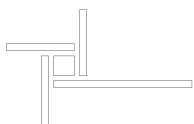
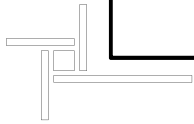
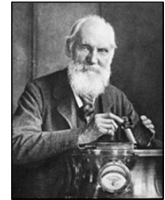


# Addressing the Cyber Language Barrier

## Measuring and Communicating Cyber Risk More Effectively

*"When you can measure what you are speaking  
about and express it in numbers, you know  
something about it." - Lord Kelvin*

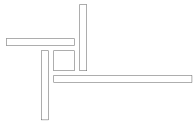


## Disclaimer:

**I am not a lawyer**

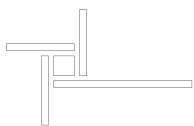


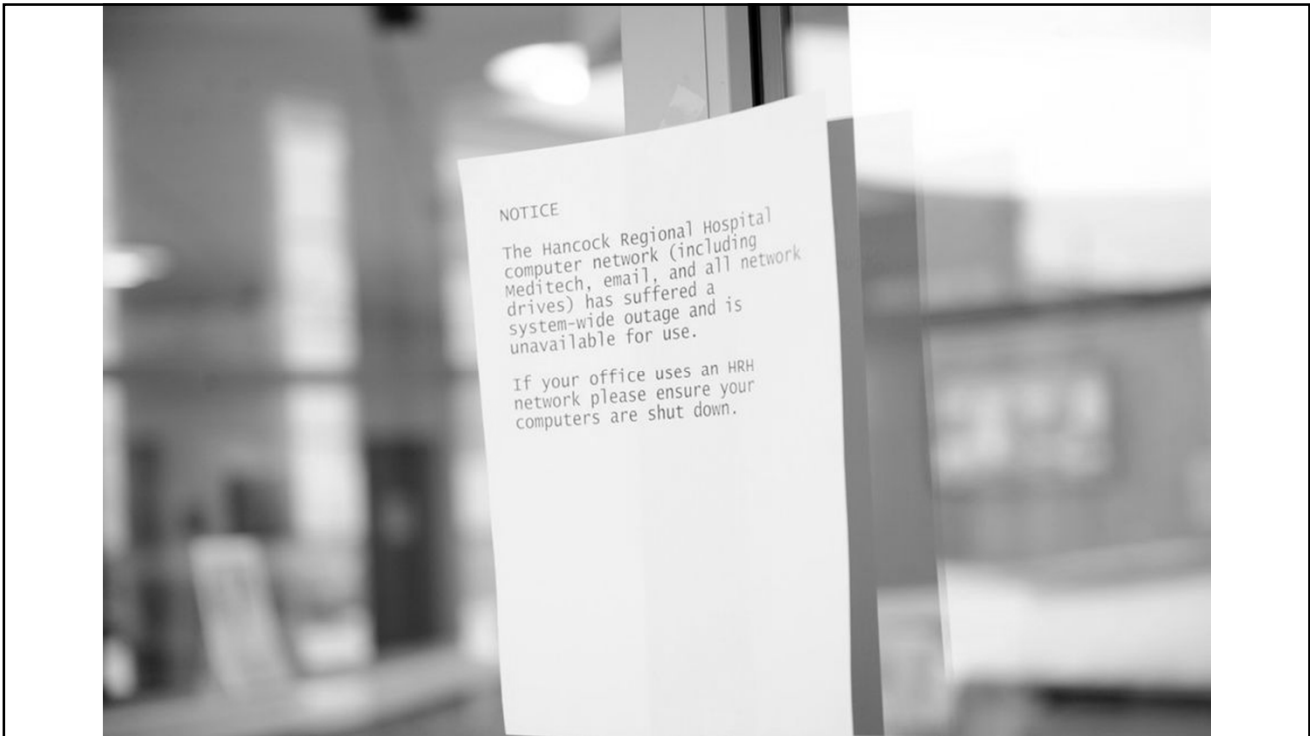
**This is not legal advice**




*Business &  
Healthcare*

# Is Cyber Security an Issue?



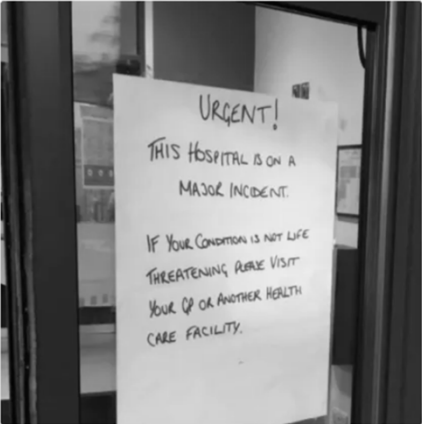




**Jamie Bartlett**  
@JamieJBartlett

Follow


This is the human cost of easy to launch, extremely efficient, digital ransomware attacks. Hospital in Stevenage. Via @BeckyJohnsonSky



**Becky Johnson**  
@BeckyJohnsonSky

Follow

Signs going up at this hospital in Hertfordshire saying this 24 hour urgent care centre is now CLOSED due to cyberattack





**Production shutdown resulted in  
\$240M in lost sales**

**FierceHealthcare**

HEALTHCARE IT PAYER

**Privacy & Security**



**NUANCE**

**Health systems battle workflow disruptions as Nuance  
continues Petya recovery**

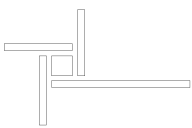
**Adjusted Q3 revenue from  
\$510M to \$494M**



<b>Organization</b>	<b>Estimated Cost</b>	<b>Year</b>
Epsilon	\$4 Billion	2011
Veterans Administration	\$500 Million	2006
Merck	\$275 Million	2017
Hannaford Bros	\$252 Million	2007
Sony PlayStation	\$171 Million	2011
Target	\$162 Million	2013
TJ Maxx	\$162 Million	2007
Heartland Payment	\$140 Million	2008
Anthem	\$100 Million	2015
Sony Pictures Entertainment	\$100 Million	2014
Home Depot	\$56 Million	2014

# \$2.1 Trillion

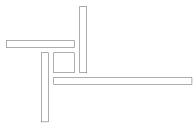
Cost of cyber crime by 2019 – Juniper Networks





