How to Measure Anything in Cybersecurity Risk

Presented by:

Douglas Hubbard

Hubbard Decision Research

My Co-Author and I

Richard Seiersen

Currently the General Manager of Cybersecurity and Privacy at GE Health Care. Data driven executive with ~20 years experience spanning subject matters in Cyber Security, Quantitative Risk Management, Predictive Analytics, Big Data and Data Science, Enterprise Integrations and Governance Risk and Compliance (GRC). Led large enterprise teams, provided leadership in multinational organizations and tier one venture capital backed start-ups.

Douglas Hubbard

Mr. Hubbard is the inventor of the powerful Applied Information Economics (AIE) method. He is the author of the #1 bestseller in Amazon's math for business category for his book titled ***How to Measure Anything: Finding the Value of Intangibles in Business*** (Wiley, 2007; 3rd edition 2014). His other two books are titled ***The Failure of Risk Management: Why It's Broken and How to Fix It*** (Wiley, 2009) and ***Pulse: The New Science of Harnessing Internet Buzz to Track Threats and Opportunities*** (Wiley, 2011).

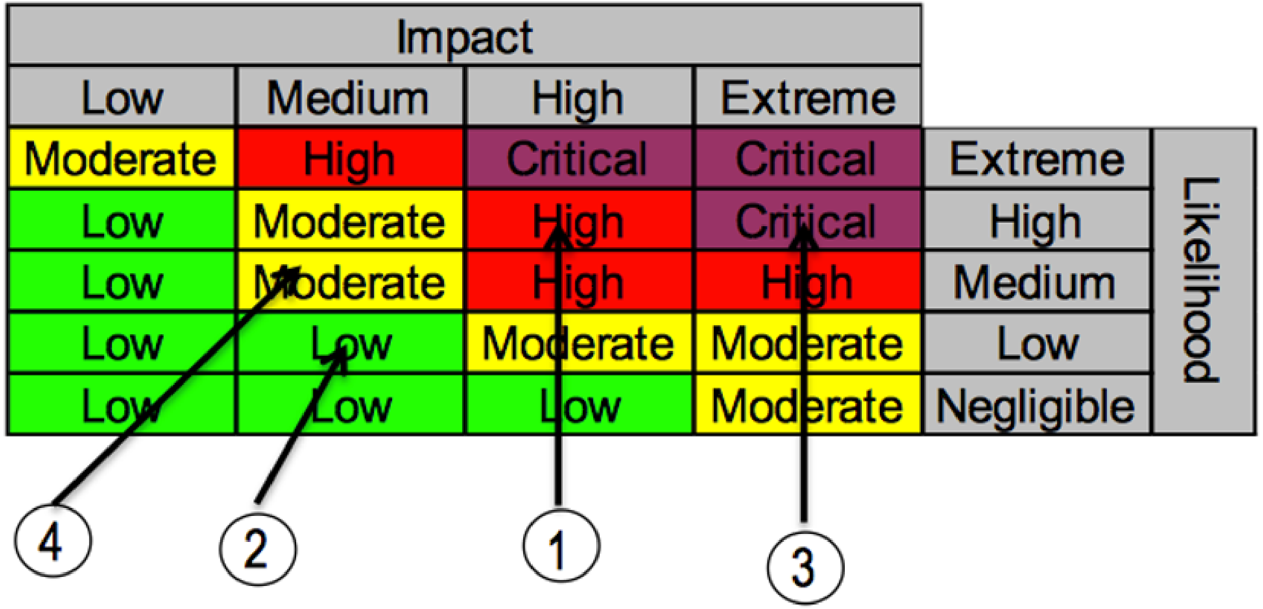
The Biggest Cybersecurity Risk

Question: What is Your Single Biggest Risk in Cybersecurity?

Answer: How You Measure Cybersecurity Risk

Current Solution

- Here are some risks plotted on a "typical heat map".
- Suppose mitigation costs were:
  - Risk 1: $725K – High
  - Risk 2: $95K – Low
  - Risk 3: $2.5M – Critical
  - Risk 5: $375K – Moderate
- What mitigations should be funded and what is the priority among these?



Impact					
Low	Medium	High	Extreme		Likelihood
Moderate	High	Critical	Critical	Extreme	
Low	Moderate	High	Critical	High	
Low	Moderate	High	High	Medium	
Low	Low	Moderate	Moderate	Low	
Low	Low	Low	Moderate	Negligible	

Current Solutions

Most standards and certification tests promote risk analysis as a type of ordinal scoring method

The “Risk Rating Methodology” on OWASP.org states:

- “Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the "**likelihood**". At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. *Generally, identifying whether the likelihood is low, medium, or high is sufficient* .”

Can Analysis or Expertise be a "Placebo"?

"The first principle is that you must not fool yourself, and you are the easiest person to fool." — Richard P. Feynman

- Collecting more than a few data points on horses makes experts worse at estimating outcomes. (Tsai, Klayman, Hastie)
- Interaction with others only improves estimates up to a point, then they get worse. (Heath, Gonzalez)
- Collecting more data about investments makes people worse at investing. Collecting more data about students makes counselors worse at predicting student performance. (Andreassen)
- An experiment with a structured decision analysis method shows confidence increased whether decisions are improved or degraded. (Williams, Dennis, Stam, Aronson)

In short, we should *assume* increased confidence from analysis is a "placebo." Real benefits have to be measured.

What the Research Says

- There is mounting evidence against (and none for) the effectiveness of “risk scores” and “risk matrices.”
- Fundamental misconceptions about statistical inference may keep some from adopting quantitative methods.
- Experts using even naïve statistical models outperform human experts who do not.

Note: Every improvement we are about to has already been adopted in several cybersecurity environments.

