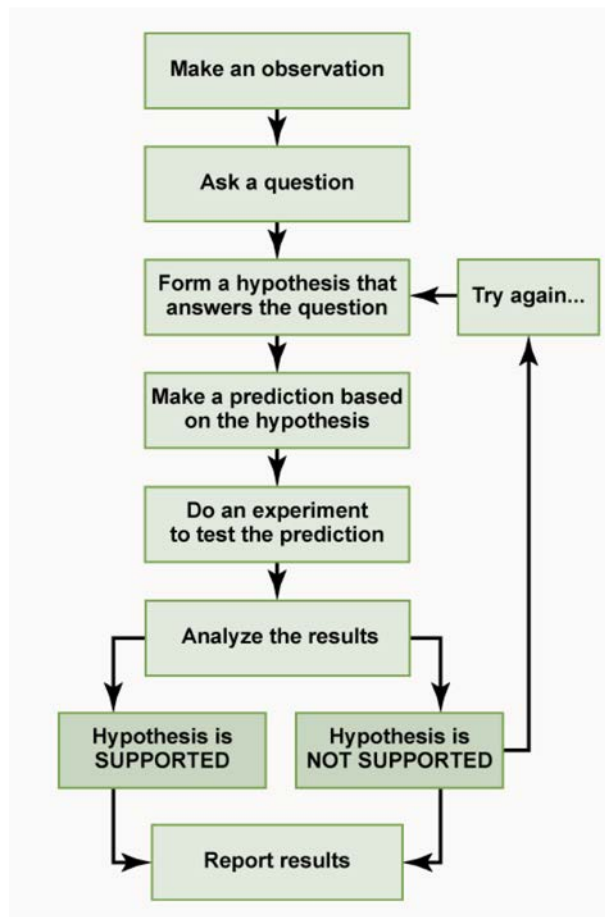
Scientific Method

Decision Science

Choice Architecture



# Scientific Method



Flowchart of The Scientific Method  
Source: Rice University / CC BY 4.0.



<https://yourbias.is/>

<https://yourlogicalfallacyis.com/>

## The Ranch – Sunk Cost, and Loss Aversion



# Decision Science

## Your Decisions



### WIDEN YOUR OPTIONS

Narrow framing leads us to overlook options. (*Teenagers and executives often make “whether or not” decisions.*) We need to uncover new options and, when possible, consider them simultaneously through multitracking. (*Think AND not OR.*) Where can you find new options? Find someone who has solved your problem. Try laddering: First look for current bright spots (*local*), then best practices (*regional*) and then analogies from related domains (*distant*).

### REALITY-TEST YOUR ASSUMPTIONS

In assessing our options, the confirmation bias leads us to collect skewed, self-serving information. To combat that bias, we can ask disconfirming questions (*What problems does the iPod have?*). We can also zoom out (*looking for base rates*) and zoom in (*seeking more texture*). And whenever possible we should ooch, conducting small experiments to teach us more. Why predict when you can know?

### ATTAIN DISTANCE BEFORE DECIDING

Short-term emotion tempts us to make choices that are bad in the long term. To avoid that, we need to attain distance by shifting perspective: What would I tell my best friend to do? Or, what would my successor do? (*Or try 10/10/10.*) When decisions are agonizing, we need to clarify our core priorities—and go on the offensive for them. (*Remember the stainless steel bolts on the Navy ship.*)