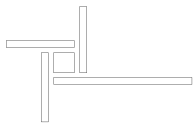
# \$231.94 Billion

Cyber Security Market by 2022

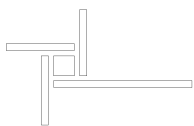


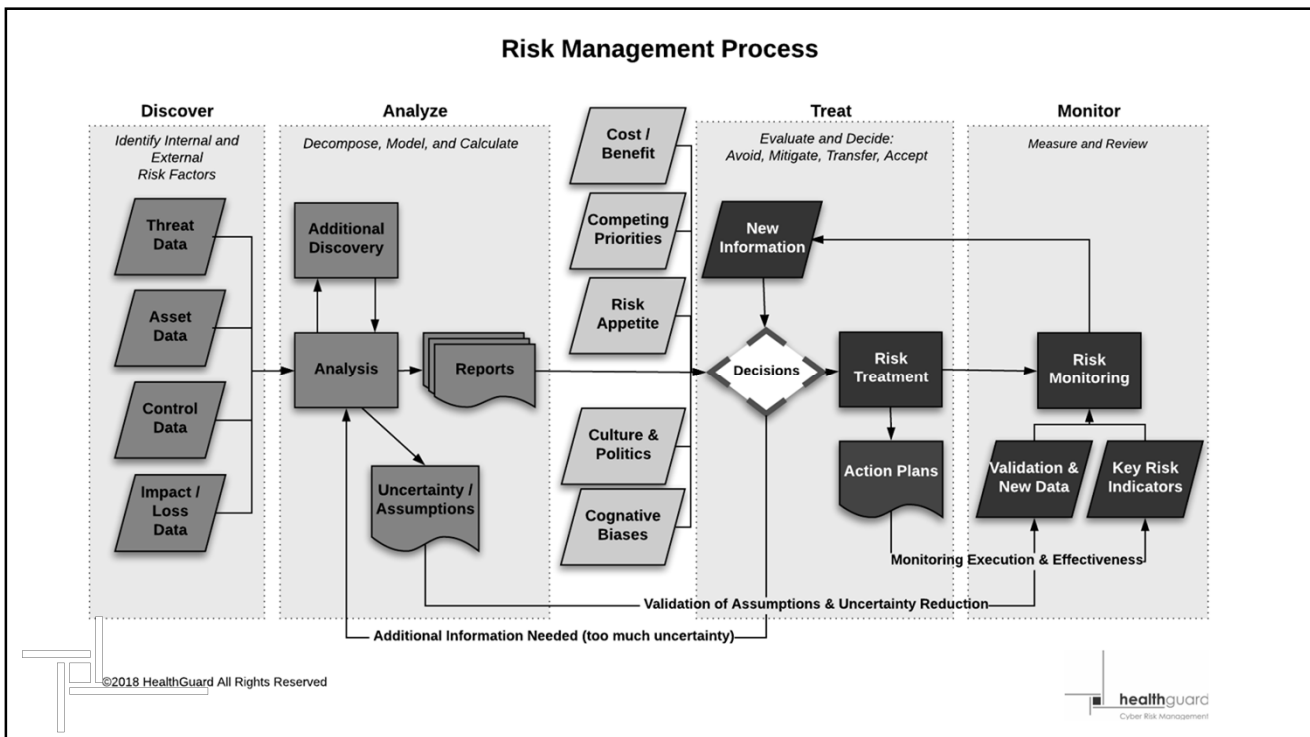
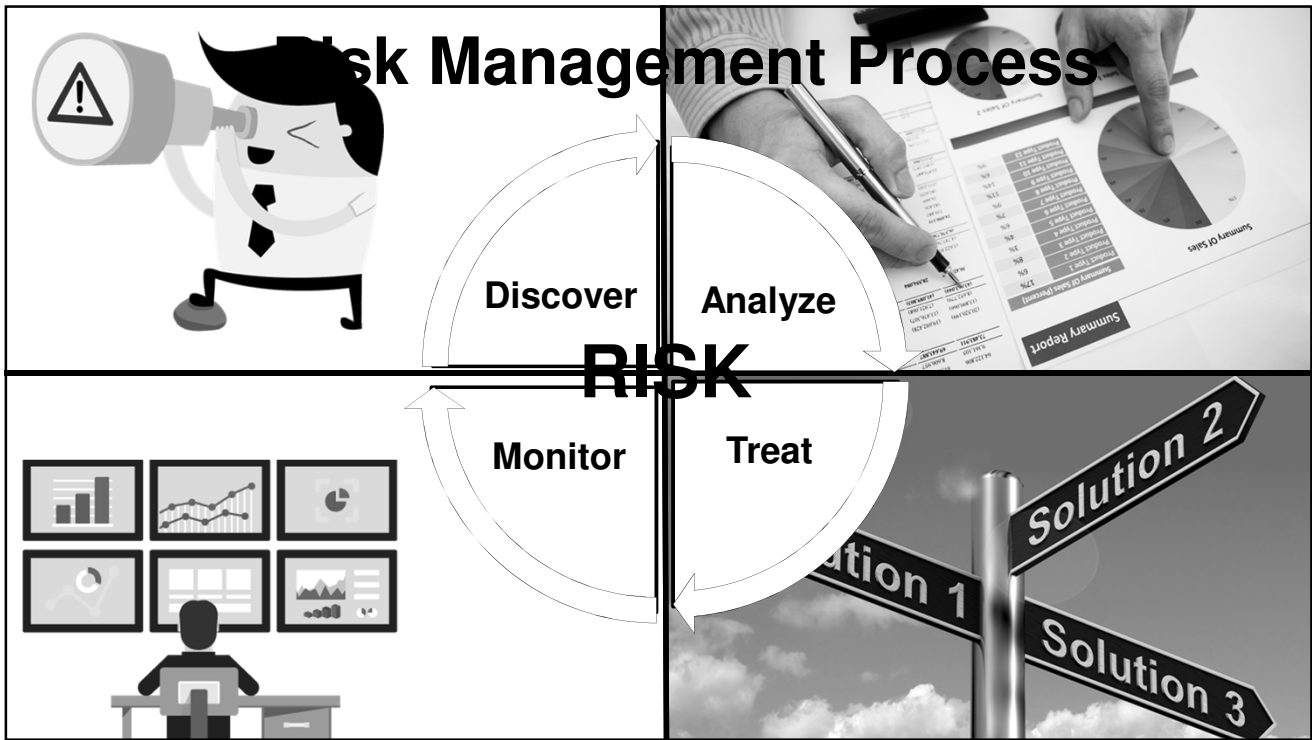


# **Common Analysis Methods**



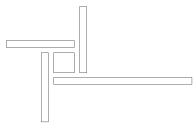
**Why do we need to  
measure (aka analyze)  
risk?**



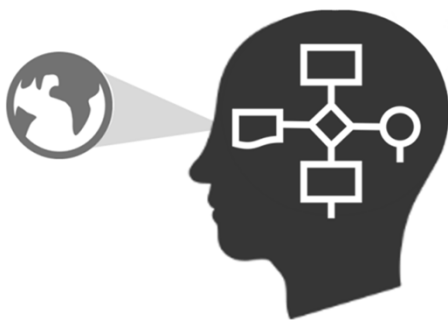


## Informing Decisions / Answering Questions

- How do we prioritize our issues?
- How much should we invest, and where?
- What are we getting for our investment?



