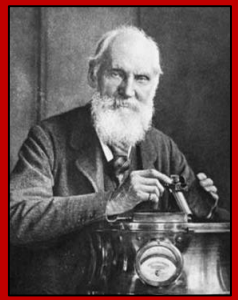
# Burned by Heatmaps

## Introduction to Quantitative Risk Analysis

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




hello
MY NAME IS

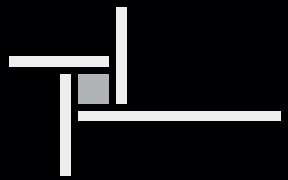
# Disclaimer:

I am not a lawyer

This is not legal advice

Business & Healthcare

# Is Cyber Security an Issue?



| Organization | Estimated Cost | Year |
|---|---|---|
| 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 |

MERCK


# Production shutdown resulted in $240M in lost sales

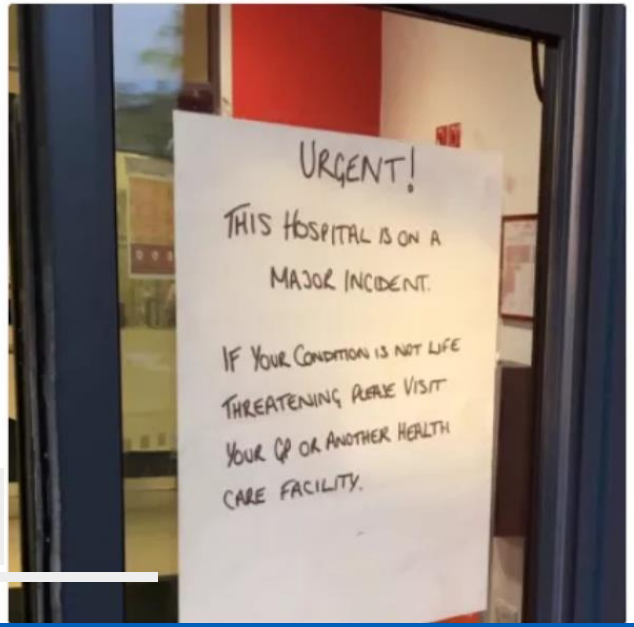

# Adjusted Q3 revenue from $510M to $494M

# NHS

**Jamie Bartlett**
@JamieJBartlett

Follow

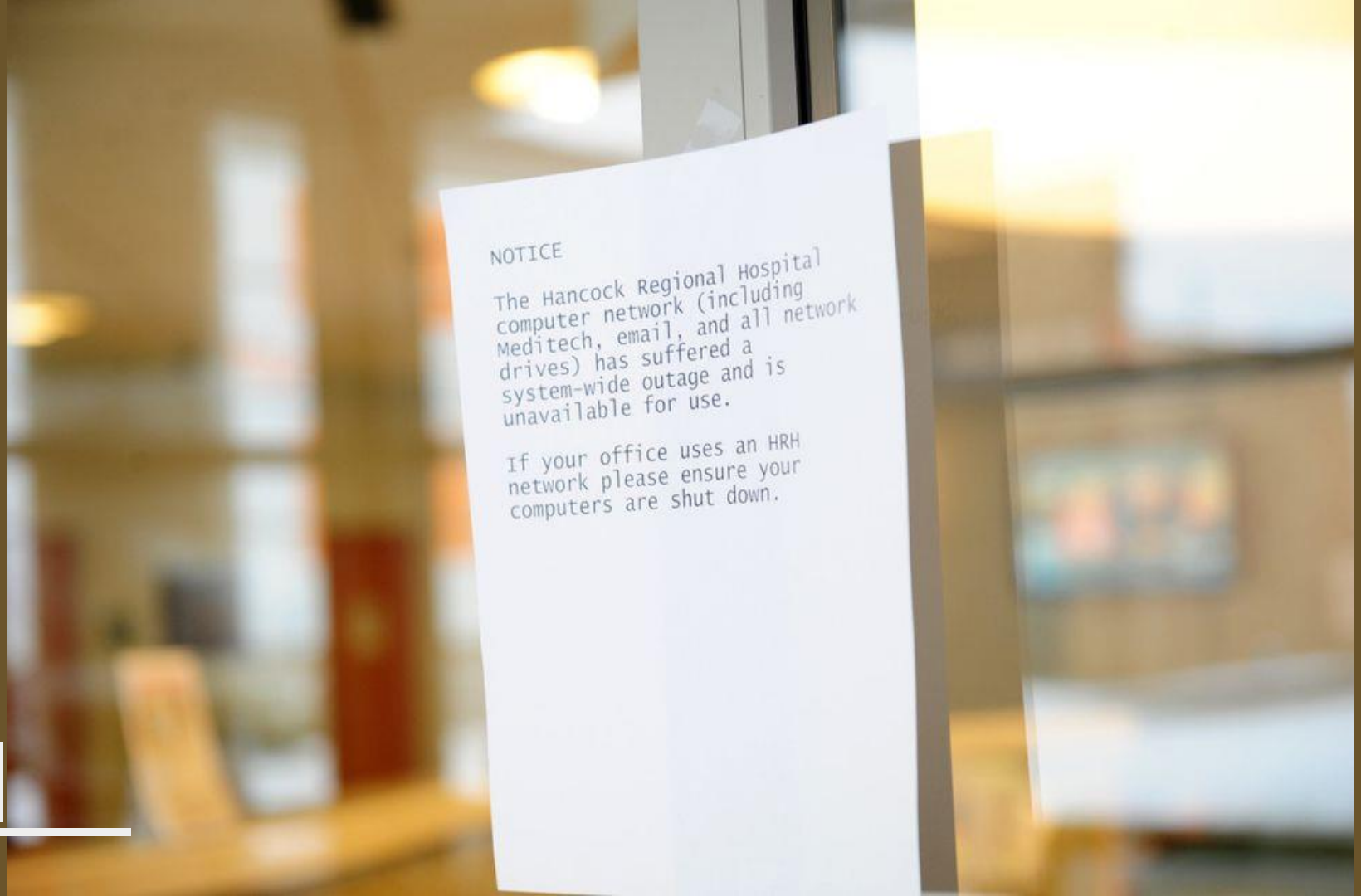
This is the human cost of easy to launch, extremely efficient, digital ransomware attacks. Hospital in Stevenage. Via @BeckyJohnsonSky