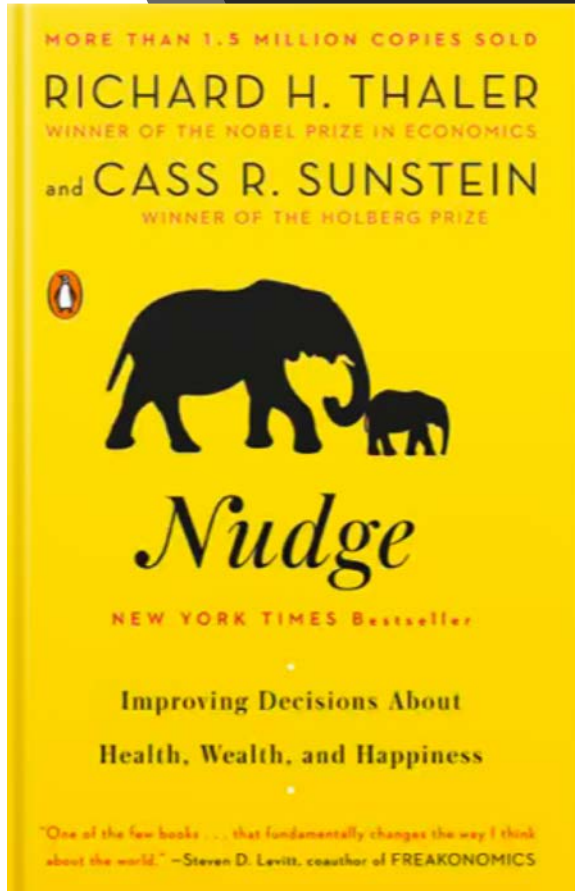
### PREPARE TO BE WRONG

We are overconfident, thinking we know how the future will unfold when we really don't. We should prepare for bad outcomes (*premortem*) as well as good ones (*preparade*). And what would make us reconsider our decisions? We can set tripwires that snap us to attention at the right moments. (*David Lee Roth's brown M&M, Zappos' \$1,000 offer*)

## Their Decisions

	Motivation	Ability
Personal	1 Do I enjoy it?	2 Am I personally Able?
Social	3 Do others motivate?	4 Do others enable?
Structural	5 Do “things” motivate?	6 Do “things” enable?

<https://cruciallearning.com/influencer-book/>



# Choice Architecture

- iNcentives
- Understand mappings
- Defaults
- Give feedback
- Expect error
- Structure of complex choices



The background image shows a person's hands typing on a laptop keyboard. The scene is overlaid with a complex digital interface. On the left, there's a large, semi-transparent circular graphic with concentric rings. Overlaid on this and the rest of the image are various icons and text elements: a clock, a padlock, a gear, a 97% progress indicator, a document, a lightbulb, and code snippets like '<CSS>', '</>', '{ }', and '<DEV>'. There are also grid lines and plus signs scattered throughout. The overall color palette is dark with blue and white highlights.

# The Business Case



# What is a business case?

Summarize the need.

Enumerate assumptions, risks, and objections.

Outline costs.

Describe the benefits.

Financial analysis including future cash flows, etc.

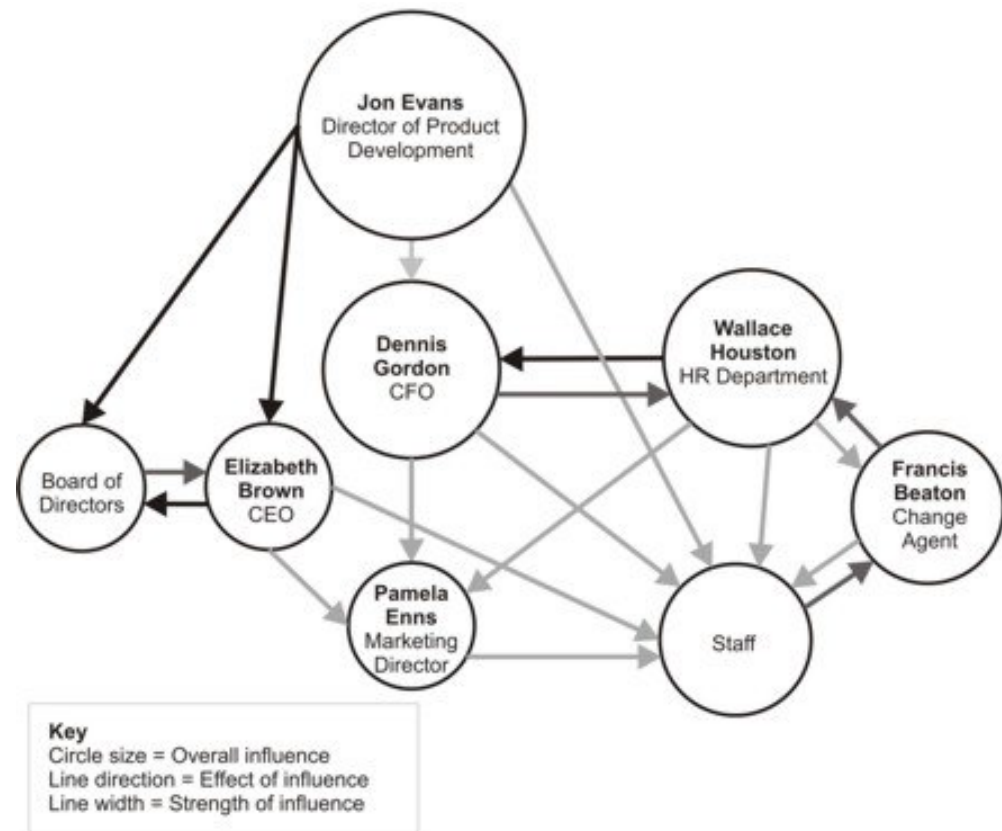
Establish a timeline and payback period

Analysis of alternatives (often including the status quo).

