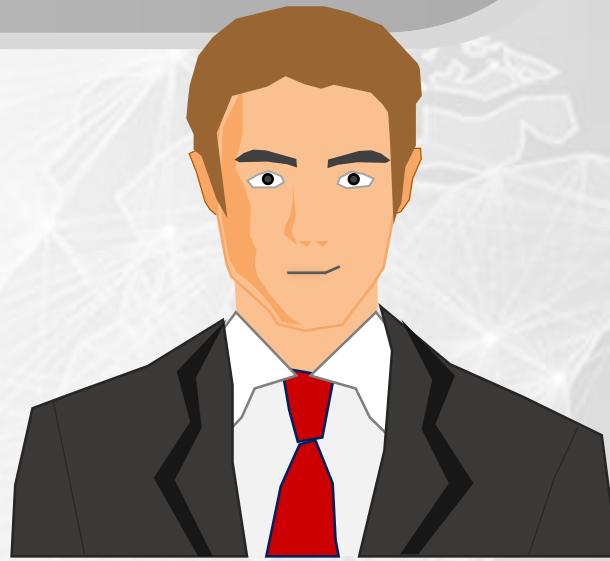
NEHEMIAH
SECURITY

You can measure anything…
but what if it's not the **RIGHT** thing?

Jerry Caponera, VP Cyber Risk Strategy


SENDING
SECURITY TEAM

The communication gap



CEO and Board members asking:

"What can happen to the business?"

"How much could this cost us (in $s)?"

"I'm spending a lot of money on cyber – will I still get hacked?"

Security leaders asking:

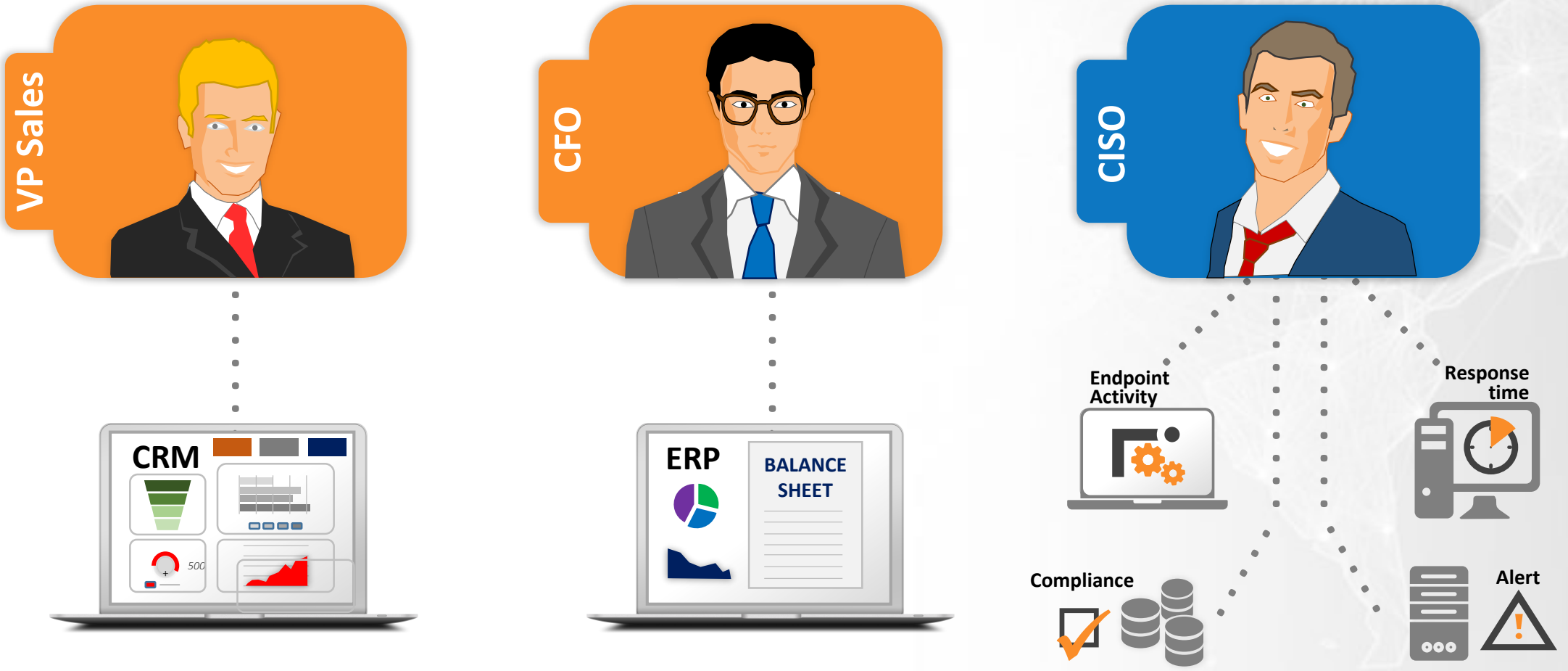
"How can they not understand the importance of needing security solution?"