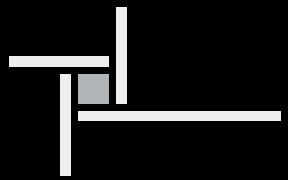

**Becky Johnson**
@BeckyJohnsonSky

Follow

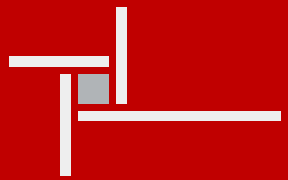
Signs going up at this hospital in Hertfordshire saying this 24 hour urgent care centre is now CLOSED due to cyberattack

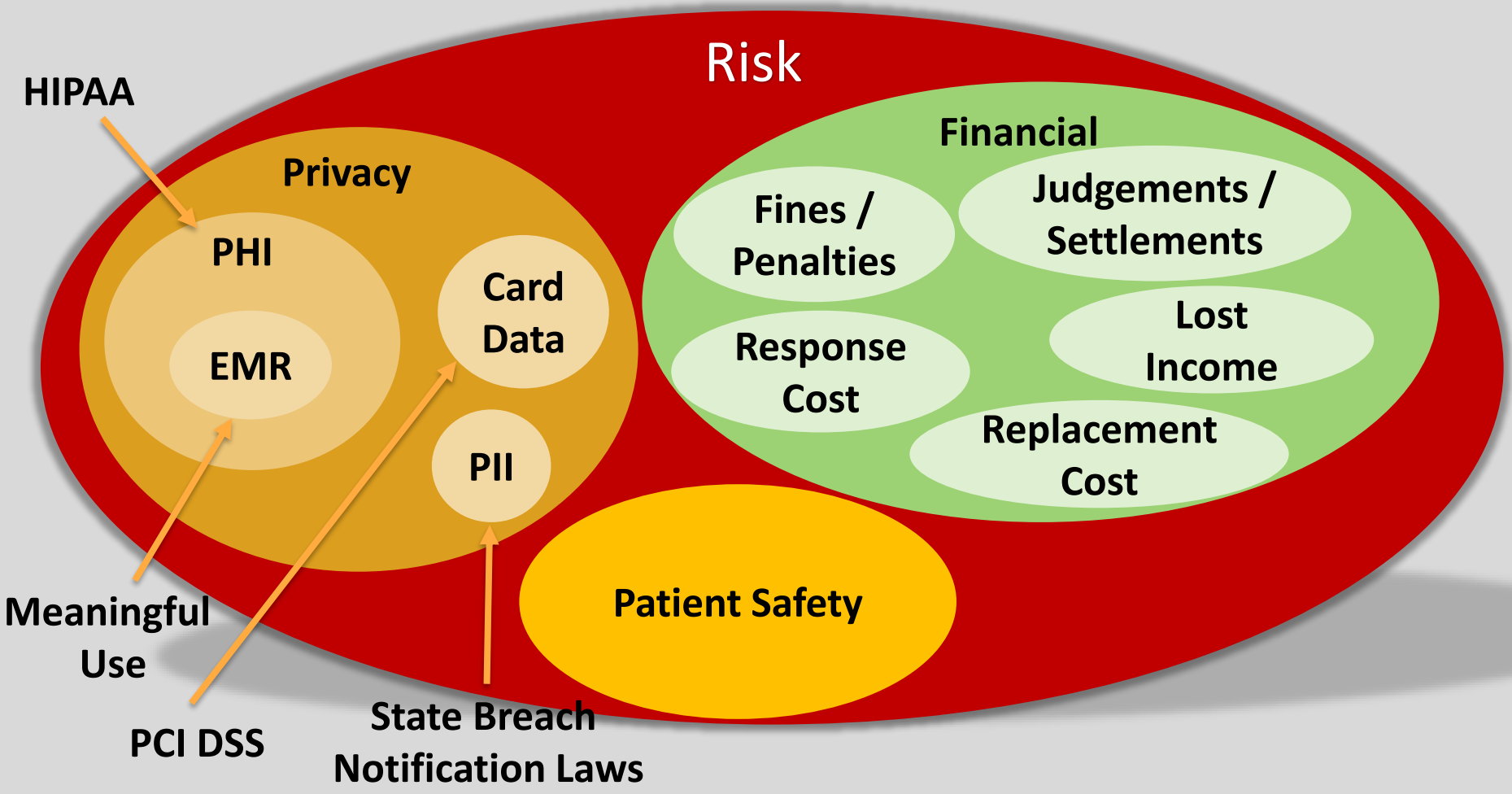

NOTICE
The Hancock Regional Hospital computer network (including Meditech, email, and all network drives) has suffered a system-wide outage and is unavailable for use.
If your office uses an HRH network please ensure your computers are shut down.

# What is risk?

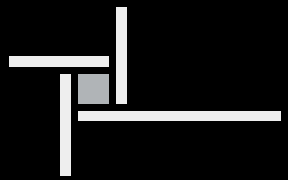


**Risk is the probable frequency and probably magnitude of loss/harm**




Risk
HIPAA
Privacy
PHI
EMR
Card Data
PII
Financial
Fines / Penalties
Judgements / Settlements
Response Cost
Lost Income
Replacement Cost
Patient Safety
Meaningful Use
PCI DSS
State Breach Notification Laws

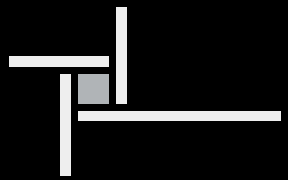
# How do we manage risk?



# Risk Management Process

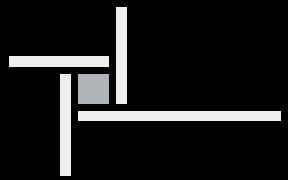


# How do we make security decisions?

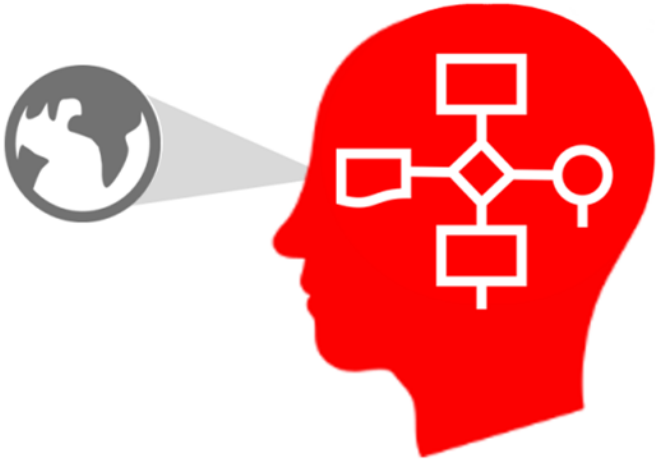


# Case Study:

# How do we assess risk?



# Risk Assessment Approaches



**Mental Models**

**Analytical Models**

# Analytical Models

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

# Method 1: Qualitative Analysis

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


What is the size of the enemy force?


What is the size of the enemy force?
Medium

# Method 2: Semi-Quantitative Analysis

| Threat agent factors | | | |
|---|---|---|---|
| Skill level | Motive | Opportunity | Size |
| 5 | 2 | 7 | 1 |

| Vulnerability factors | | | |
|---|---|---|---|
| Ease of discovery | Ease of exploit | Awareness | Intrusion detection |
| 3 | 6 | 9 | 2 |

Overall likelihood=4.375 (MEDIUM)

Next, the tester needs to figure out the overall impact. The process is similar when calculating the impact. The answer will be obvious, but the tester can take an estimate based on the factors, or they can average the score for each of the factors. Again, less than 3 is low, 3 to less than 6 is medium, and 6 to 9 is high. For example:

**Risk Rating: 20.781**

| Technical Impact | | | |
|---|---|---|---|
| Loss of confidentiality | Loss of integrity | Loss of availability | Loss of accountability |
| 9 | 7 | 5 | 8 |