## Risk Assessment Approaches

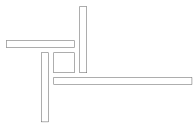


**Mental Models**

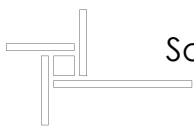


**Analytical Models**

## Case Study:



## Analytical Models



Source: NIST 800-30r1 – Guide for Conducting Risk Assessments

# Qualitative Analysis

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

# Semi-Quantitative Analysis

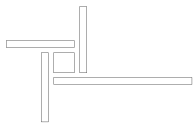
Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
				Overall likelihood=4.375 (MEDIUM)			

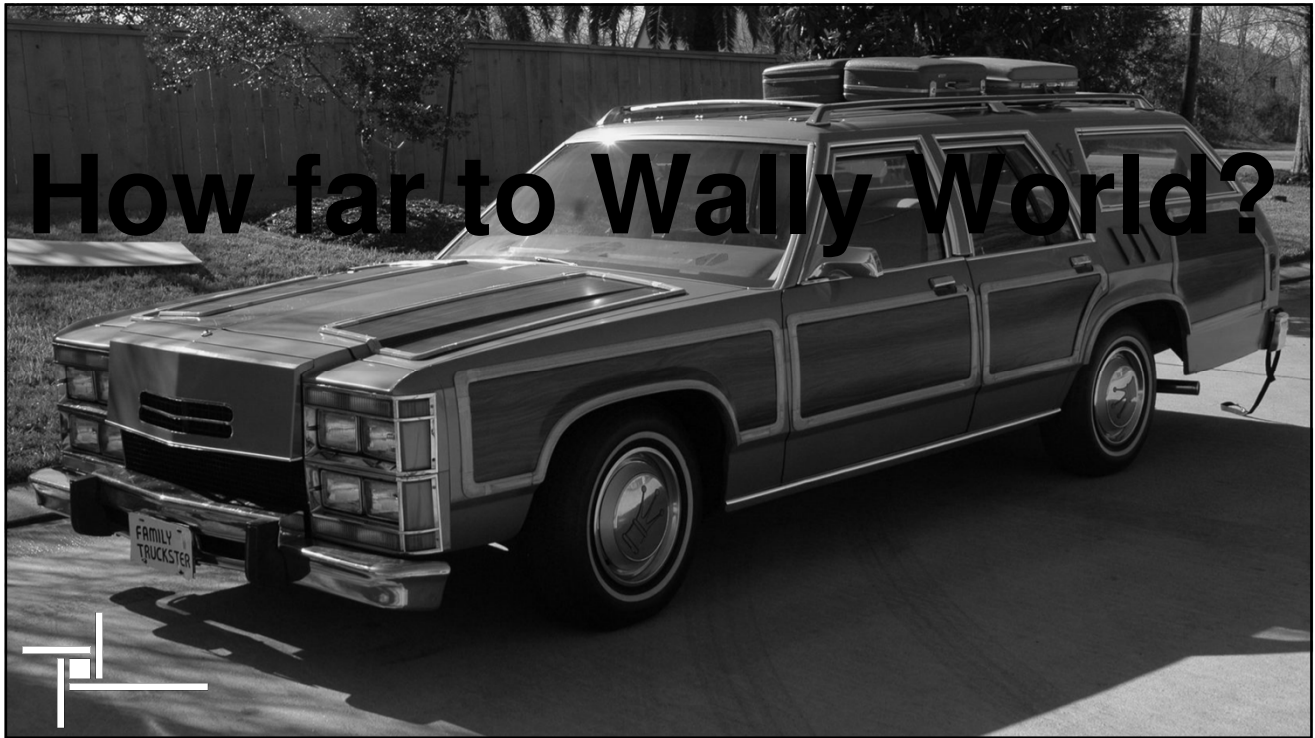
Next, the tester needs to figure out the overall impact to the process. Since there are many factors to consider, the tester can take an estimate based on the factors, or they can average the score for each of the factors. Again, the score is low, so less than is medium, and 6 to 9 is high. For example,