See also - <https://risk3sixty.com/2020/09/21/how-to-build-a-business-case-for-security-initiatives-part-4/>

# Stakeholder Analysis

- Can be done intuitively with practice
- See repeated patterns





# SCIPAB Communication Framework

*1. Create listener alignment with the problem or opportunity*

Situation	Complication	Implication
Linkage of topic to a known issue of importance to the listeners?	Changes, challenges, and/or problems?	SO WHAT? Impact to listeners and/or their business?

*2. Suggest resolution with listener relevant benefits*

Position	Action	Benefit
Your solution, point of view, idea, or recommendation?	Actions the listeners need to take relative to your position?	Benefits to taking action, linked to the listeners' care abouts?

<https://www.mandel.com/blog/what-is-scipab>



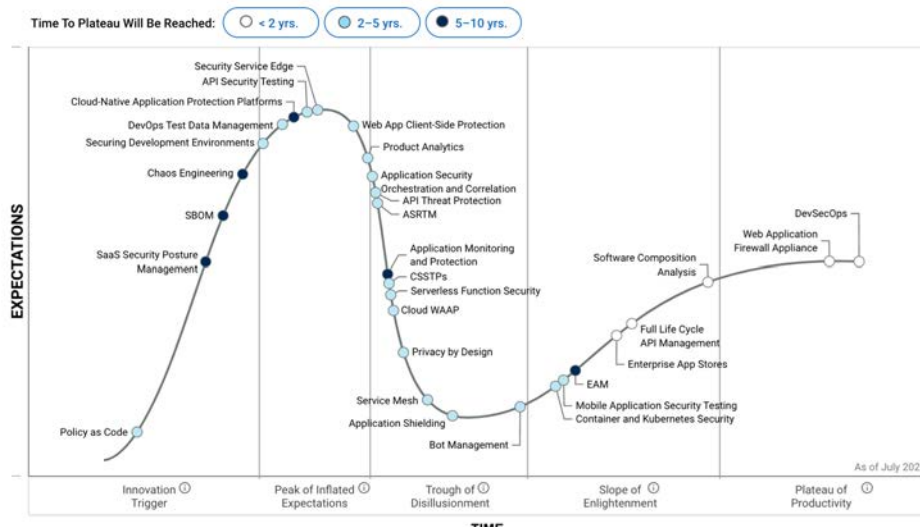
# Summary

---

**Pulling it all together**



# Think big, start small, move fast.



## Business functions

## Security practices

Governance	Design	Implementation	Verification	Operations
<b>Strategy &amp; Metrics</b> Create & promote Measure & improve	<b>Threat Assessment</b> Application risk profile Threat modeling	<b>Secure Build</b> Build process Software dependencies	<b>Architecture Assessment</b> Architecture validation Architecture mitigation	<b>Incident Management</b> Incident detection Incident response
<b>Policy &amp; Compliance</b> Policy & standards Compliance management	<b>Security Requirements</b> Software requirements Supplier security	<b>Secure Deployment</b> Deployment process Secret management	<b>Requirements-driven Testing</b> Control verification Misuse/abuse testing	<b>Environment Management</b> Configuration hardening Patch & update
<b>Education &amp; Guidance</b> Training & awareness Organization & culture	<b>Secure Architecture</b> Architecture design Technology management	<b>Defect Management</b> Defect tracking Metrics & feedback	<b>Security Testing</b> Scalable baseline Deep understanding	<b>Operational Management</b> Data protection Legacy management
Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B