Overall technical impact=7.25 (HIGH)

| Business Impact | | | |
|---|---|---|---|
| Financial damage | Reputation damage | Non-compliance | Privacy violation |
| 1 | 2 | 1 | 5 |

Overall business impact=2.25 (LOW)

# Method 2: Semi-Quantitative Analysis

| Impact Score | Impact to Mission<br>*Mission: Provide information to help remote patients stay healthy.* | Impact to Objectives<br>*Objectives: Operate profitably.* | Impact to Obligations<br>*Obligations: Patients must not be harmed by compromised information.* |
|---|---|---|---|
| 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 physicall up to and including death. |

| 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. |

# Method 2: Semi-Quantitative Analysis

| Impact Score | Impact to Mission<br>*Mission: Provide information to help remote patients stay healthy.* | Impact to Objectives<br>*Objectives: Operate profitably.* | Impact to Obligations<br>*Obligations: Patients must not be harmed by compromised information.* |
|---|---|---|---|
| 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 physicall 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. |

# Method 2: Semi-Quantitative Analysis

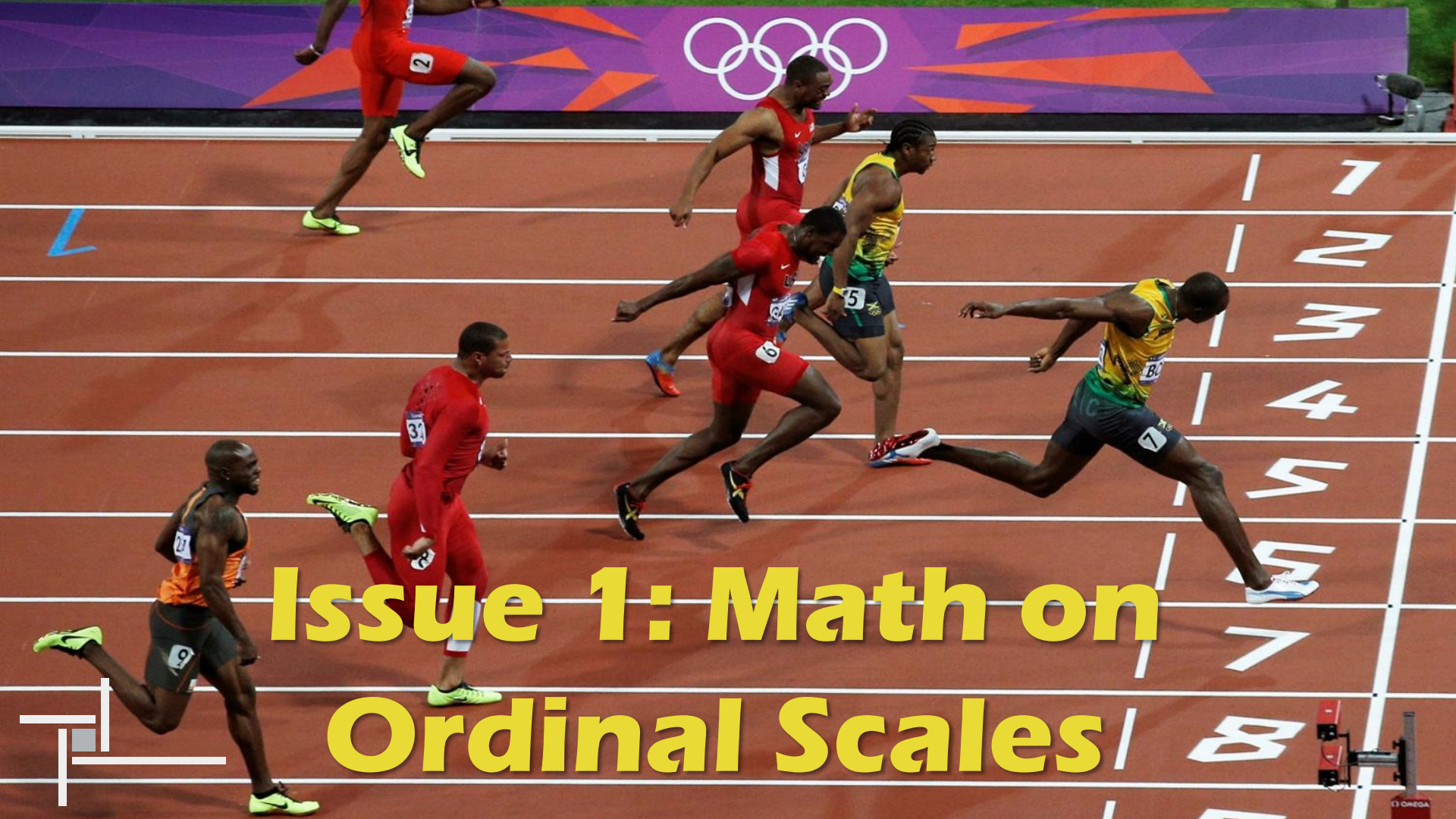
| CIS Control 1.1 - Utilize an Active Discovery Tool | | | | | |
|---|---|---|---|---|---|
| **Asset** | All devices | | **Owner** | IT | |
| **Vulnerability** | Sporadic asset scans | | **Threat** | Undetected compromised systems | |
| **Risk Scenario** | Irregular asset scans may not identify compromised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