# Risk Rating: 20.781

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

# What if everything was measured like cyber risk?





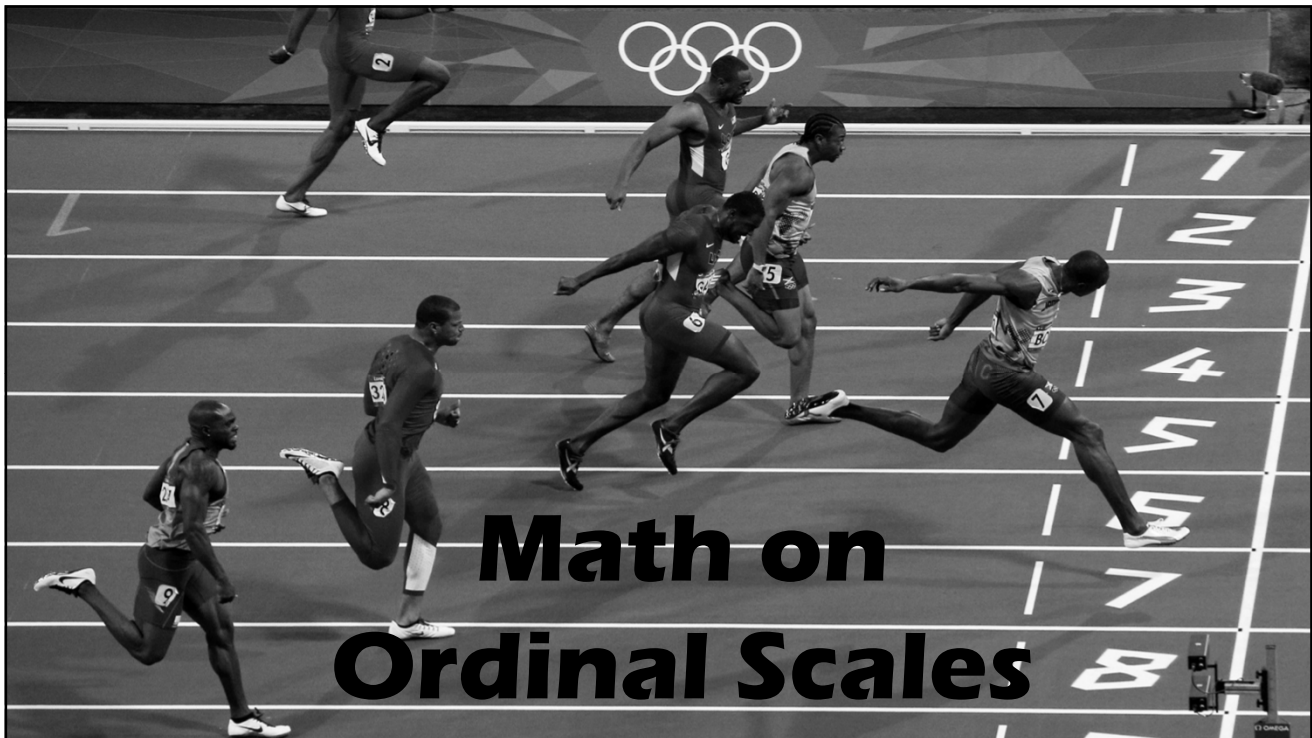




Organization	Security Risk Ratings	Year
Epsilon	\$4.25 billion	2011
Veterans Administration	\$500.25 million	2006
Merck	\$275.25 million	2017
Hannaford Bros	\$252.25 million	2007
Sony PlayStation	\$171.25 million	2011
Target	\$162.25 million	2013
TJ Maxx	\$162.25 million	2007
Heartland Payment	\$140.24 million	2008
Anthem	\$100.23 million	2015
Sony Pictures Entertainment	\$100.23 million	2014
Home Depot	\$56.22 million	2014

Organization	Security Risk Levels	Year
Epsilon	Very High	2011
Veterans Administration	Very High	2006
Merck	Very High	2017
Hannaford Bros	Very High	2007
Sony PlayStation	High	2011
Target	High	2013
TJ Maxx	High	2007
Heartland Payment	High	2008
Anthem	High	2015
Sony Pictures Entertainment	High	2014
Home Depot	Medium High	2014

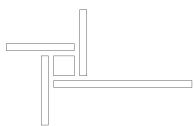
## Common Analysis Issues / Pitfalls



## Semi-Quantitative Analysis

Impact Score	Impact to Mission <i>Mission: Provide information to help remote patients stay healthy.</i>	Impact to Objectives <i>Objectives: Operate profitably.</i>	Impact to Obligations <i>Obligations: Patients must not be harmed by compromised information.</i>
1	Patients continue to access helpful information, and outcomes are on track.	Profits are on target.	Patients do not experience loss of service or protection.
2	Some patients may not get all the information they need as they request it.	Profits are off target, but are within planned variance.	Patients may be concerned, but not harmed.
3	Some patients cannot access the information they need to maintain good health outcomes.	Profits are off planned variance and may take a fiscal year to recover.	Some patients may be harmed financially or reputationally after compromise of information or services.
4	Many patients consistently cannot access beneficial information.	Profits may take more than a fiscal year to recover.	Many patients may be harmed financially or reputationally.
5	We can no longer provide helpful information to remote patients.	The organization cannot operate profitably.	Some patients may be harmed financially, reputationally, or physically up to and including death.

Likelihood Score	Foreseeability
1	<b>Not foreseeable.</b> This is not plausible in the environment.
2	<b>Foreseeable.</b> This is plausible, but not expected.
3	<b>Expected.</b> We are certain this will eventually occur.
4	<b>Common.</b> This happens repeatedly.
5	<b>Current.</b> This may be happening now.



# Semi-Quantitative Analysis

Impact Score	Impact to Mission <i>Mission: Provide information to help remote patients stay healthy.</i>	Impact to Objectives <i>Objectives: Operate profitably.</i>	Impact to Obligations <i>Obligations: Patients must not be harmed by compromised information.</i>
1	Patients continue to access helpful information, and outcomes are on track.	Profits are on target.	Patients do not experience loss of service or protection.
2	Some patients may not get all the information they need as they request it.	Profits are off target, but are within planned variance.	Patients may be concerned, but not harmed.
3	Some patients cannot access the information they need to maintain good health outcomes.	Profits are off planned variance and may take a fiscal year to recover.	Some patients may be harmed financially or reputationally after compromise of information or services.
4	Many patients consistently cannot access beneficial information.	Profits may take more than a fiscal year to recover.	Many patients may be harmed financially or reputationally.
5	We can no longer provide helpful information to remote patients.	The organization cannot operate profitably.	Some patients may be harmed financially, reputationally, or physically up to and including death.

Impact Threshold	x	Likelihood Threshold	=	Risk Threshold
3	x	3	=	9
... therefore ...				
Acceptable Risk				< 9

Likelihood Score	Foreseeability
1	Not foreseeable. This is not plausible in the environment.
2	Foreseeable. This is plausible, but not expected.
3	Expected. We are certain this will eventually occur.
4	Common. This happens repeatedly.
5	Current. This may be happening now.

# Semi-Quantitative Analysis

CIS Control 1.1 - Utilize an Active Discovery Tool			
Asset	All devices	Owner	IT
Vulnerability	Sporadic asset scans	Threat	Undetected compromised systems
Risk Scenario	Irregular asset scans may not identify compromised systems that join the network and attack routable systems.		
Mission Impact	2	Likelihood	<u>3</u>
Objectives Impact	<u>4</u>	Risk Score: Max(Impact) x Likelihood	12
Obligations Impact	<u>4</u>		
Treatment	Implement NAC, and a system assessment process for alerted devices.		
Mission Impact	2	Likelihood	<u>2</u>
Objectives Impact	<u>4</u>	Risk Score: Max(Impact) x Likelihood	8
Obligations Impact	<u>4</u>		