Summarizing Research on Ordinal Scales

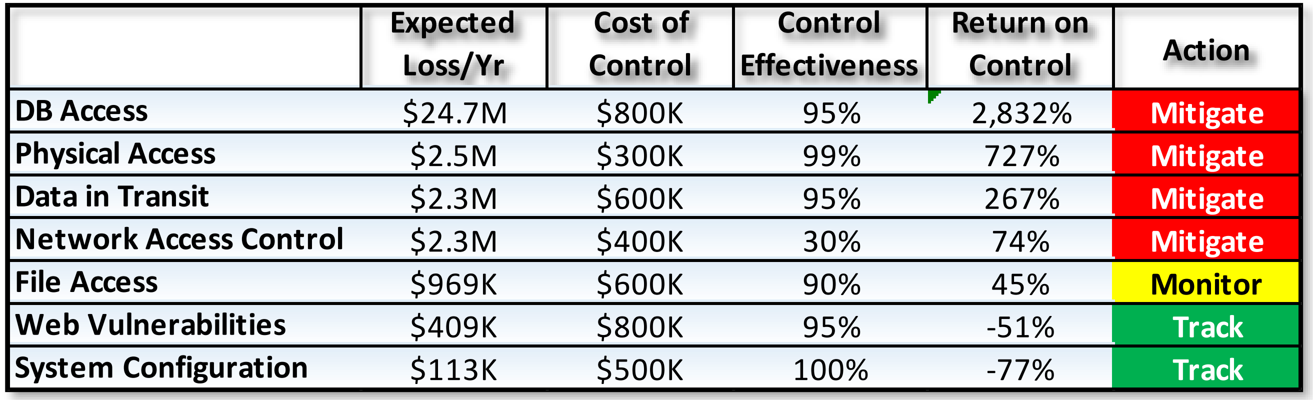
- Bickel et al. “The Risk of Using Risk Matrices”, *Society of Petroleum Engineers, 2014*
- They performed an extensive literature review to-date as well as a statistical analysis of RM used in Petroleum Engineering Risk (which are nearly identical to RM’s in Cyber) – including computing a “Lie Factor” of the degree of distortion of data.

“How can it be argued that a method that distorts the information underlying an engineering decision in nonuniform and uncontrolled ways is an industry best practice? The burden of proof is squarely on the shoulders of those who would recommend the use of such methods to prove that these obvious inconsistencies do not impair decision making, much less improve it, as is often claimed.”

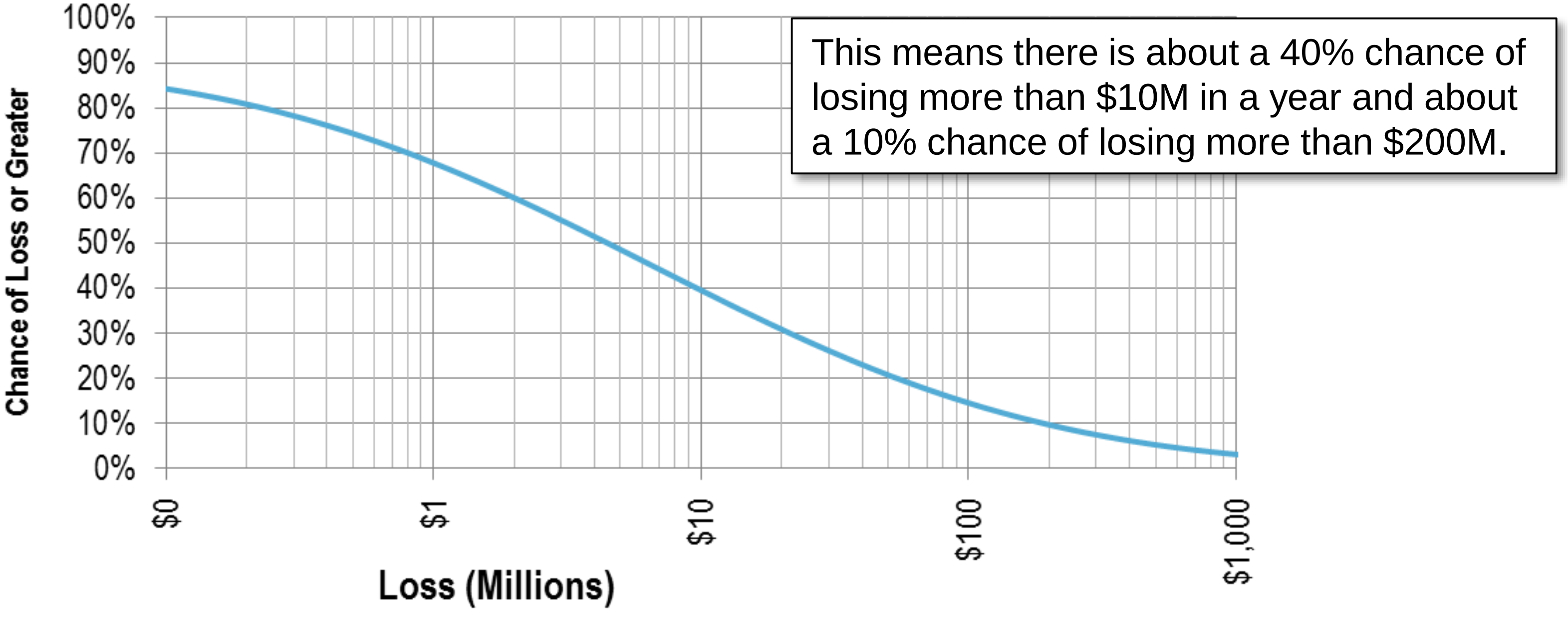
What if We Could *Actually Measure Risk* in Cybersecurity?

What if we could measure risk more like an actuary – "The probability of losing more than $10 million due to security incidents in 2016 is 16%"

What if we could prioritize security investments based on a "Return on Mitigation"?



	Expected Loss/Yr	Cost of Control	Control Effectiveness	Return on Control	Action
DB Access	$24.7M	$800K	95%	2,832%	Mitigate
Physical Access	$2.5M	$300K	99%	727%	Mitigate
Data in Transit	$2.3M	$600K	95%	267%	Mitigate
Network Access Control	$2.3M	$400K	30%	74%	Mitigate
File Access	$969K	$600K	90%	45%	Monitor
Web Vulnerabilities	$409K	$800K	95%	-51%	Track
System Configuration	$113K	$500K	100%	-77%	Track



This means there is about a 40% chance of losing more than $10M in a year and about a 10% chance of losing more than $200M.

© Hubbard Decision Research, 2012

Why Not Better Methods?

- Cybersecurity is too complex or lacks sufficient data for quantitative analysis…

  …yet can be analyzed with unaided expert intuition or soft scales.
- Probabilities can't be used explicitly because _______ ….

  …yet we can *imply* probabilities with ambiguous labels.

Remember, softer methods never <u>*alleviate*</u> a lack of data, complexity, rapidly changing environments or unpredictable human actors…

…they can only <u>*obscure*</u> it.

A Major Fallacy Regarding Comparing Methods

- Don’t make the classic “Beat the Bear” fallacy.