"Why isn't my budget approved?"

"Why don't they view me as their peer?"

CISO in the business

Which one has the communication gap?



The balance sheet business snapshot

CYBER BALANCE SHEET

ASSETS	
Business Application	
Revenue	?
Petty cash	?
Temporary investment	?
Accounts receivable	?
Inventory	31,000
Contracts	3,800
Prepaid insurance	1,500
Total current assets	?
Security Defenses	?
Investments	36,000
Total assets	**?**
Property, plant & equipment	
Land	5,500
Land improvements	6,500
Buildings	180,000
Equipment	419,000
Less: accum depreciation	(56,000)
Prop, plant, & equip	357,000
Intangible assets	
Goodwill	105,000
Trade names	200,000
Total intangible assets	305,000
Total assets	**770,000**

LIABILITIES	
Current liabilities	
Notes payable	5,000
Accounts payable	35,900
Wages payable	8,500
Interest payable	2,900
Taxes payable	6,100
Warranty liability	1,100
Unearned revenues	1,500
Total current liabilities	61,000
Long-term liabilities	
Notes payable	20,000
Bonds payable	400,000
Total long-term liabilities	420,000
Total liabilities	**481,000**

STOCKHOLDERS EQUITY	
Common stock	110,00
Retained earnings	220,000
Accum other income	9,000
Less: Treasury stock	(50,000)
Total owner's equity	289,000
Total liabilities & SH equity	**770,000**

numbers in thousands

CYBER EXPLOITABILITY

Exploitability

Confidence interval

Probability of attack

Example

Example: Point-of-Sale System

Supporting key applications:
NetSuite

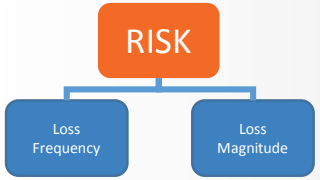
Revenue value:
$350M

Business interruption value:
$1 m
/ 90 days

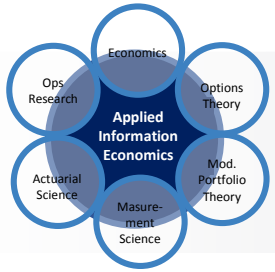
Record count:
50,000

How do we get there?

Business Impact Analysis



Factor Analysis of Information Risk (FAIR)



Hubbard Method

Remember:
Perfect is the enemy of good enough

Step 1: Filling it in

CYBER "BALANCE" SHEET

CYBER ASSETS

Point of Sale (POS) system	
Revenue	350,000
PCI	100
PII	100
Labor	250
Key Contracts	
Supplier 1	500
Distributor	250
Security defenses	100
Total assets	**351,300**

CYBER LIABILITIES

1st Party liabilities
- Revenue
- Business interruption
- Fines/data loss
- Remediation

3rd Party liabilities
- Legal
- Data protection

Loss by system(s)