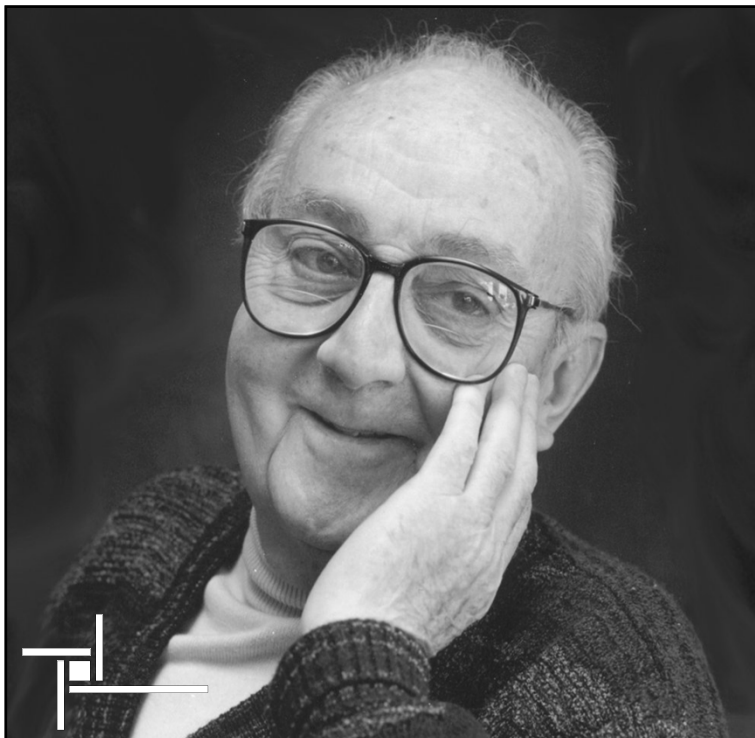
15

## Measurement Scales

Scale	Order	Distance	True Zero	Examples
Nominal	No	No	No	Color, Gender, Ethnicity, Country
Ordinal	Yes	No	No	Rating Scales, Rank Order
Interval	Yes	Yes	No	Time of Day, IQ, Likert Scale, Temp.
Ratio	Yes	Yes	Yes	Age, Height, Cost, Weight

## Measurement Scales

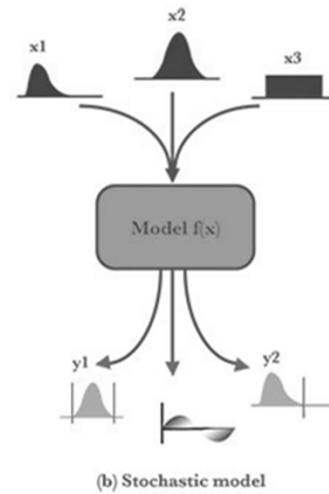
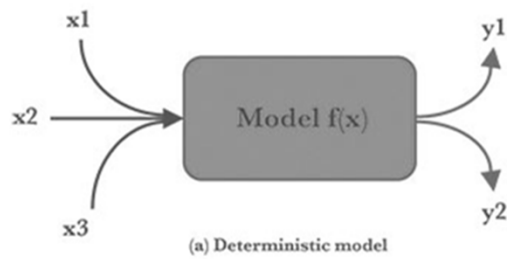
Scale	Permitted Mathematical Operations
Nominal	Counting
Ordinal	Greater than/less than
Interval	Addition, subtraction, multiplication, division; cannot make ratio statements
Ratio	Any, including ratios



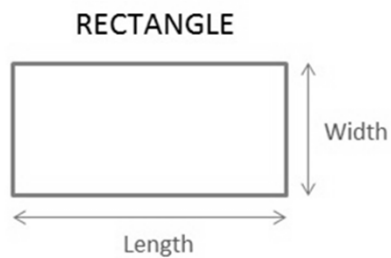
**Essentially, all  
models are wrong,  
but some are  
useful.**

- George E. P. Box

## Wrong Type of Model



### Deterministic Models



Area of rectangle = *Length X Width*

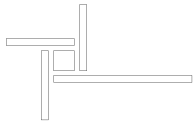
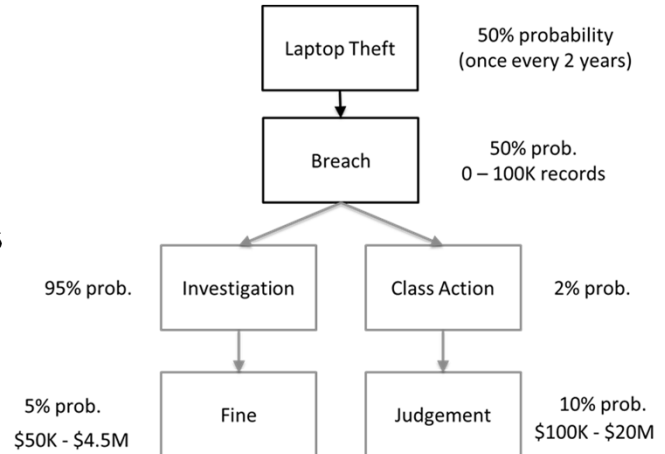
### Stochastic Models



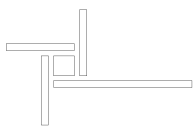
## Poor Model Design

**threat x**  
**Risk = vulnerability x**  
**consequence**

vs



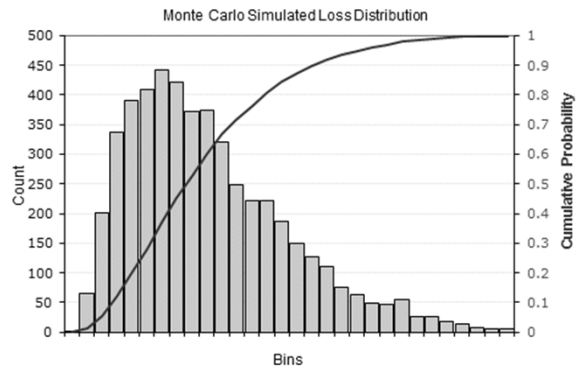
# Don't Account for Cognitive Biases



# Quantitative Analysis

The histogram table below is used for calculating the likelihood of landing on a specific value during the simulation of loss over the 5000 sample trials.

Histogram Plot Calculations				
Min \$	5,197.12			
Max \$	112,835.58			
Number	5000			
Bins	Count	Likelihood	Scaled	Total
\$ 5,197.12	1	0.02%	5.6E-08	0.0002
\$ 8,785.07	66	1.32%	3.7E-06	0.0134
\$ 12,373.02	202	4.04%	1.1E-05	0.0538
\$ 15,960.96	338	6.77%	1.9E-05	0.1214
\$ 19,548.91	390	7.81%	2.2E-05	0.1994
\$ 23,136.86	410	8.21%	2.3E-05	0.2814
\$ 26,724.81	443	8.87%	2.5E-05	0.37
\$ 30,312.76	421	8.43%	2.3E-05	0.4542
\$ 33,900.71	372	7.45%	2.1E-05	0.5286
\$ 37,488.66	375	7.51%	2.1E-05	0.6036
\$ 41,076.61	320	6.41%	1.8E-05	0.6676
\$ 44,664.55	249	4.98%	1.4E-05	0.7174
\$ 48,252.50	222	4.44%	1.2E-05	0.7618
\$ 51,840.45	222	4.44%	1.2E-05	0.8062

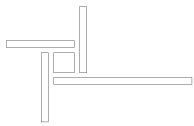


This graph is built up from the histogram plot calculations table and shows the loss distribution function as a bar chart, as well as the cumulative probability distribution function.