Exsupero Ursus

- If you doubt the effectiveness of quantitative methods, remember, all you have to do is outperform the alternative:

- …unaided expertise or soft scoring methods.

Your Intuition About Sample Information is Wrong

SECURE360

- Cybersecurity experts are not immune to widely held misconceptions about probabilities and statistics – especially if they vaguely remember some college stats.
- These misconceptions lead many experts to believe they lack data for assessing uncertainties or they need some ideal amount before anything can be inferred.

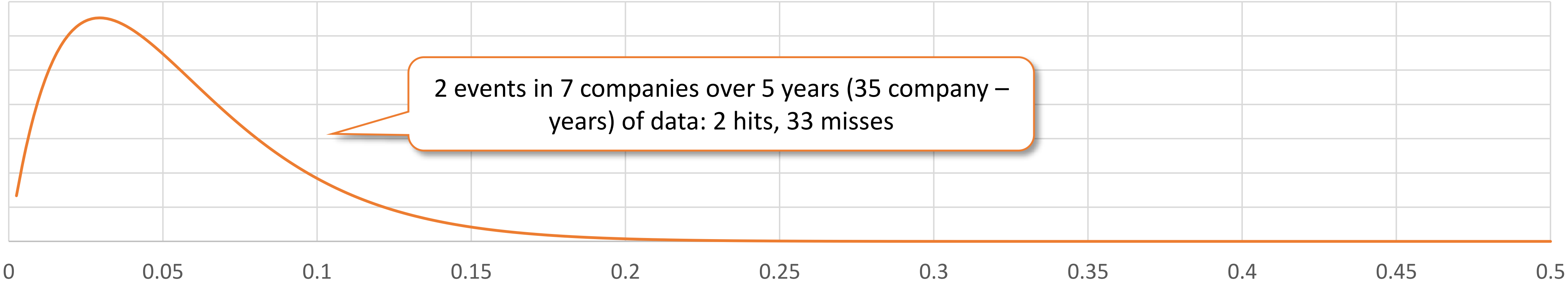
"Our thesis is that people have strong intuitions about random sampling…these intuitions are wrong in fundamental respects...[and] are shared by naive subjects and by trained scientists"

Amos Tversky and Daniel Kahneman,
Psychological Bulletin, 1971

Hubbard Decision Research

You Need Less Data Than You Think

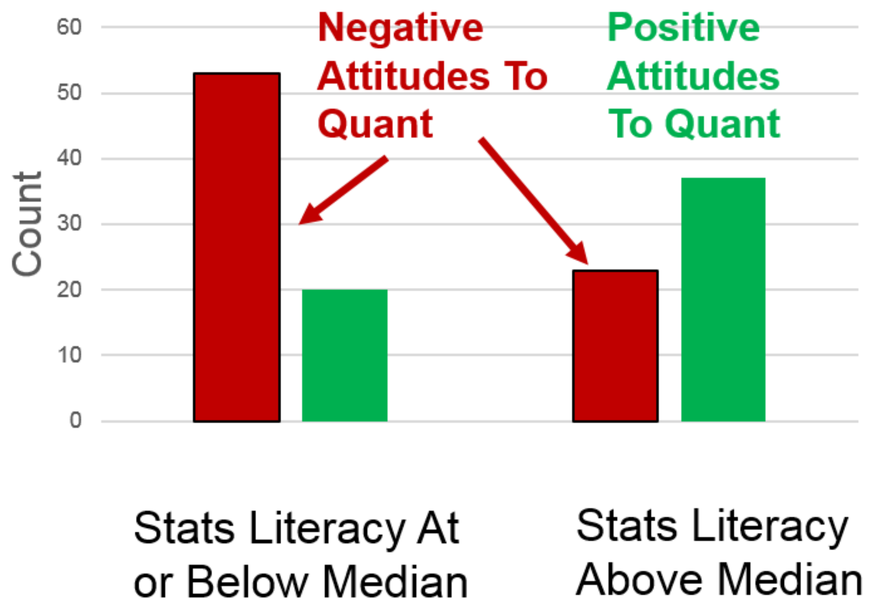
- A beta distribution computes the probability of a frequency being below a given amount (e.g. chance that rate of occurrence is <2/100)
- In Excel it can be written as "=Betadist(frequency,alpha,beta)"
- A uniform prior can be made with alpha=1 and beta=1. This can be used as a starting point for maximum uncertainty.
- "Hits" and "Misses" can be simply added to the priors (=Betadist(frequency,hits+1,misses+1))



2 events in 7 companies over 5 years (35 company – years) of data: 2 hits, 33 misses

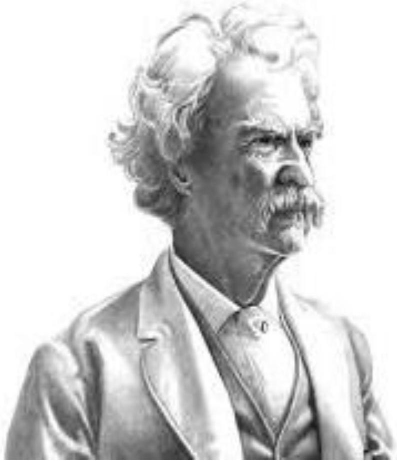
Survey Results: The "Stats Concepts" Quiz

- We conducted a survey of 171 Cybersecurity professionals
- One Finding: Strong opinions against "quant" are associated with poor stats understanding.



"It's not what you don't know that will hurt you, it's what you know that ain't so."

Mark Twain



Historical Models – Still Better Than Experts

When experts assess probabilities, many events “. . .are perceived as so unique that past history does not seem relevant to the evaluation of their likelihood.” Tversky, Kahneman, *Cognitive Psychology* (1973)

Yet, Historical models routinely outperform experts in a variety of fields (even considering “Black Swans”)

