Why Your Cybersecurity Program is a Horse's Behind

Ira Winkler, CISSP
ira@cyesec.com


James Johnston
Photography

What Can We Learn?

- It’s easy to perpetuate things year after year
- Continuing to follow the ass keeps things simple
  - Not better, but easier
- Removes need to think and experiment
- Advances limited by ruts
- Attempts to deviate can cause damage and setbacks without the right infrastructure

Typical Cybersecurity Budget Game

- What was last year’s budget?
- Is there more money?
- Are there any countermeasures you really want?
- Validate against percent of IT budget

The Big Problem

CISOs get the budgets they Deserve, not the budgets they Need. They need to learn to Deserve what they Need

Does This Make Any Sense?

Are you protecting IT or organizational value?

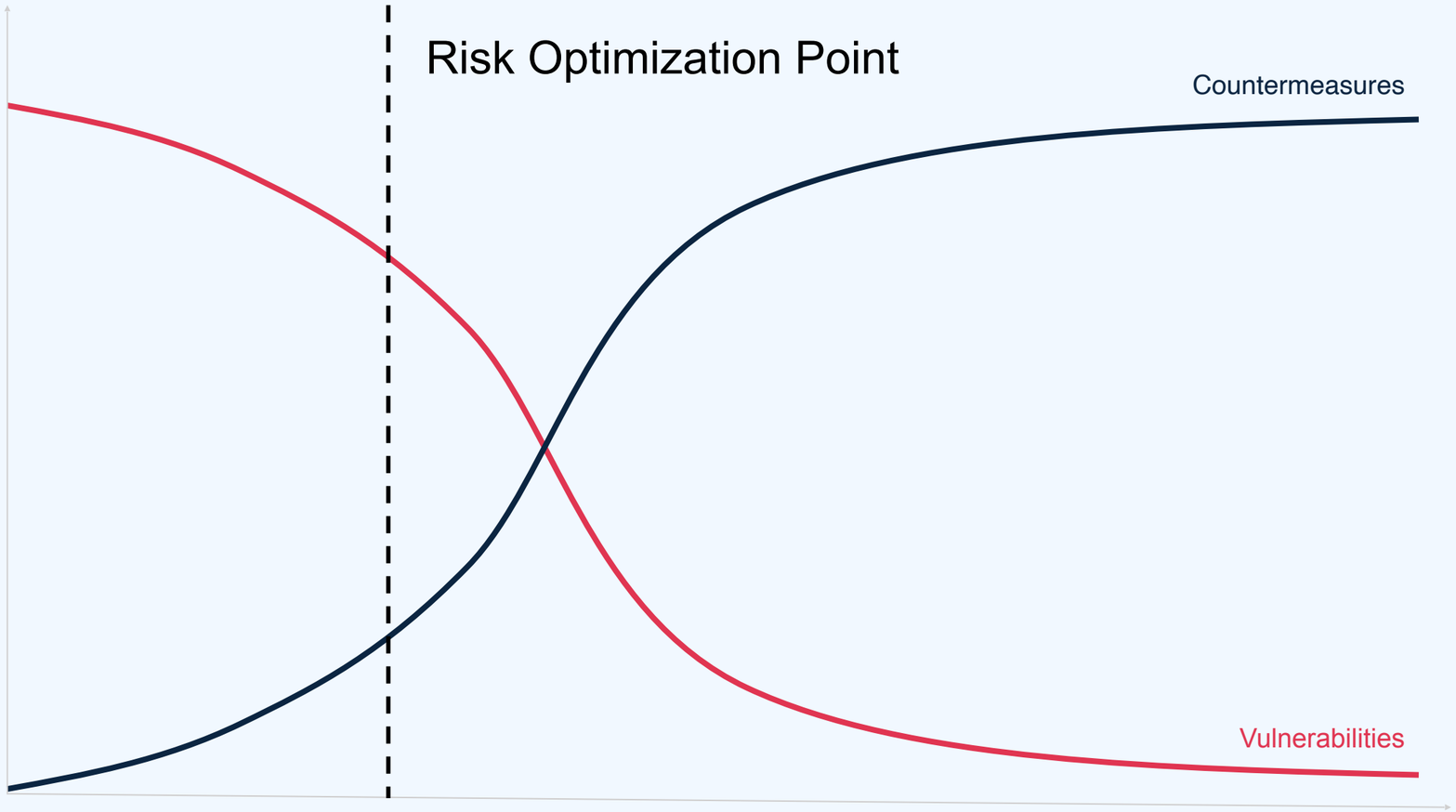
Other Disciplines Collect Hard Numbers

- Operations
- Accounting
- Safety Science
- Supply Chain

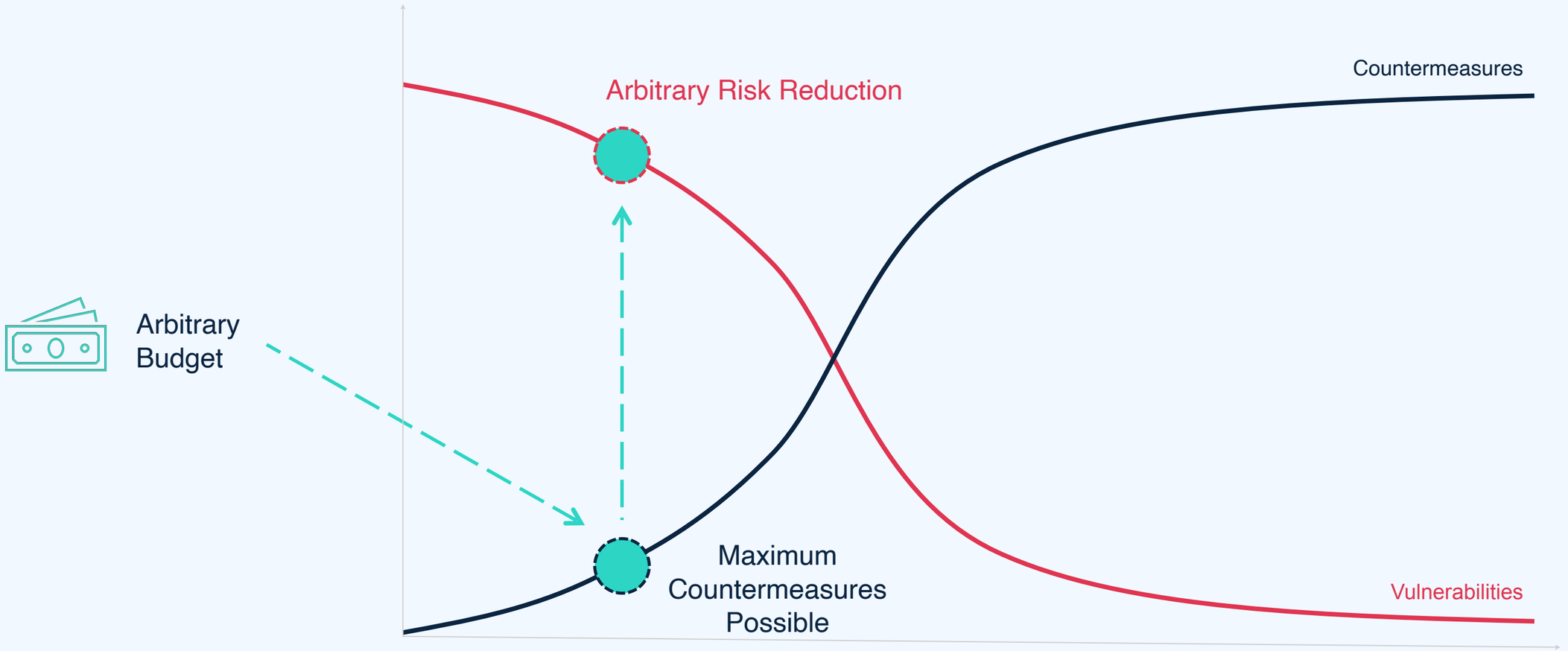
Crude Risk Equation

$$Risk = \frac{Value\ x\ (Threat\ x\ Vulnerability)}{Countermeasure}$$

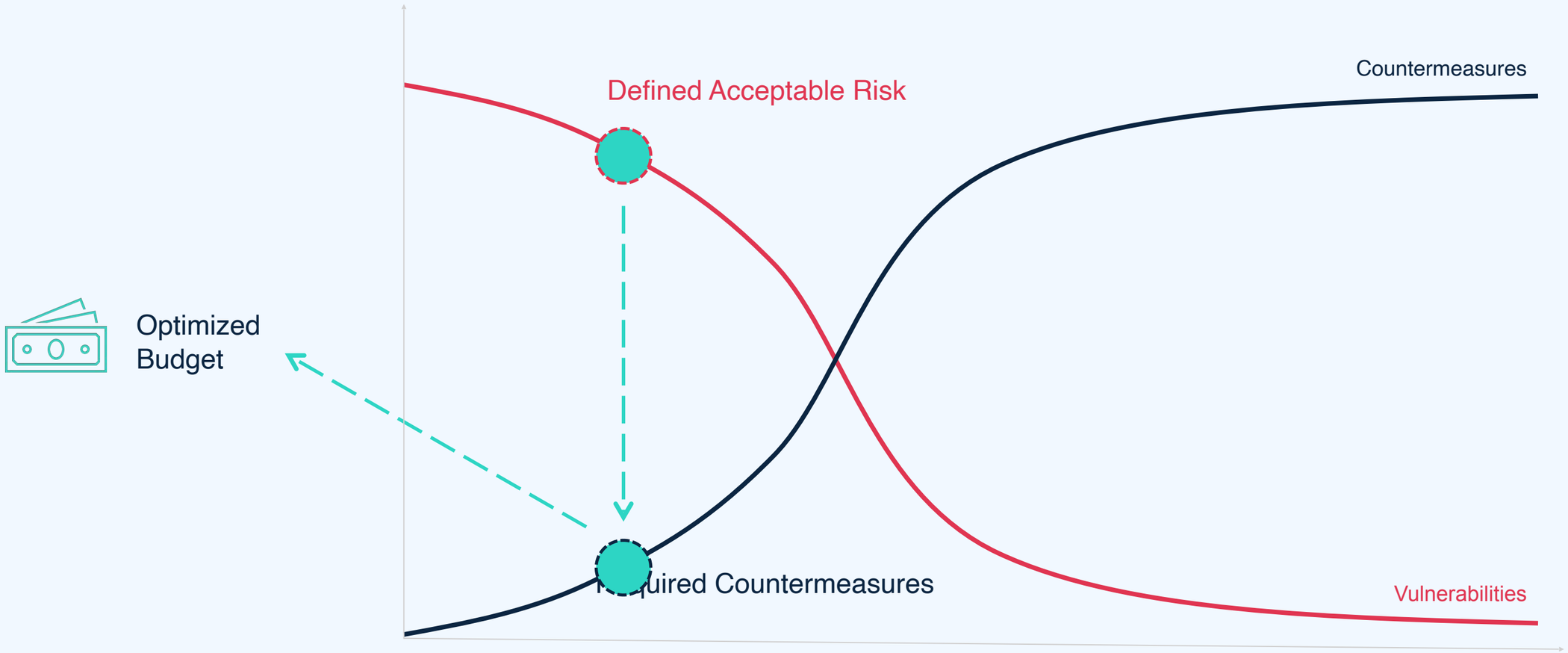
Optimized Risk



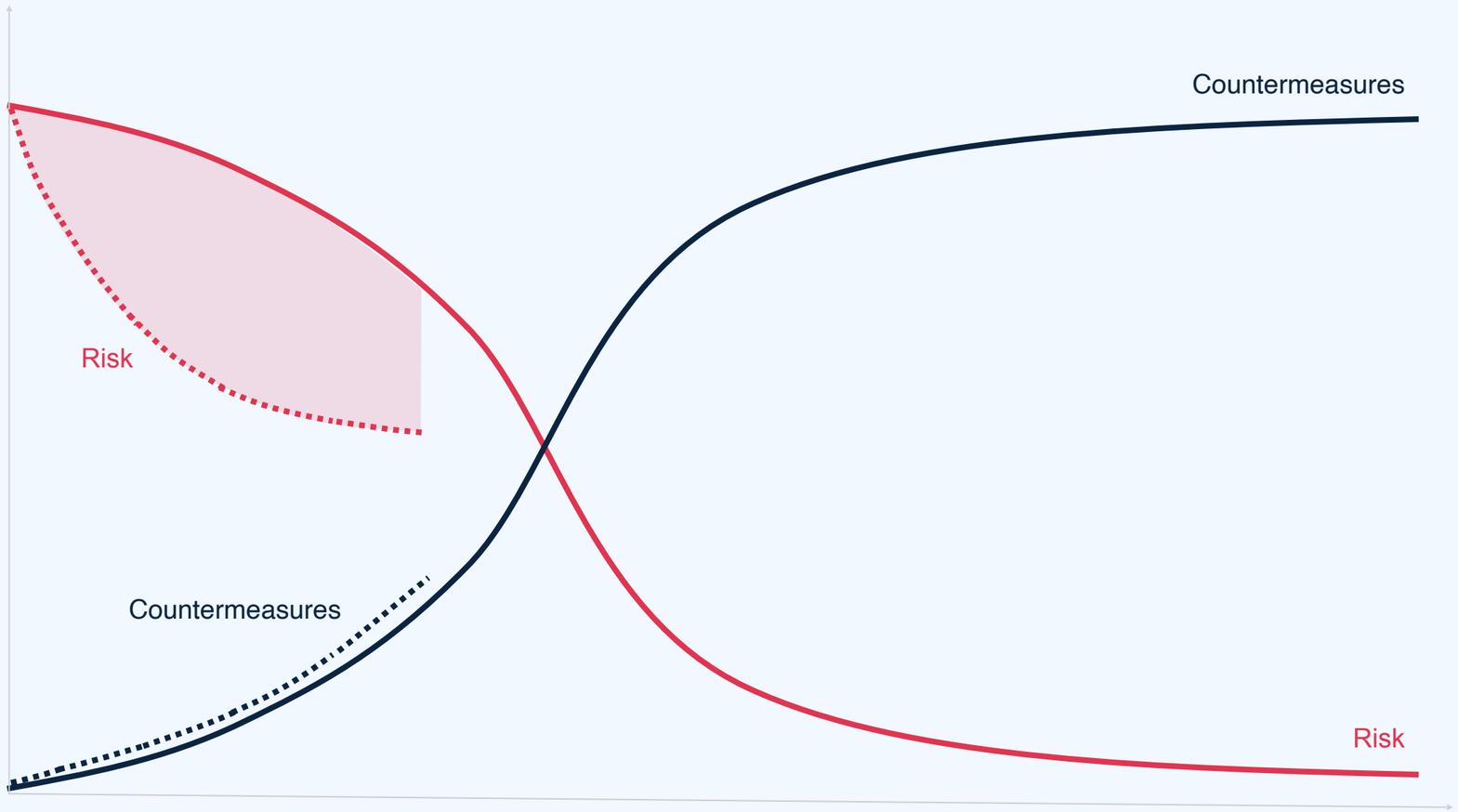
Budget-Driven Implementation of Countermeasures



Return on Investment-Driven Budget



Optimization of the Cyber Risk Investment



Determine Potential Loss

- Hard and soft
- Financial theft
- Cost of outage
  - Availability loss
  - Income losses
  - Customer acquisition costs
- Data breach costs
- Investigation
- Recovery

- Fines*
- Reputation costs
- Insurance deductible
- Insurance increases
- Will insurance pay at all?