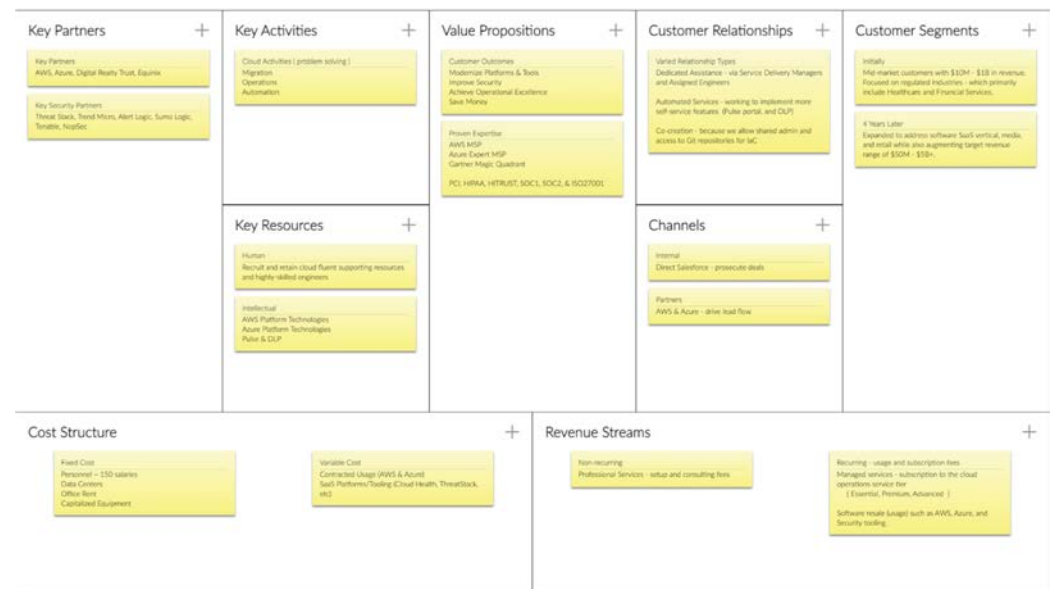
# Case Study: Stakeholder Desires

1. CISO – Secure Software
2. CTO – Feature Release Velocity
3. CFO – Value Protection
4. CEO & Board – Revenue Growth



# Business Context

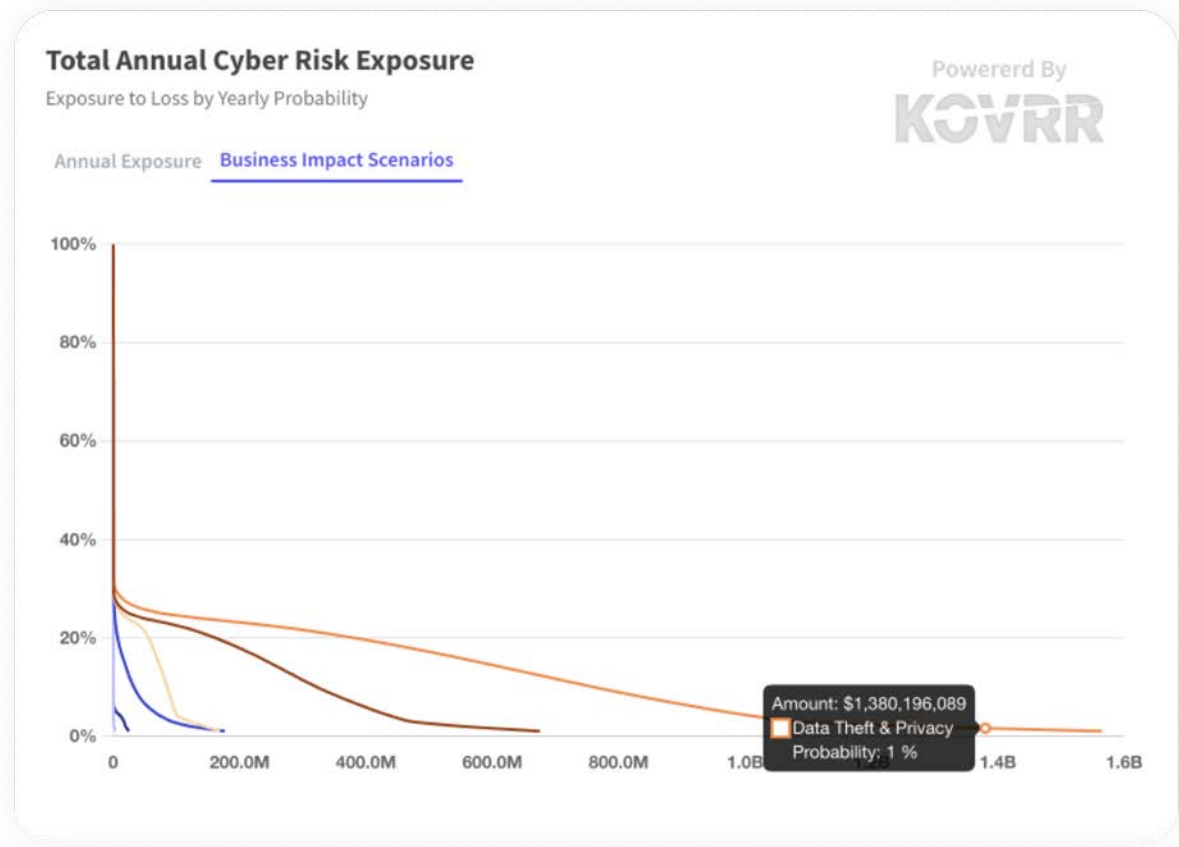
- Private equity back business that was early in the investment fund and investment.
- Vision was to create a software-driven cloud MSP with a cybersecurity differentiator targeting Healthcare and FinTech.
- Software would enable SaaS-like economics (LTV/CAC, strong margin profile, net retention, 80%+ recurring revenue model) which should impact overall EV.
- Massive and growing TAM for Public Cloud.
- Talent and cash are the two primary constraints in the business.