FAMILY
TRUCKSTER


How far to Wally World?
FAMILY
TRUCKSTER


How far to Wally World?
Distance rating: 6
FAMILY TRUCKSTER

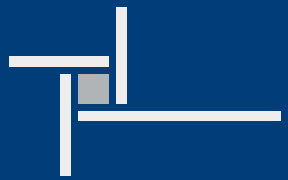

# Common Analysis Issues



# Issue 1: Math on Ordinal Scales

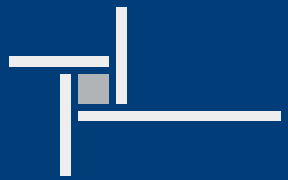
# Measurement Scales

| 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 |

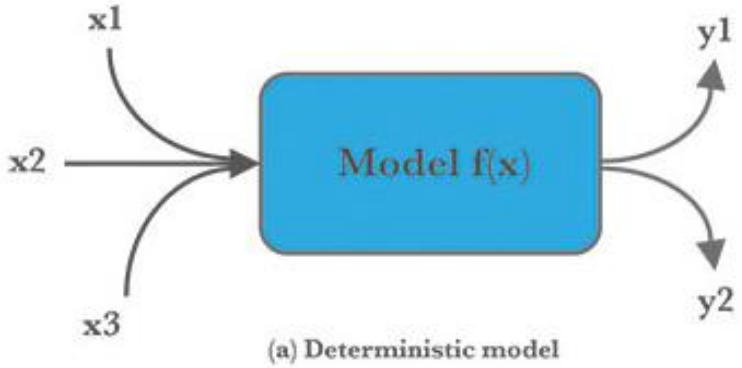


# Issue 2:BAD MODELS

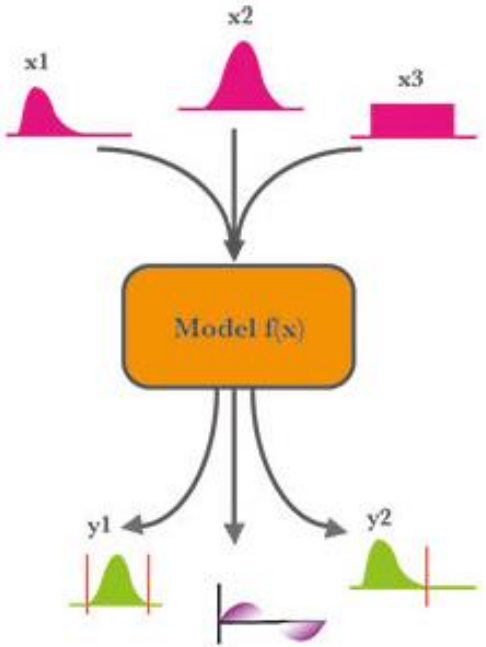
**Essentially, all models are wrong, but some are useful.**