Variable Factors

- Geographies
- Regulatory environments
- Legal environments
- Company size
- Industries
- Incident history
- Viability of cybersecurity and risk program
- Highly complicated if you’re in multiple areas

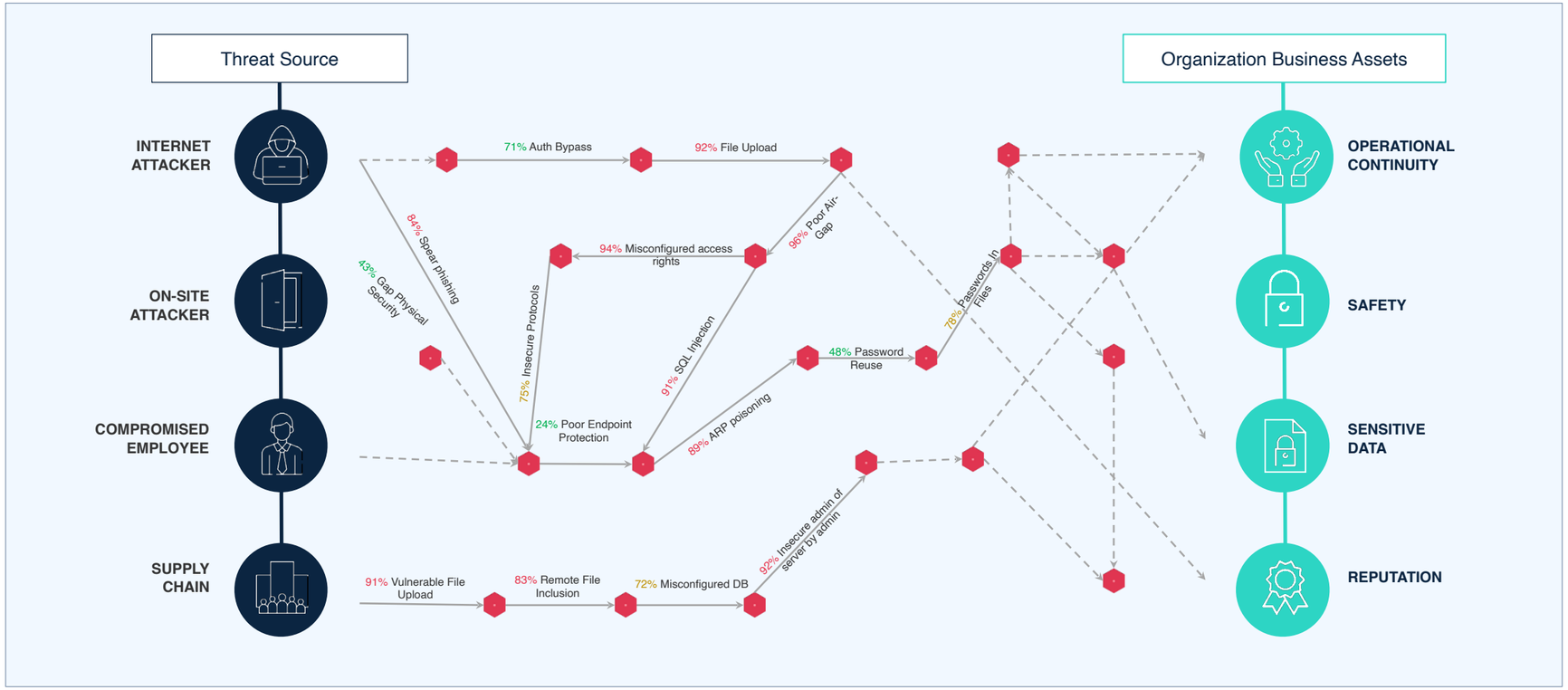
Obtaining Value

- Admittedly not easy
- CFO
- Industry incidents
- Insurance data
- Third party tools