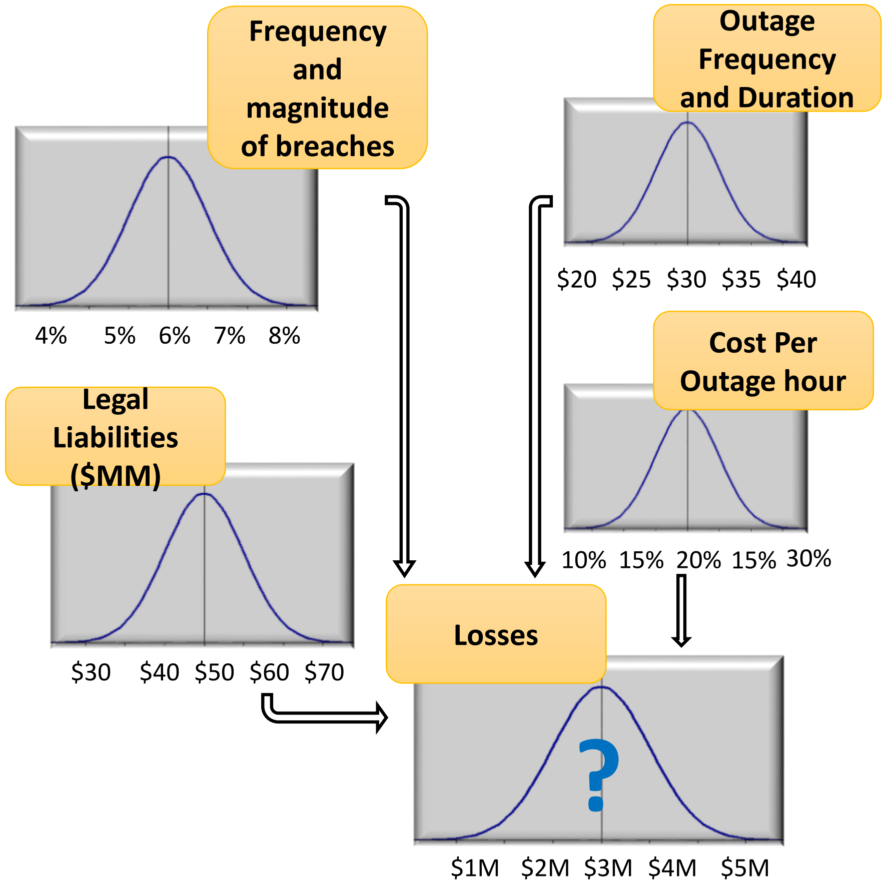
Paul Meehl assessed 150 studies comparing experts to statistical models in many fields (sports, prognosis of liver disease, etc.).

“There is no controversy in social science which shows such a large body of qualitatively diverse studies coming out so uniformly in the same direction as this one.”

Philip Tetlock tracked a total of over 82,000 forecasts from 284 political experts in a 20 year study covering elections, policy effects, wars, the economy and more.

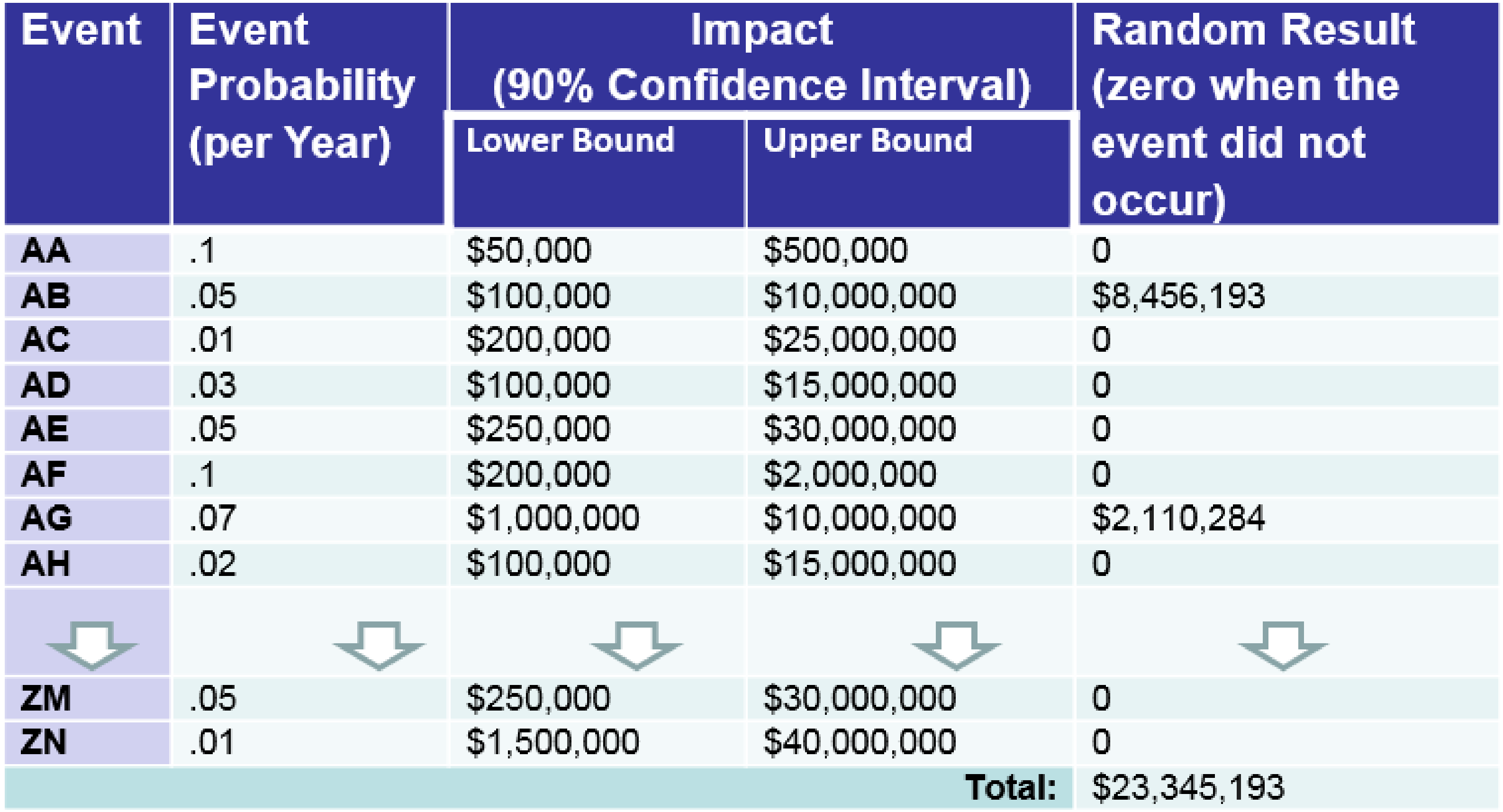
“It is impossible to find any domain in which humans clearly outperformed crude extrapolation algorithms, less still sophisticated statistical ones.”