- George E. P. Box

# Issue 2a: Wrong Type of Model

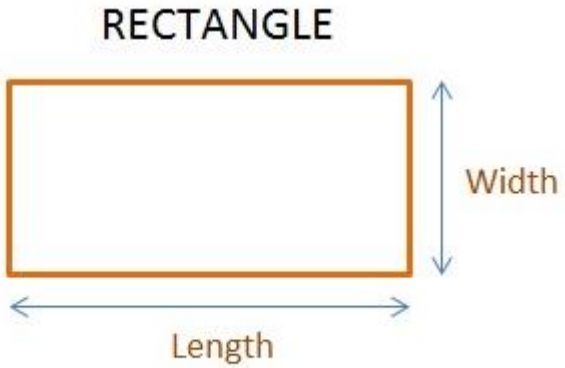



(a) Deterministic model




(b) Stochastic model

## When to Use Deterministic Models



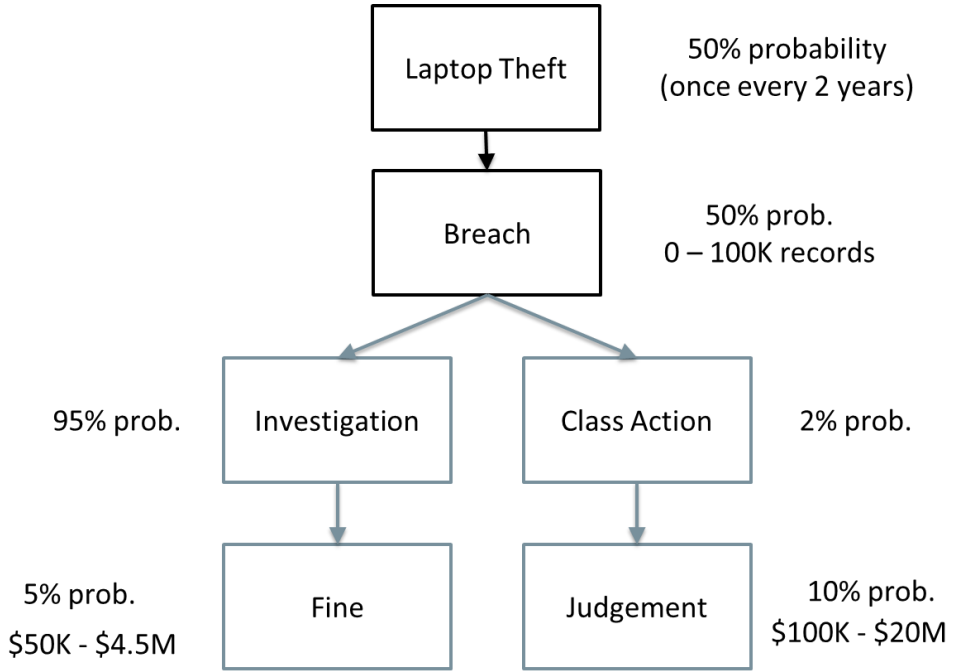

Area of rectangle $= Length\ X\ Width$

## When to Use Stochastic Models

# Issue 2b: Poor Model Design

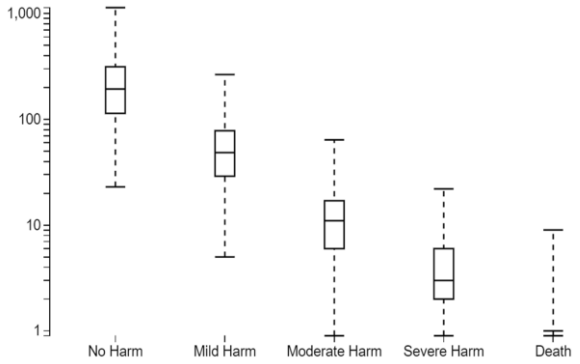
**Risk = threat x vulnerability x consequence**