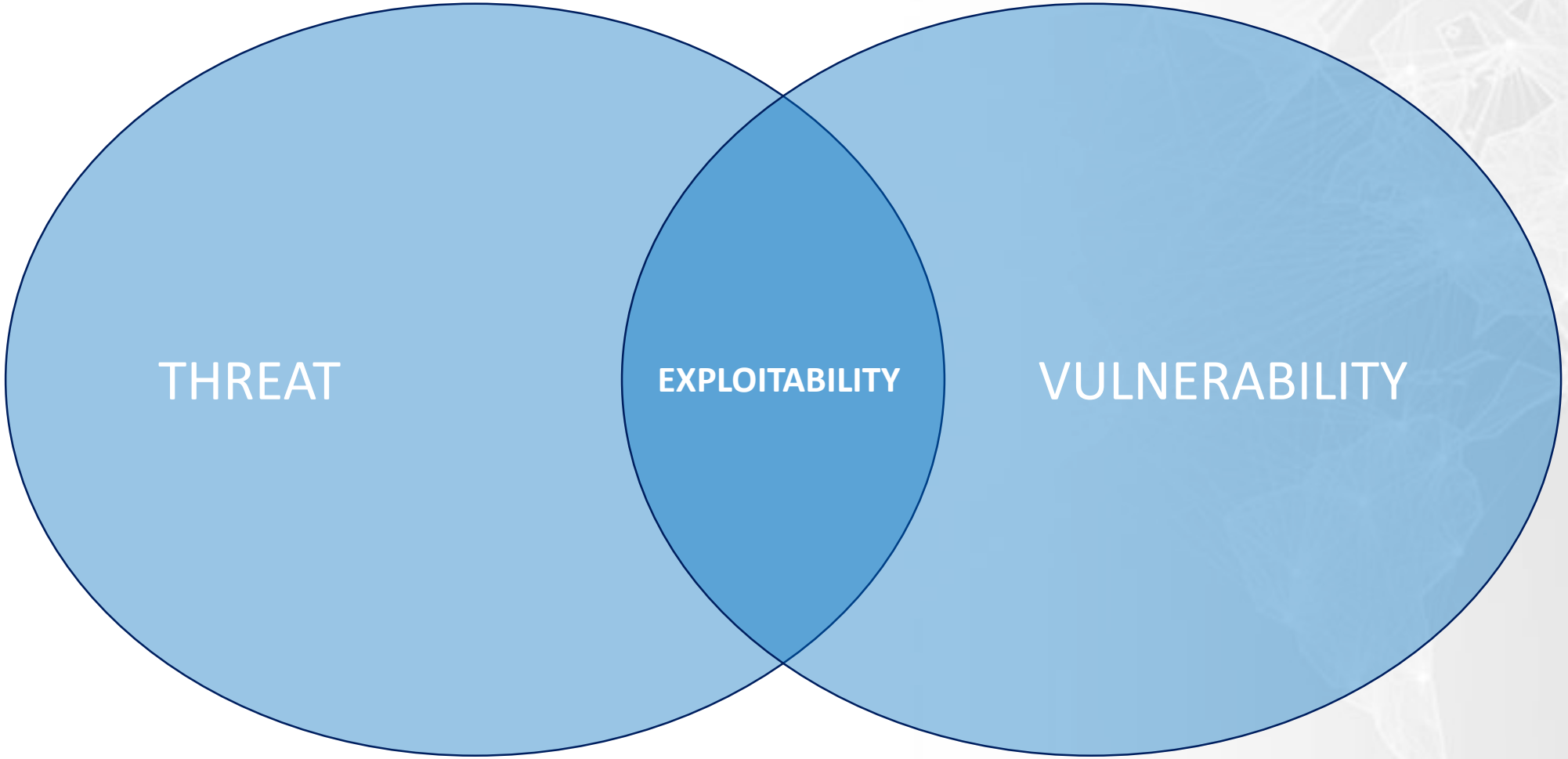
Total liabilities

CYBER EXPLOITABILITY

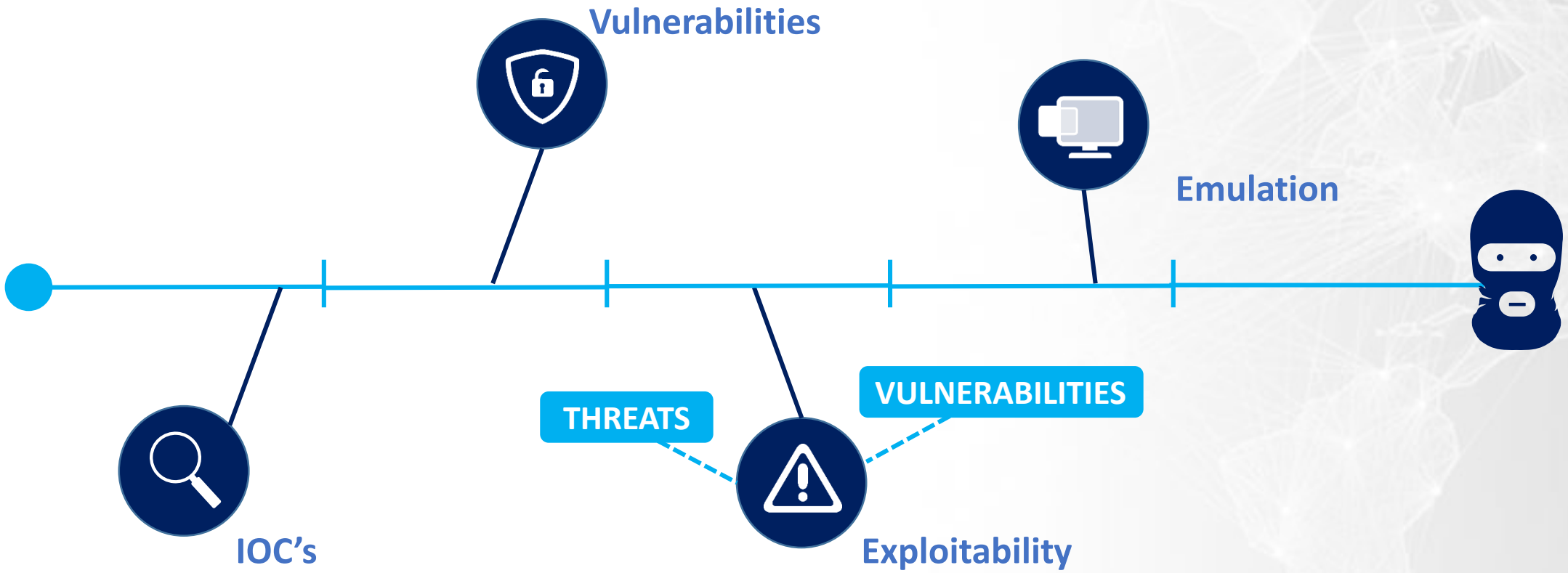
Exploitability
Confidence interval
Probability of attack

numbers in thousands

What is an exploitability?



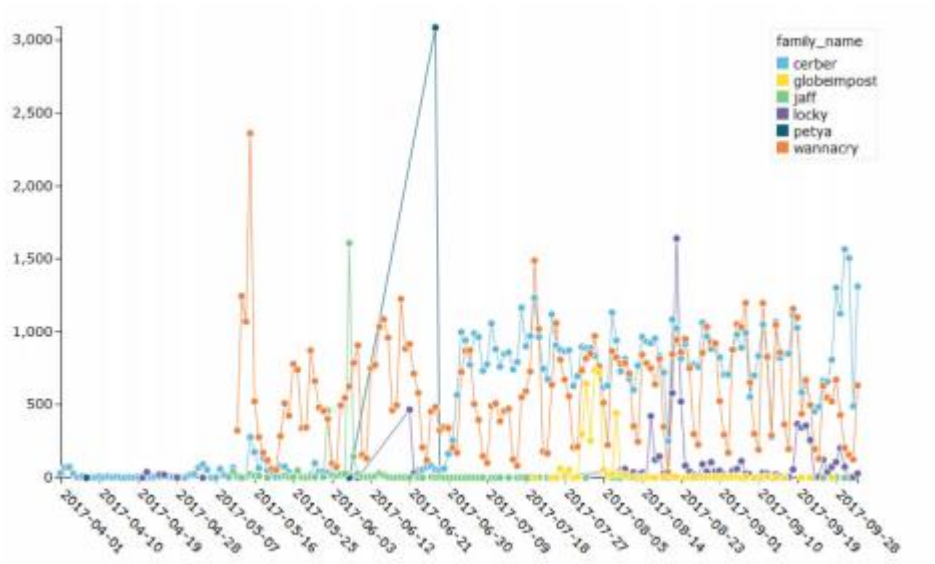
Getting as close as possible to the attacker



You can't compute cyber risk without understanding the attacker

Exploitability (continued) – two ways to measure

OCCURRENCE



IMPACT

TIME PERIOD	MIN LOSS	MAX LOSS
1 hour	1%	5%
8 hours	4%	8%
1 day	8%	16%
1 week	25%	40%

Step 2: Filling in exploitability

CYBER "BALANCE" SHEET

CYBER ASSETS

Point of Sale (POS) system	
Revenue	350,000
PCI	100
PII	100
Labor	250
Key contracts	
Supplier 1	500
Distributor	250
Security defenses	100
Total assets	**351,300**