# Personal Conviction = WRAP + CRQ

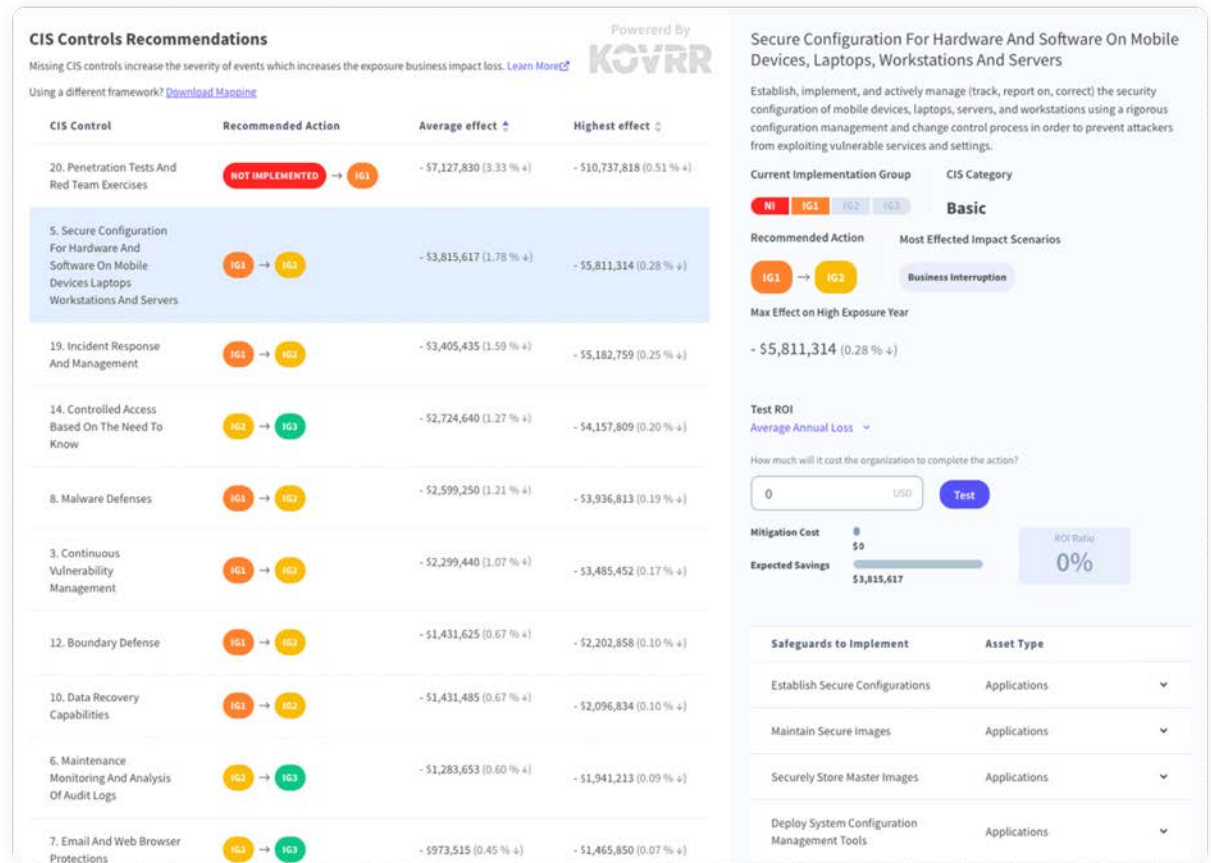
Use Cyber Risk Quantification  
to WRAP your head around  
department capital allocation:

- Widen Your Options
- Reality Test Assumptions
- Attain Distance
- Prepare to be Wrong

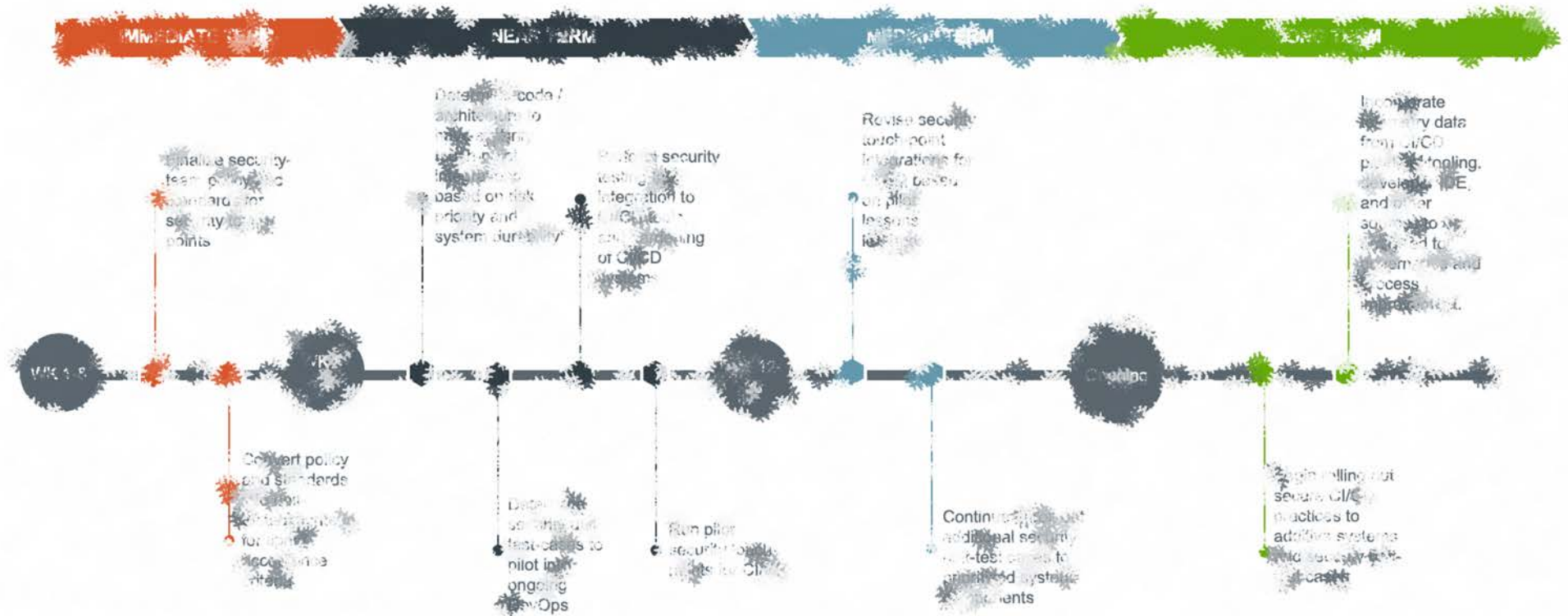


# Nudge CFO Forward

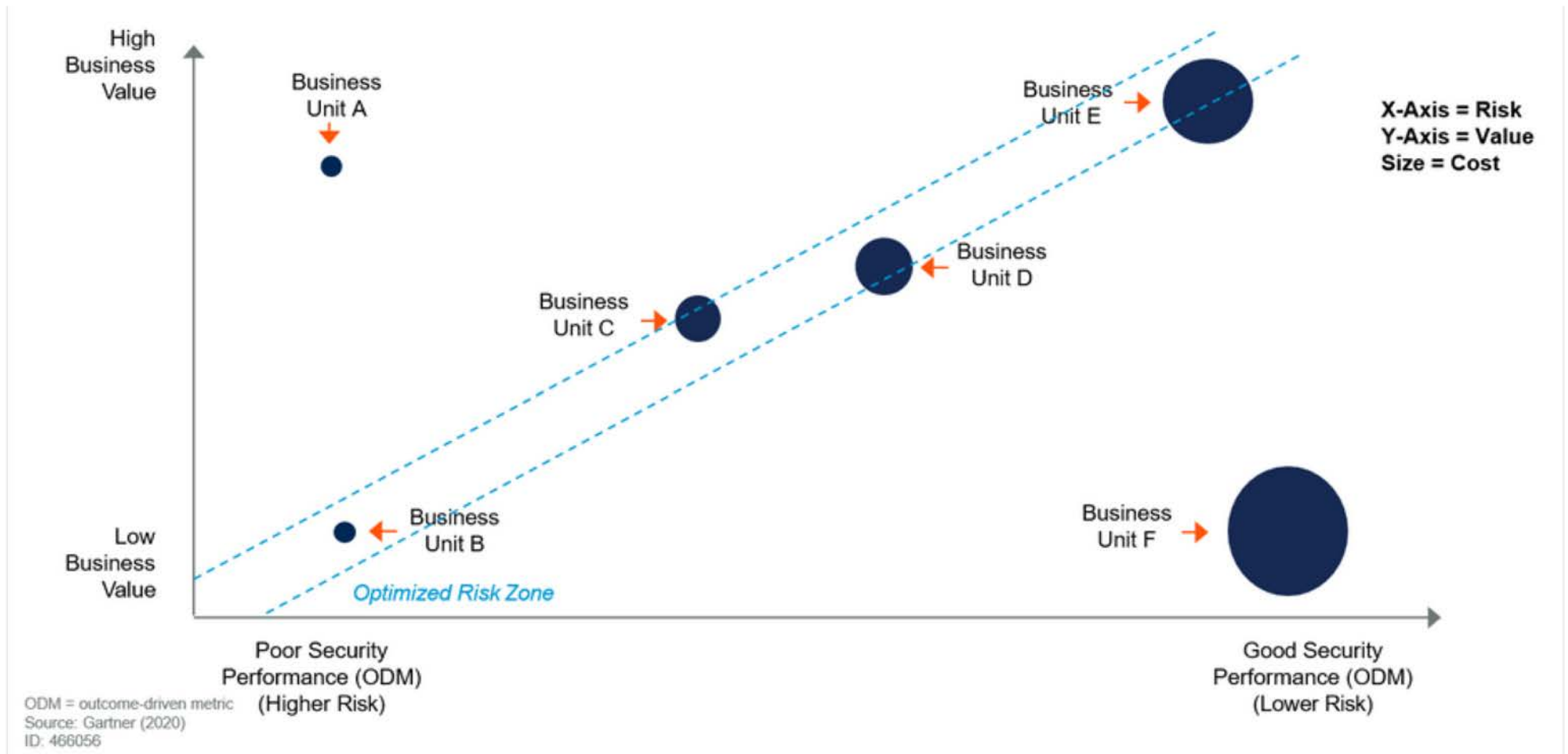
- Reality Test Assumptions (WRAP) – Complete ROI Analysis
- Choice architecture (NUDGES):
  - Understand Mappings – by framing investment in terms of optimizing Financial Risk.
  - Structure to Complex Choices – You offer 3 alternatives
    - do nothing / accept
    - focus on other risk
    - invest in SSI