Probability

- Likelihood a threat will exploit the vulnerability
- Skill level of threat
- Availability of exploit
- Data on dark web
- Threat intelligence
- Difficulty of exploitation
- Motivation
- Attack path dependencies
- Vulnerability Criticality not a determining factor

Calculate the likelihood of incident scenarios



Determine Vulnerability Cost

- Vulnerability Cost(N) = Prob(N) x $\sum_{R0}^{RN} Risk$

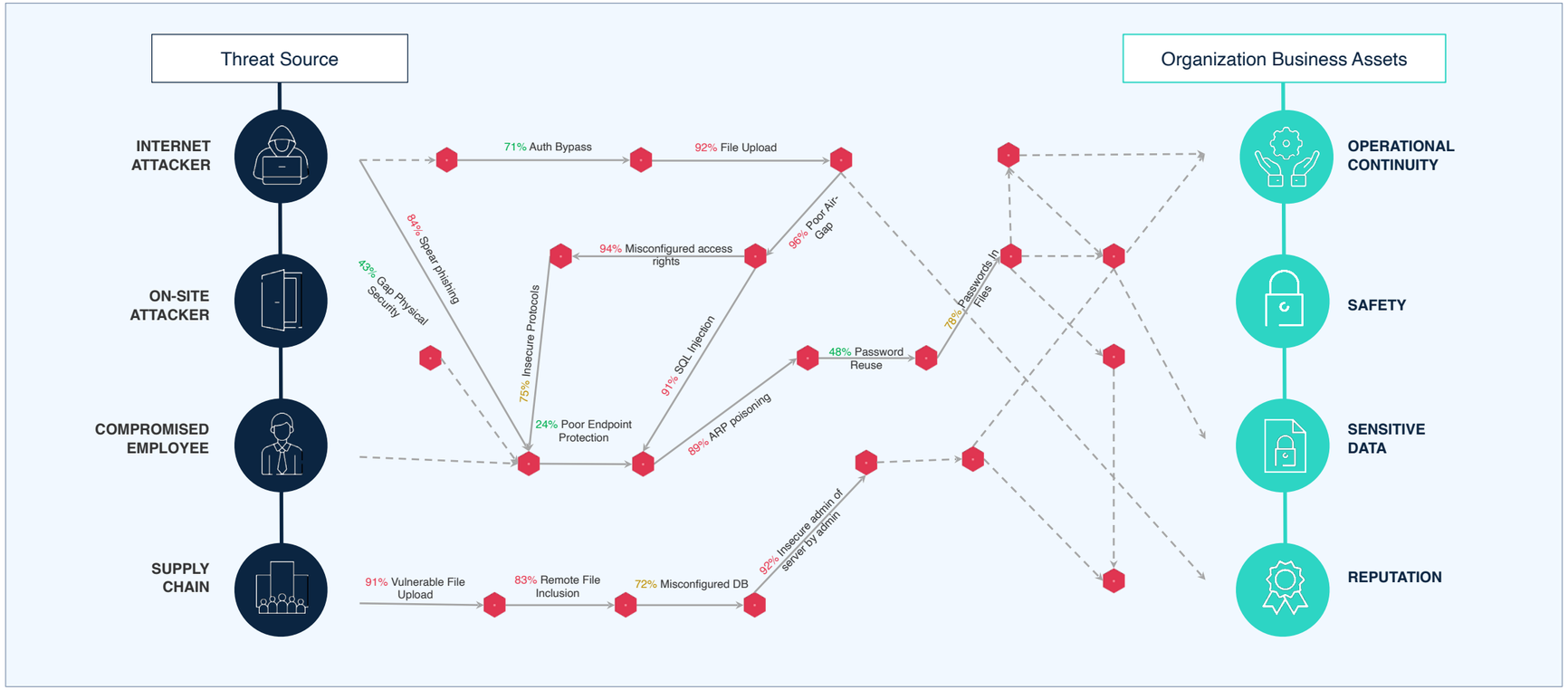
Is It Worth Mitigating a Vulnerability?