CYBER LIABILITIES

1st Party liabilities
- Revenue
- Business interruption
- Fines/data loss
- Remediation

3rd Party liabilities
- Legal
- Data protection

Loss by system(s)

Total liabilities

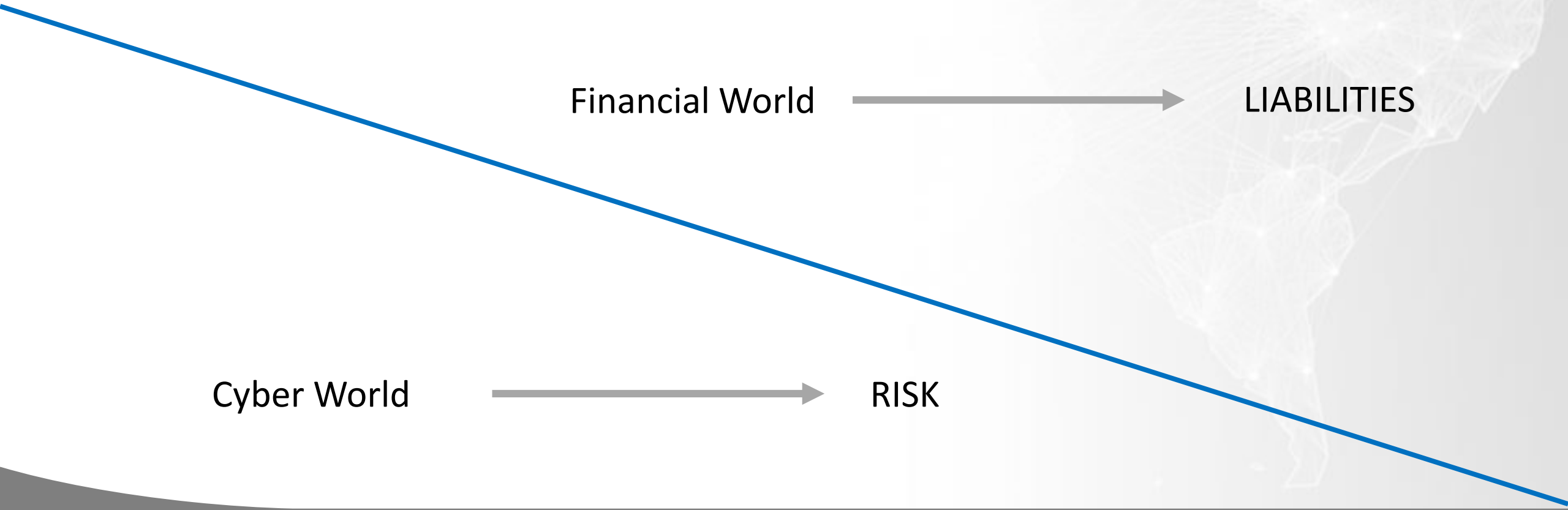
CYBER EXPLOITABILITY

Exploitability	15%
Confidence interval	75%
Probability of attack	6%

numbers in thousands

Now the hard part: Liabilities

1. **What is a liability**
2. **How do you calculate liabilities?**



There are lots of formula's to compute risk

Risk = Loss event frequency x Loss magnitude

Risk = Threats x Likelihood x Impact

Controls

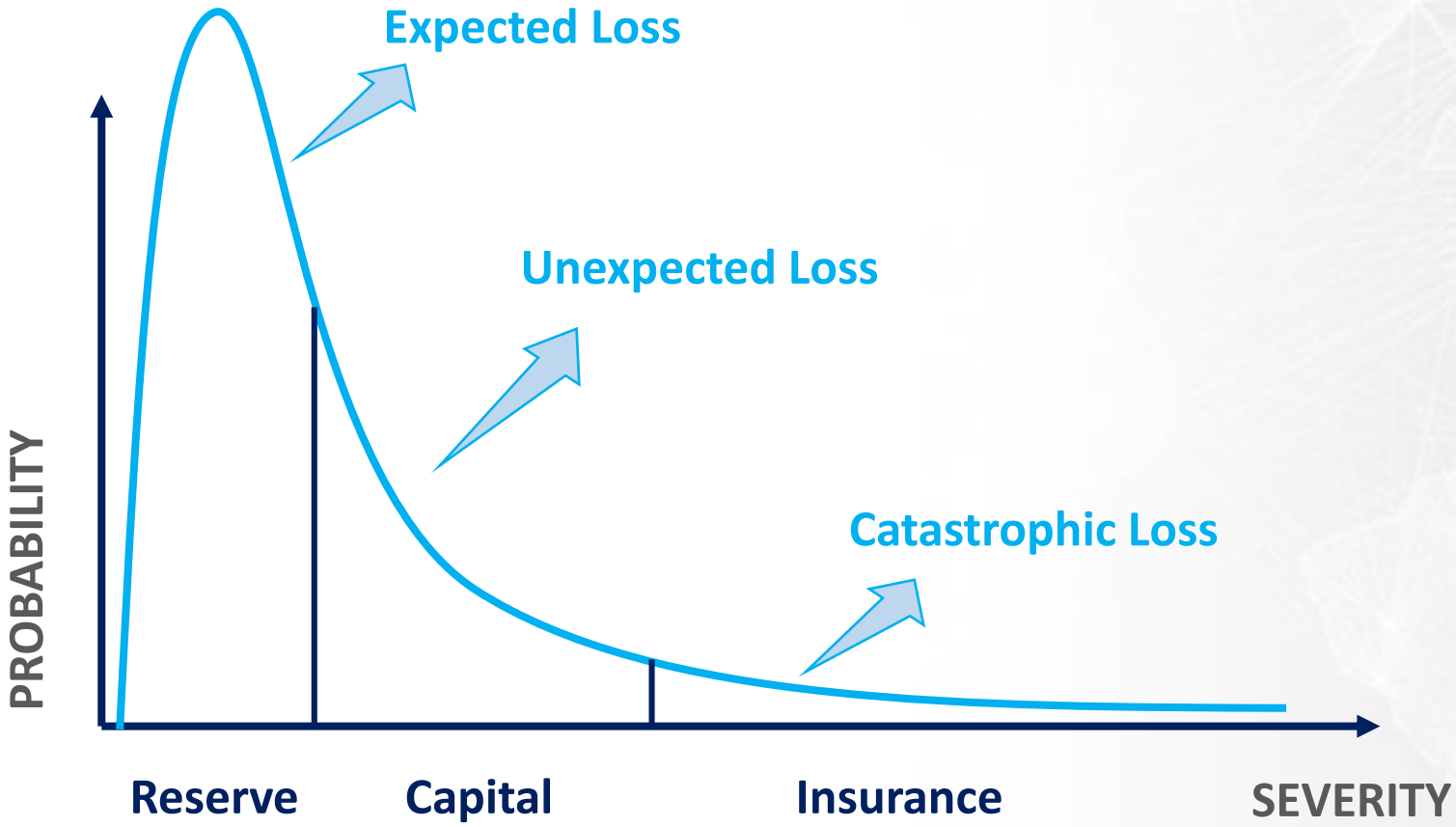
EXPLOITABILITY

$$Risk = \left(\frac{Vulnerability \times Threat}{Counter\ measure\ score} \right) \times Valuation$$

FINANCIAL

$$Risk = \frac{Hazard \times Vulnerability}{Capacity\ to\ cope}$$

Using our equation we produce results like this



Step 3: Filling in liabilities

CYBER "BALANCE" SHEET

CYBER ASSETS

Point of Sale (POS) system	
Revenue	350,000
PCI	100
PII	100
Labor	250
Key contracts	
Supplier 1	500
Distributor	250
Security defenses	100
Total assets	**351,300**

CYBER LIABILITIES

1st Party liabilities	
Revenue	130
Business interruption	7
Fines/data loss	23
Remediation	5
3rd Party liabilities	
Legal	10
Data protection	15
Loss by system(s)	
Total liabilities	**190**

CYBER EXPLOITABILITY

Exploitability	15%
Confidence interval	75%
Probability of attack	6%

numbers in thousands

Note: assets & liabilities don't add up (and they shouldn't)

Key takeaways

1. Aim to provide security leaders with a single view of their current security
2. Get as close to empirical data as possible
3. Perfect is the enemy of good enough


Cyber Balance
SENDING

www.nehemiahsecurity.com