# Phased Roadmap



## SCIPAB for Budget Request (Risk, Value and Cost)



# Customer Acquisition = Revenue Growth

**cardknox**  
DEVELOPER-FRIENDLY PAYMENTS

**D3 SECURITY**

**DST**  
SYSTEMS

**EVERCORE** | Wealth Management  
THE NEW STANDARD IN WEALTH MANAGEMENT

**GEISINGER**  
HEALTH SYSTEM

**HENRY SCHEIN®**

**Janus Henderson**  
INVESTORS

**Legacy.com®**



**MassMutual**  
FINANCIAL GROUP®

**ORION**   
HEALTH

  
PARTYLITE

**3M**

 **Alnylam®**  
PHARMACEUTICALS

**BAMBOO ROSE** 

  
MASSACHUSETTS

**BMT**  
BRYN MAWR TRUST

**chewy**

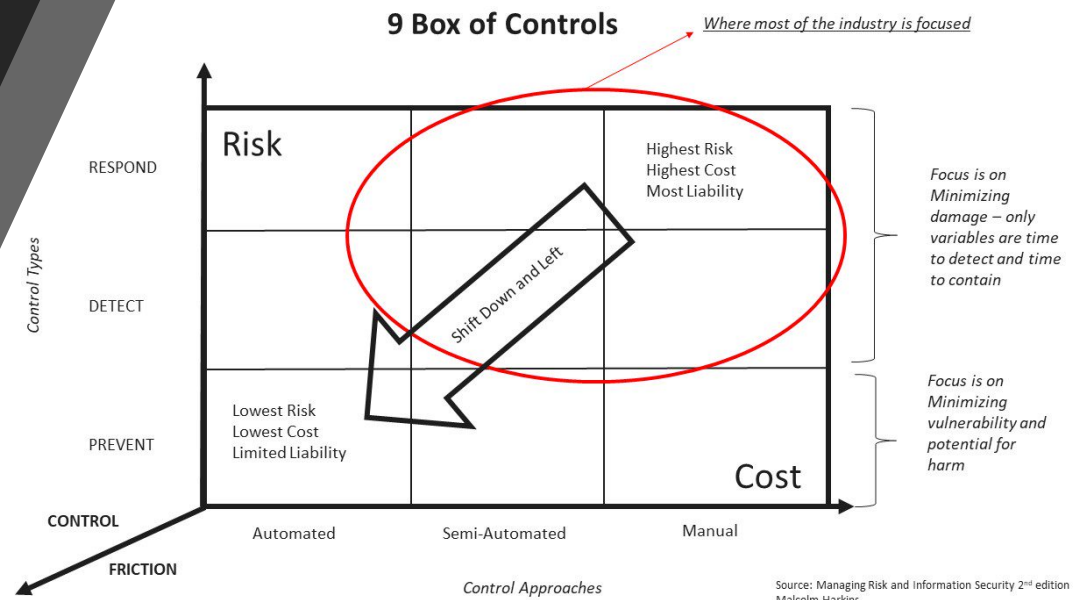
**Columbia**  
 **Bank**

**EBSCO**



# 10x Influence using 9 Box of Controls

- Sources of Influence:
  - P M - more time on functionality
  - P A - automated controls
  - So M - security champ on culture
  - St A - emphasizes standard CI pipelines



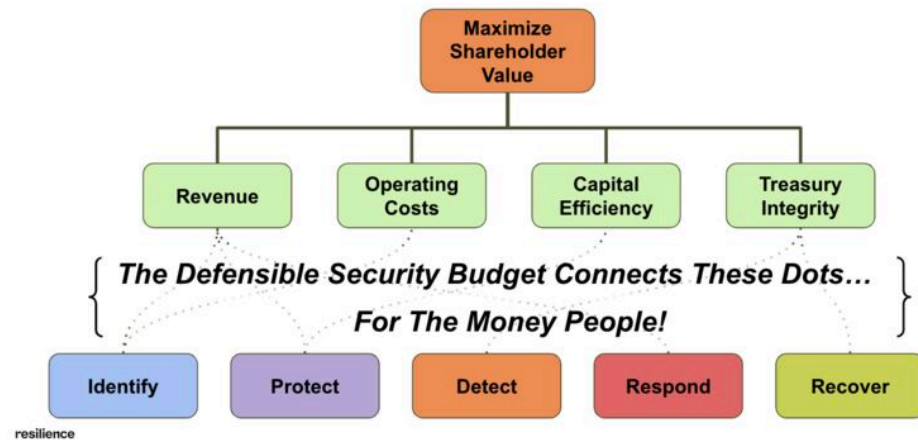
# Data Driven Approach



# Conclusion

Recall Case Study Decisions:

1. CRQ + WRAP established conviction
2. NUDGE CFO into SSI benchmark
3. SCIPAB + Biz Model Canvas → Open Source License Compliance + SCA to protect EV
4. Customer Acquisition drives Source Code Review
5. 9 Box + Influencer gets CTO to advocate for ASPM + HC



# Key Resources

## Books:

- The CISO Evolution: Business Knowledge for Cybersecurity Executives
- Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers
- Managing Risk and Information Security: Protect to Enable
- Decisive: How to Make Better Choices in Life and Work
- Nudge: Improving Decisions About Health, Wealth, and Happiness
- Influencer: The New Science of Leading Change

## Web Resources:

- Stakeholder Analysis by MindTools
- Mandel Communications SCIPAB Framework
- Risk3Sixty Business Case Reference
- Logical Fallacy - <https://yourlogicalfallacyis.com/>
- Cognitive Bias - <https://yourbias.is/>

## Featured Vendors:

- Kovrr – Cyber Risk Quantification
- Enso Security – Application Security Posture Management