Monte Carlo: How to Model Uncertainty in Decisions



- Simple decomposition greatly reduces estimation error for estimating the most uncertain variables (MacGregor, Armstrong, 1994)
- As Kahneman, Tversky and others have shown, we have a hard time doing probability math in our heads
- In the oil industry there is a correlation between the use of quantitative risk analysis methods and financial performance – and the improvement started after using the quantitative methods. (F. Macmillan, 2000)
- Data at NASA from over 100 space missions showed that Monte Carlo simulations beat other methods for estimating cost, schedule and risks (I published this in *The Failure of Risk Management* and *OR/MS Today*).

A Simple “One-For-One Substitution”



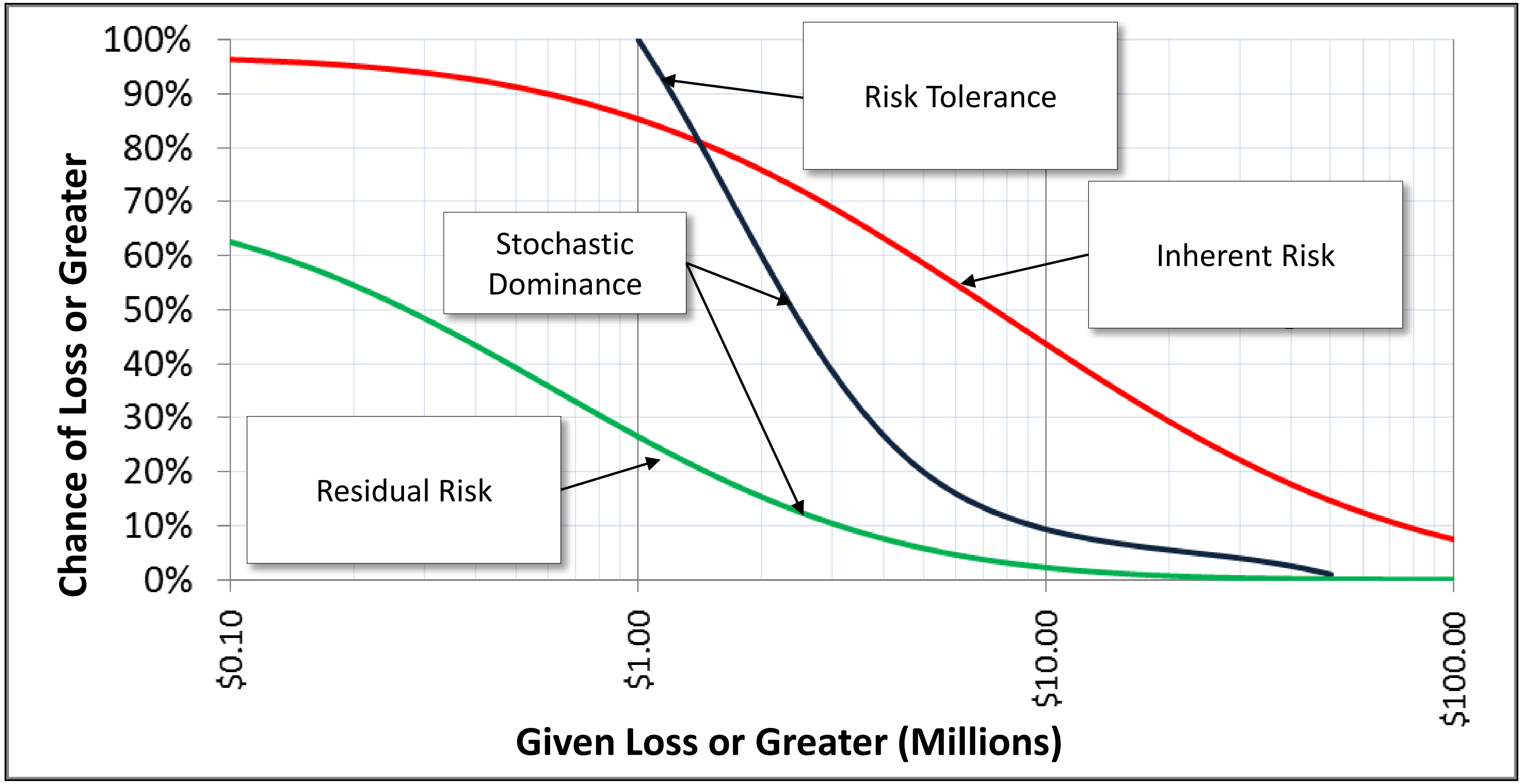
Event	Event Probability (per Year)	Impact (90% Confidence Interval)		Random Result (zero when the event did not occur)
		Lower Bound	Upper Bound	
AA	.1	$50,000	$500,000	0
AB	.05	$100,000	$10,000,000	$8,456,193
AC	.01	$200,000	$25,000,000	0
AD	.03	$100,000	$15,000,000	0
AE	.05	$250,000	$30,000,000	0
AF	.1	$200,000	$2,000,000	0
AG	.07	$1,000,000	$10,000,000	$2,110,284
AH	.02	$100,000	$15,000,000	0
⇩	⇩	⇩	⇩	⇩
ZM	.05	$250,000	$30,000,000	0
ZN	.01	$1,500,000	$40,000,000	0
			Total:	$23,345,193

Each “Dot” on a risk matrix can be better represented as a row on a table like this

The output can then be represented as a Loss Exceedance Curve.

Loss Exceedance Curves: Before and After

- How do we show the risk exposure after applying available mitigations?



SECURE360

Overconfidence

- “Overconfident professionals sincerely believe they have expertise, act as experts and look like experts. You will have to struggle to remind yourself that they may be in the grip of an illusion.”
  - Daniel Kahneman, Psychologist, Economics Nobel

- Decades of studies show that most managers are statistically “overconfident” when assessing their own uncertainty.
- Studies also show that measuring *your own* uncertainty about a quantity is a general skill that <u>can be taught</u> with a ***measurable*** improvement
- Training can “calibrate” people so that of all the times they say they are 90% confident, they will be right 90% of the time.