## Quantifying risk in three steps

## Risk Analysis Basics

1. Develop The Risk Scenarios
2. Build the Model/Gather Data
3. Run The Simulation



## Risk Scenario

Scenarios are a powerful tool in a risk manager's armory—they help professionals ask the right questions and prepare for the unexpected. **Scenario analysis has become a 'new' and best practice in enterprise risk management (ERM)**

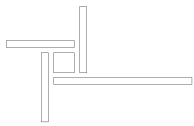
(Source: [isaca.org](http://isaca.org))



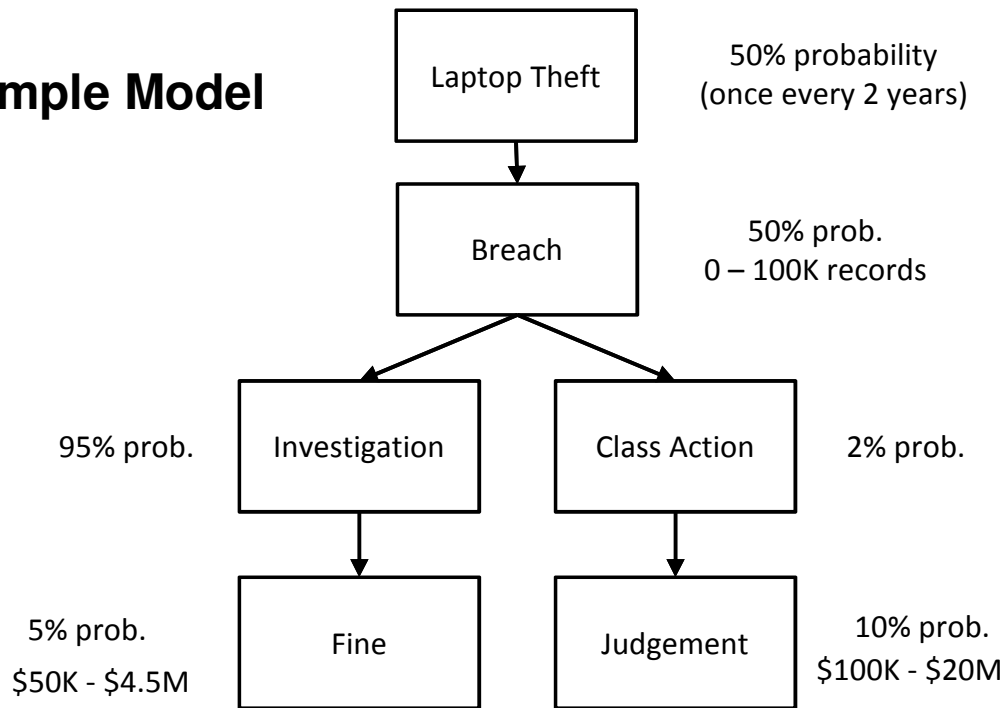
## Example Risk Scenario Statement

Risk scenario statement:

*What is the risk associated with PHI being exposed via a lost/stolen laptop?*



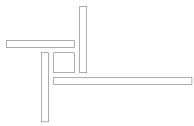
## Example Model



## **Simulations**

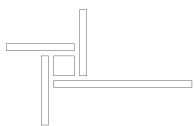
Two primary tools:

1. Probability Distributions (e.g. PERT)
2. Stochastic Modeling (e.g. Monte Carlo Simulation)

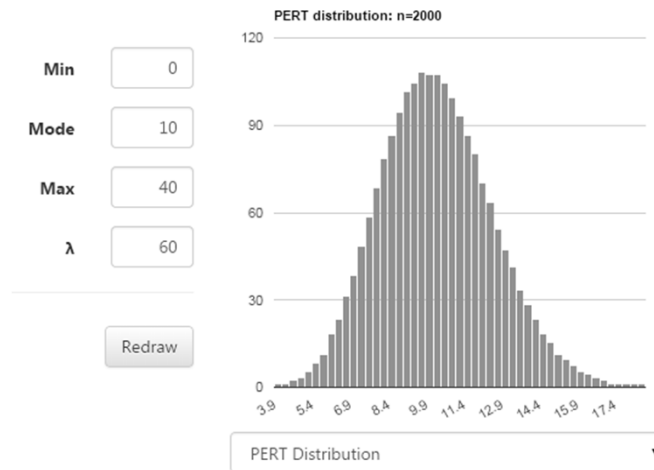


## **Pert Distributions**

Form of probability distribution used  
to model expert data.



## Pert Distribution Histogram



## Monte Carlo Simulation

Computerized mathematical technique that allows people to account for risk in quantitative analysis and decision making.

## **Exercise:**

**Auditors report lack of laptop encryption is a “high risk” issue.**

**Encryption will require a \$200-250K investment.**

**CFO wants to know if this is worth the investment.**



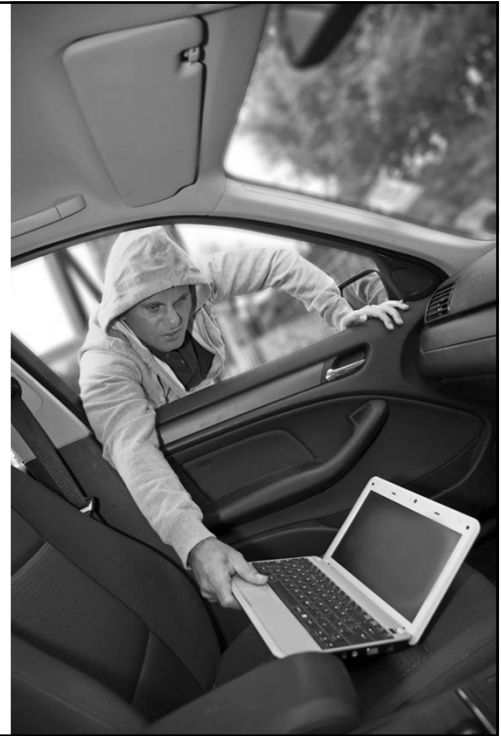
## **Primary Loss Event Frequency**

	<b>Min (95% CI)</b>	<b>Most Likely</b>	<b>Max (95% CI)</b>
<b>LEF</b>	<b>0</b>	<b>1</b>	<b>5</b>