**vs**

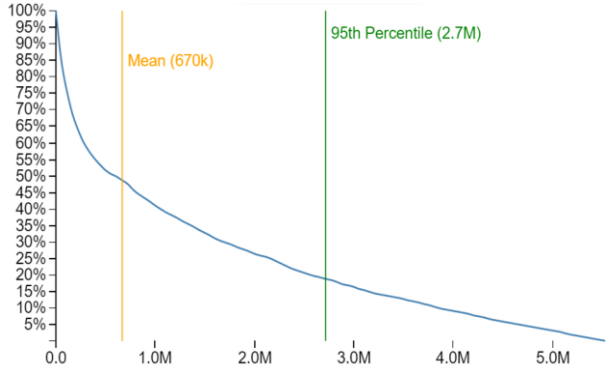


# Issue 3: Don’t Account for Cognitive Biases

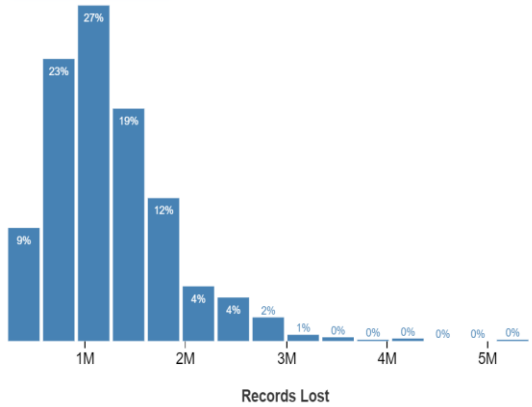
# Method 3: Quantitative Analysis




**Patient Safety Risk**

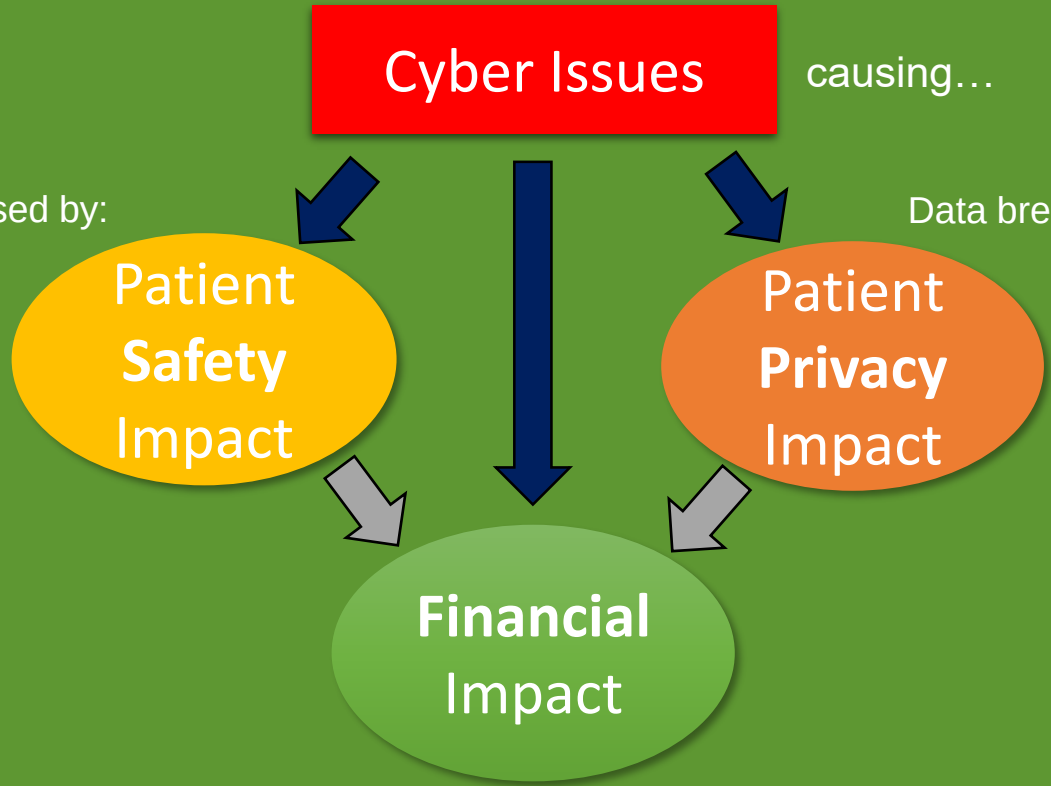



**Financial Risk**




**Risk to PHI**

# Modeling Risk in Healthcare




Unsafe conditions caused by:

- Medical Device Failure
- Mission Critical System Outages

(e.g. Epic, Cerner, McKesson, PIXIS)

Data breaches caused by:

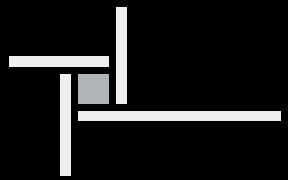
- Hackers & Malware
- Unauthorized Access / Disclosures
- Human Error

Resulting in multiple forms of financial loss including: fines, judgements, revenue.

# Risk associated with cyber criminals gaining access to PHI via external facing applications:

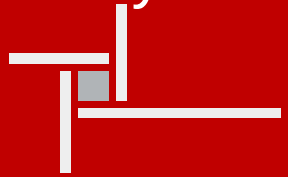
| Risk Category | Avg Annual Expected Loss | 95th Percentile |
|---|---|---|
| Patient Safety Risk | none | none |
| Privacy Risk | 10 records | 5% prob. > 100K records |
| Financial Risk | $10K | 5% prob. > $10M |