Hubbard Decision Research

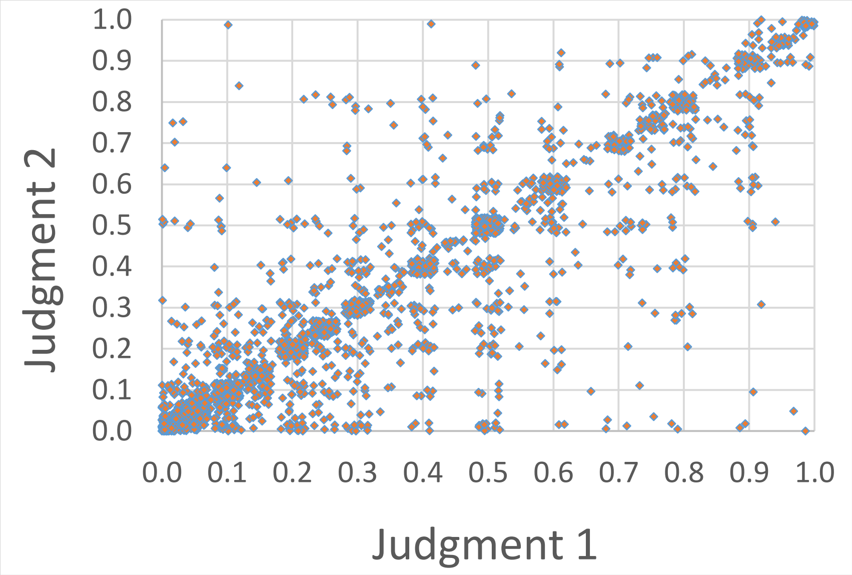
Inconsistency vs. Discrimination

- *Discrimination* is how much your estimates vary when given different information.
- *Inconsistency* is the amount of your discrimination that is due to random differences in estimates - this may be in addition to differences in interpreting verbal scales, so let’s assume we are using explicit probabilities.
- Experts are routinely influenced by irrelevant, external factors - *anchoring*, for example, is the tendency for an estimator to be influenced by recent exposure to an another unrelated number (Kahneman).

Inconsistency Measurement Results

- We have gathered estimates of probabilities of various security events from:
  - 48 experts from 4 different industries.
  - Each expert was given descriptive data for over 100 systems.
  - For each system each expert estimated probabilities of six or more different types of security events.
- Total: Over 30,000 individual estimates of probabilities
- These estimates included over 2,000 duplicate scenarios pairs.

Comparison of 1st to 2nd Estimates of Cyber risk judgements by same SME

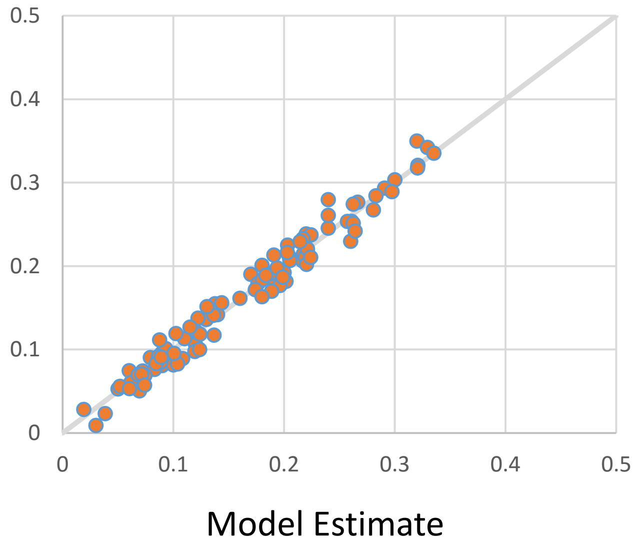


21% of variation in expert responses are explained by *inconsistency.*

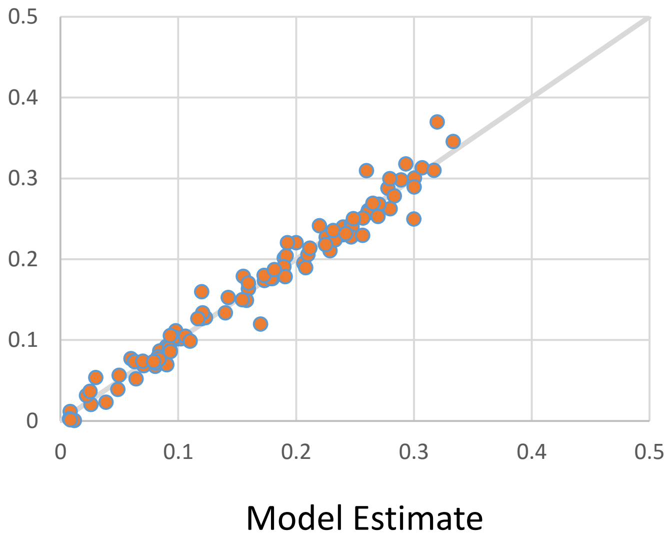
(79% are explained by the actual information they were given)

Modeling Group Estimates of IT Security Event Likelihood

- Examples of Models vs. Group Averages: Probabilities of different security events happening in the next 12 months for various systems prior to applying particular controls.



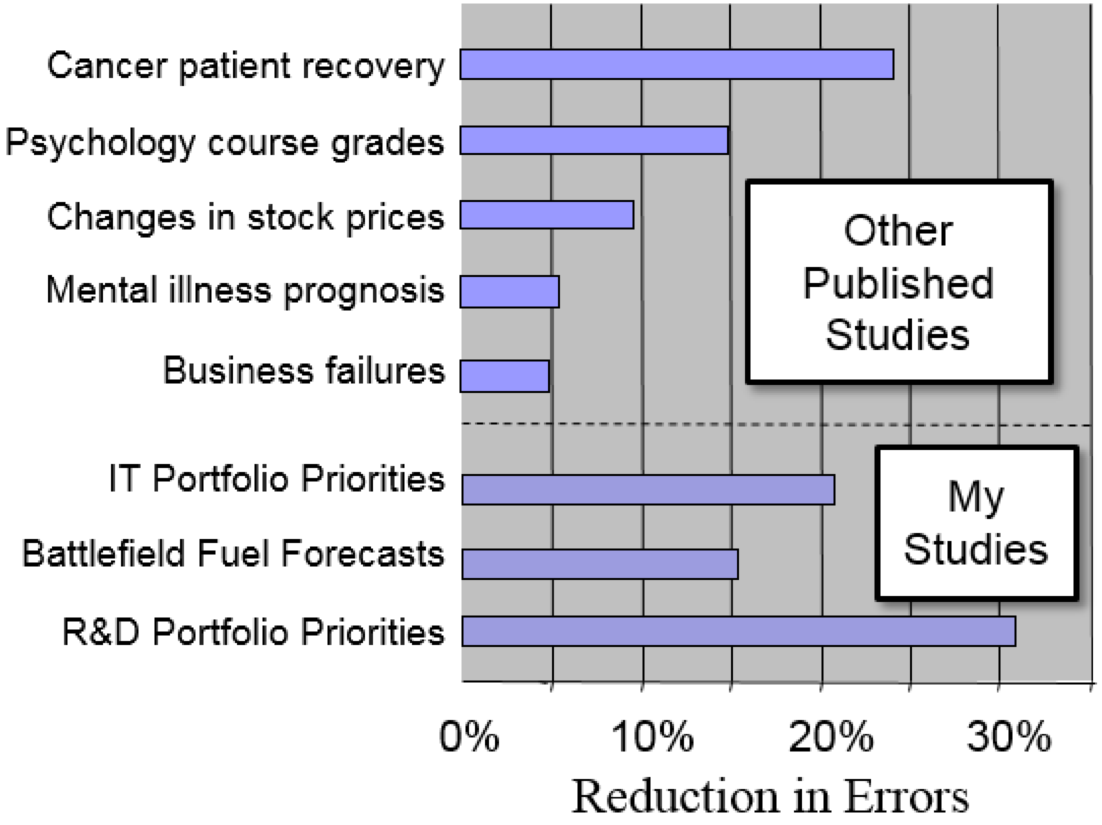
Confidentiality Breach Resulting In Fines