## Primary Loss Magnitude

	Min (95% CI)	Most Likely	Max (95% CI)
<b>Replacement Costs</b>	<b>\$1,200</b>	<b>\$1,750</b>	<b>\$2,500</b>
<b>Response Costs</b>	<b>\$2,500</b>	<b>\$75K</b>	<b>\$250K</b>

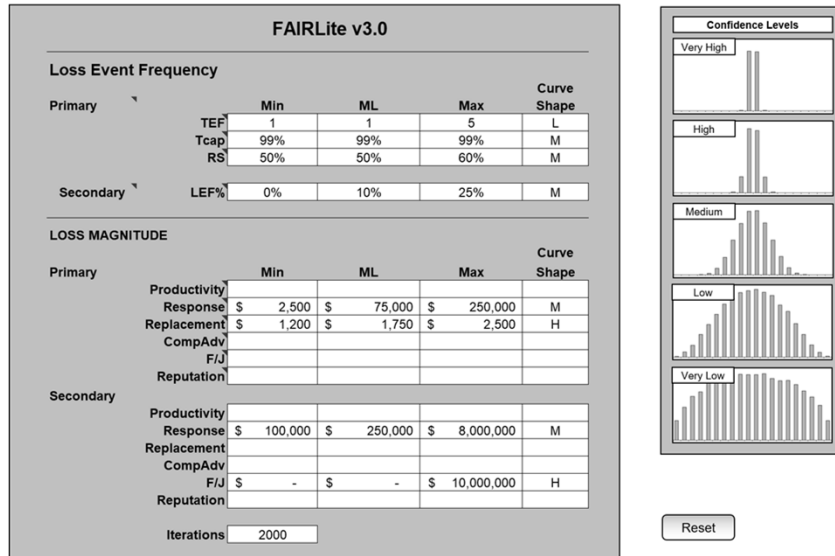


## Secondary Loss Magnitude

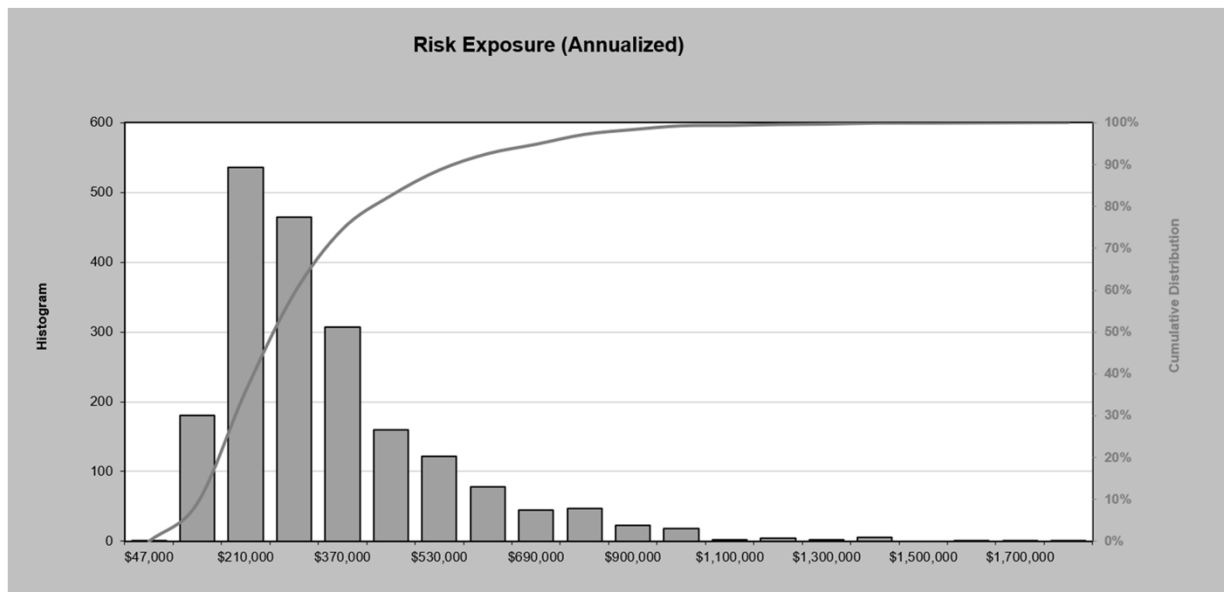
	Min (95% CI)	Most Likely	Max (95% CI)
<b>Response Costs</b>	<b>\$100K</b>	<b>\$250K</b>	<b>\$8M</b>
<b>Fines / Judgement</b>	<b>\$0</b>	<b>\$0</b>	<b>\$10M</b>