- Does the countermeasure cost more than a loss?
- Determine cost including all factors
  - Price, people, maintenance, geography,
- Consider one countermeasures might mitigate multiple vulnerabilities

Prioritize

- Attack path choke points
- High return countermeasures
- Multiple mitigation countermeasures
- Quick wins
- Low effort

Choke Points



Put it Together

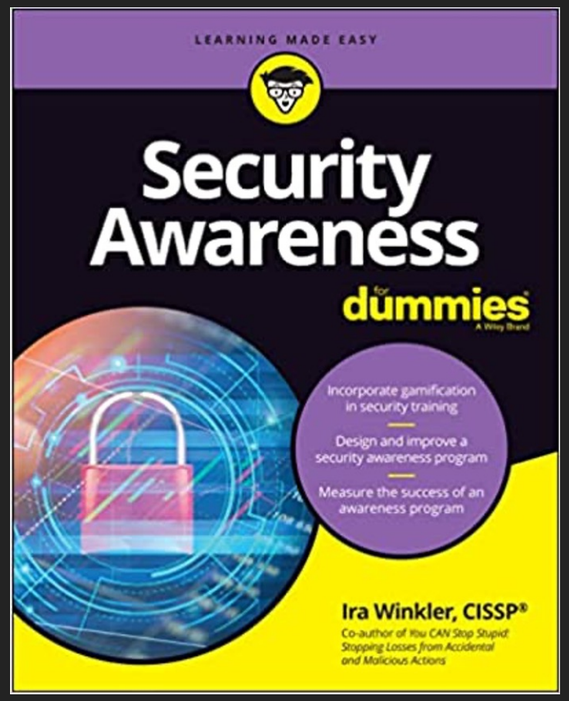
- Deserve What You Need!
- ”With a cost of $XXX,XXX, I will mitigate $YY, YYY, YYY.”
- Highlight regulatory losses
- Highlight recent lawsuits
- Have management acknowledge costs of rejection of request
- Document it?
  - Nice if you can.

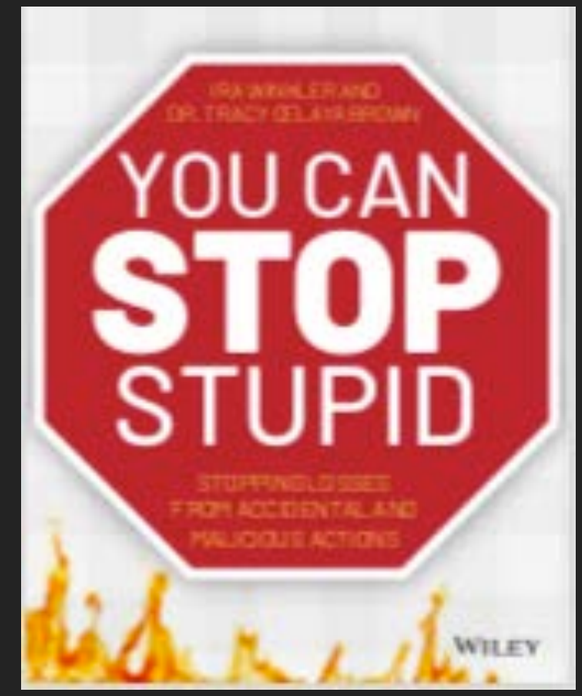
Deserve What You Need

- Every countermeasure has a calculated ROI
- Present your cybersecurity program as having a very specific risk reduction
- Counter any budget cuts with specific increase in monetary risk
- Define the cybersecurity program in the same way all other business processes are

CYE

For Your Reading Pleasure





Thank you

ira@cyesec.com

www.cyesec.com

Ira Winkler, CISSP
ira@cyesec.com
@irawinkler
www.linkedin.com/in/irawinkler

www.cyesec.com