Internal Unauthorized Access Resulting In Productivity Loss

- The models created produce results which closely match the group’s average.
- A large portion of the model error is due to judge inconsistency.
- This nearly eliminates the inconsistency error.

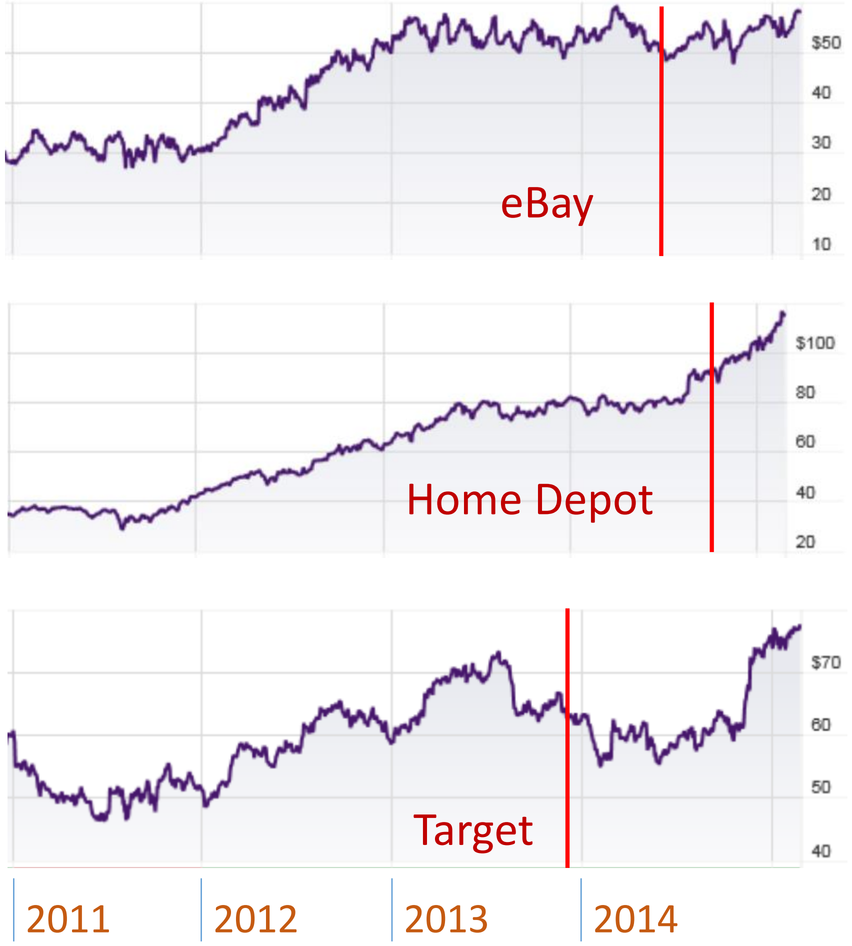
Effects of Removing Inconsistency Alone



- A method of improving expert estimates of various quantities was developed in the 1950's by Egon Brunswik.
- He called it the "Lens Method"
- It has been applied to several types of problems, including expert systems, with consistently beneficial results.

Measurement Challenge: Reputation Damage

- One of the perceived most difficult measurements in cybersecurity is damage to reputation.
- Trick: *There is no such thing as a "secret" damage to reputation!*
- How about comparing stock prices after incidents? (That's all public!)
- So what is the *REAL* damage?
  - Legal liabilities,
  - Customer outreach
  - "Penance" projects (security overkill)
- The upshot, damage to reputation actually has available information and easily observable measured costs incurred to *avoid* the bigger damages!



© Hubbard Decision Research, 2012

Supporting Decisions

- If risks and mitigation strategies were quantified in a meaningful way, decisions could be supported.
- In order to compute an ROI on mitigation decisions, we need to quantify likelihood, monetary impact, cost, and effectiveness

Risk	Likelihood / Yr	Impact / Yr	Mitigation Effectiveness	Mitigation Cost / Yr	Mitigation ROI	Action
Risk 1	37%	$2M to $40M	95%	$725K	725%	Mitigate
Risk 2	11%	$50K to $400K	100%	$95K	-80%	Track
Risk 3	34%	$5M to $80M	90%	$2.5M	329%	Monitor
Risk 4	29%	$500K to $20M	98%	$375K	437%	Mitigate