## Monte Carlo Simulation



## Simulation Output

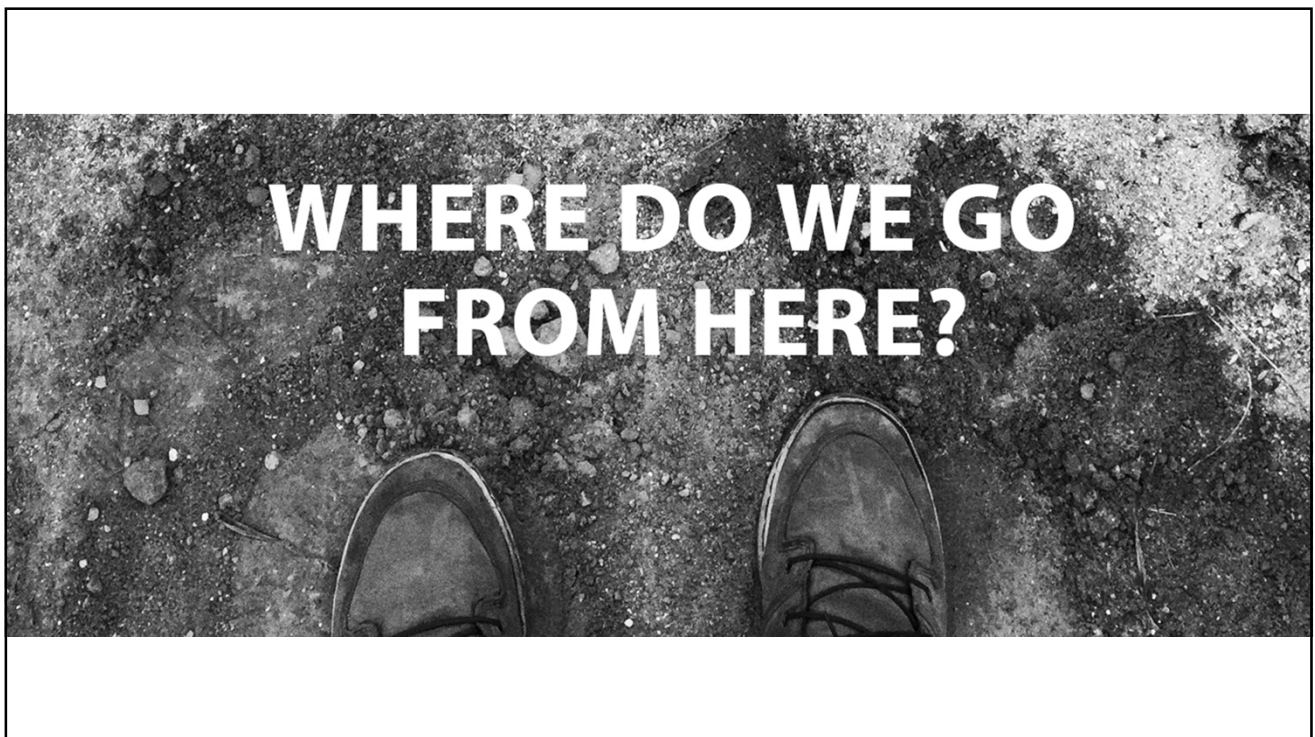
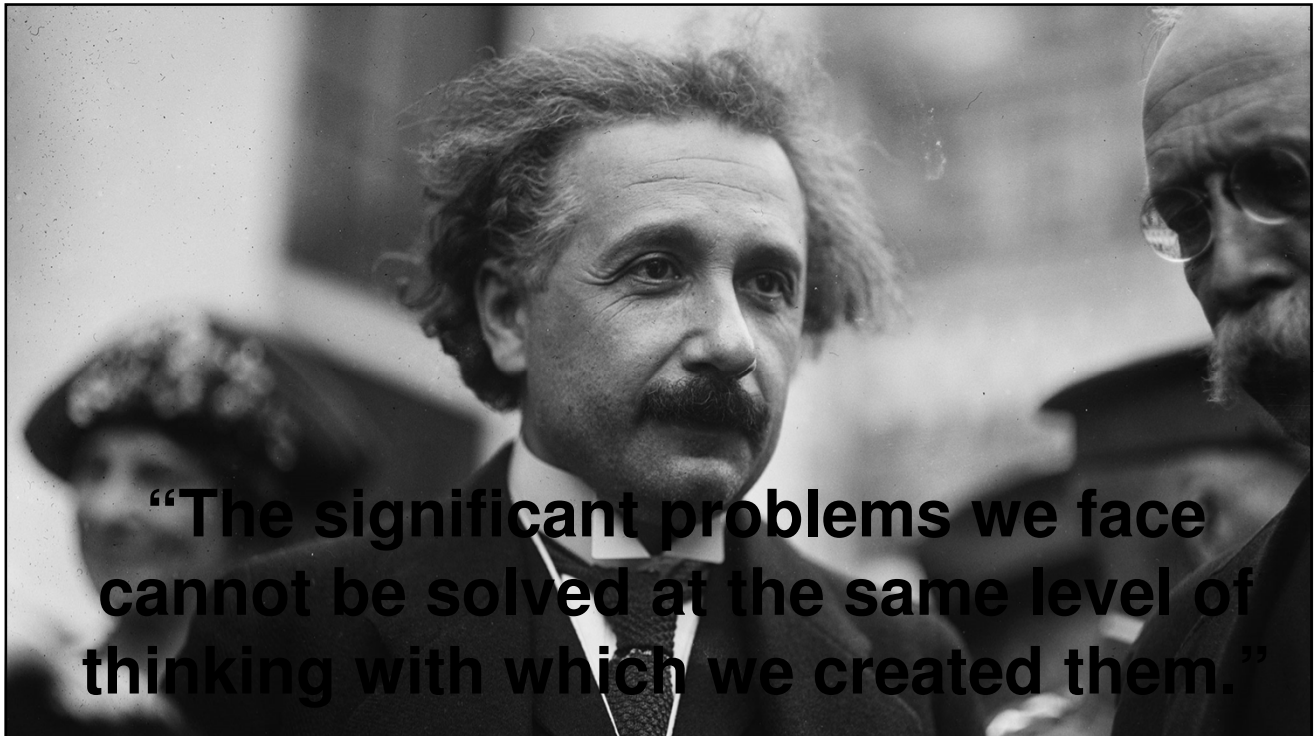


## Simulation Output

Primary		Minimum	Average	Mode	Maximum
LEF (yr)		1.00	1.63	1.08	4.19
LM	\$	13,570	\$ 81,416	\$ 77,864	\$ 185,020
Secondary		Minimum	Average	Mode	Maximum
LEF (yr)		0.00	0.26	0.13	1.01
LM	\$	122,599	\$ 657,007	\$ 321,225	\$ 2,770,946
<b>Total Exposure</b> (Annualized)		\$ 13,677	\$ 306,874	\$ 124,815	\$ 3,569,140
Vuln		100%			

## Simulation Output

Primary		Minimum	Average	Mode	Maximum
	LEF (yr)	1.00	1.63	1.08	4.19
	LM	\$ 13,570	\$ 81,416	\$ 77,864	\$ 185,020
Secondary					
	LEF (yr)	0.00	0.26	0.13	1.01
	LM	\$ 122,599	\$ 657,007	\$ 321,225	\$ 2,770,946
Total Exposure (Annualized)					\$ 3,569,140
Vul	Risk Levels		Avg Exp > ▾		
	Very High		\$ 1,000,000		
	High		\$ 100,000		
	Medium		\$ 10,000		
	Low		\$ 1,000		
	Very Low		\$ 100		



PUBLIC BETA  
COMING SOON



## Introducing CyberEHR Analyze

[www.healthguardsecurity.com/cyberehr-analyze/](http://www.healthguardsecurity.com/cyberehr-analyze/)



**Apolonio “Apps” Garcia**

 @appsgarcia  
[agarcia@healthguardsecurity.com](mailto:agarcia@healthguardsecurity.com)  
 513.549.4272