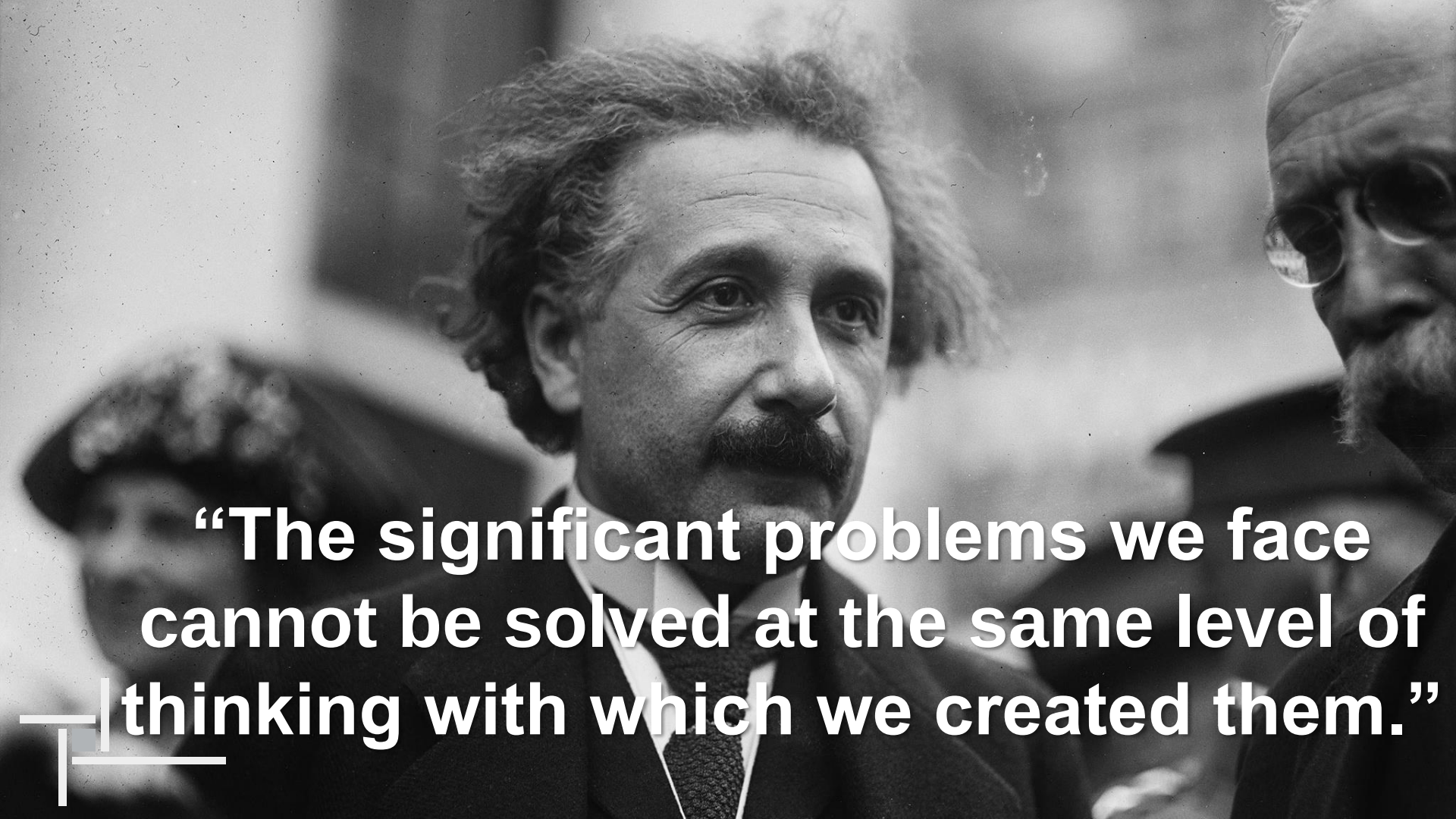
# Why Quantify Risk?

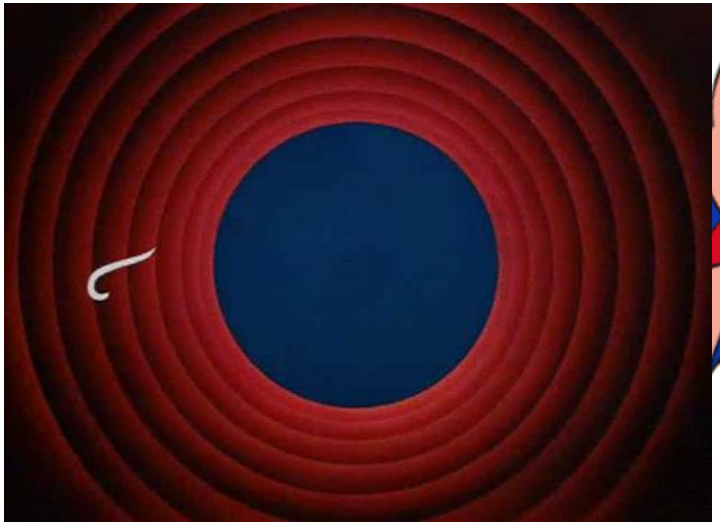


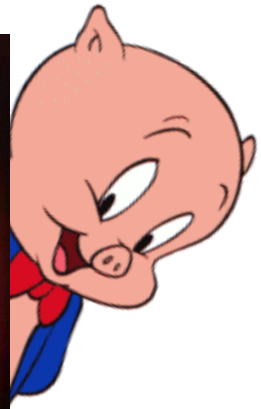
# Summary

- ✓Cyber security is a business issue
- ✓Risk management is process
- ✓Effective risk management requires good decision making
- ✓Decision makers need good information
- ✓Traditional risk analysis produces “questionable” results
- ✓Cyber risk can and should be measured




“The significant problems we face cannot be solved at the same level of thinking with which we created them.”





**Where to find me online…**

linkedin.com/in/apoloniogarcia

@appsgarcia

www.healthguardsecurity.com

Stop by and


register to win!