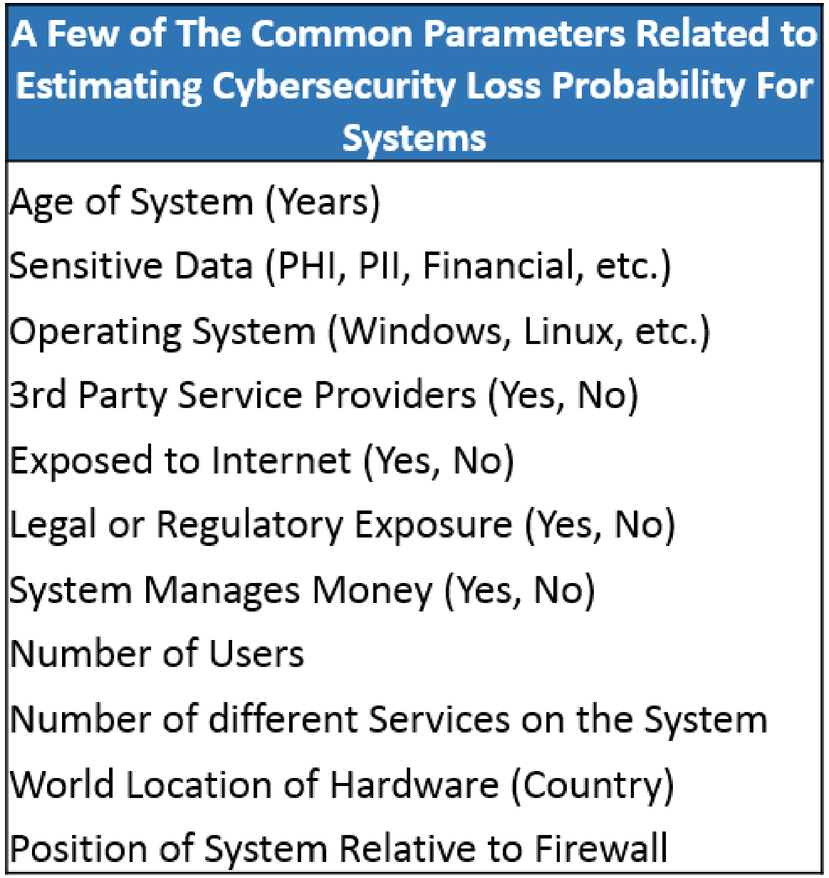
- The optimal solution would be to mitigate Risks1 & 4 first.
- If you have the resources, then mitigate Risk 3.
- Risk 2 is not worth fixing.

Call to Action for Cybersecurity

- Organizations should stop using risk scores and risk matrixes and standards organizations should stop promoting them
- Adopt simple probabilistic methods now: They demonstrate a measurable improvement over unaided intuition and they have already been used. So there is no reason not to adopt them.
- Build on simple methods when you are ready – always based on what shows a measurable improvement.

Supplementary Material

Parameters Cybersecurity Models



A Few of The Common Parameters Related to Estimating Cybersecurity Loss Probability For Systems
Age of System (Years)
Sensitive Data (PHI, PII, Financial, etc.)
Operating System (Windows, Linux, etc.)
3rd Party Service Providers (Yes, No)
Exposed to Internet (Yes, No)
Legal or Regulatory Exposure (Yes, No)
System Manages Money (Yes, No)
Number of Users
Number of different Services on the System
World Location of Hardware (Country)
Position of System Relative to Firewall

- Experts are given values on a variety of parameters as a basis for their estimates.
- For each scenario they may be asked to estimate a probability of a breach, outage, legal liability, etc.
- Some companies estimated risks of incidence for particular systems, others estimated threats or additional detail for types of losses, but there were some common themes (see table).

“Opinion Toward Quantitative Methods” (18 Questions)

18 questions on opinions of the use of quantitative methods in cybersecurity were asked. Here are some examples:

(Responses: Agree, Disagree, No Opinion/Don’t Know)

Information security is too complex to model with probabilistic methods.
Management and users won't understand the quantitative methods’ output.
An expert using quantitative probabilistic methods will do better risk assessments then an expert using intuition alone.

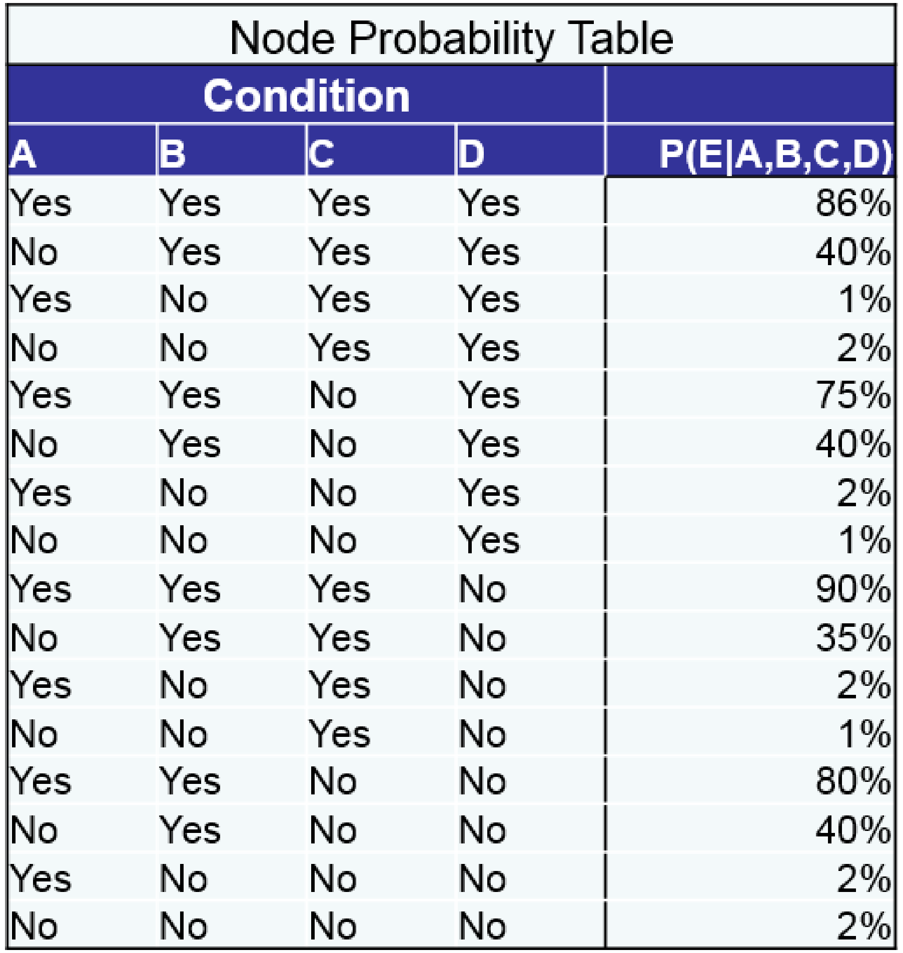
RESULTS: 80% of respondents had more “pro” than “anti” quantitative responses. Only 22% were consistently “pro” on quantitative and “anti” on softer scoring methods.

The Stats Concepts Quiz (10 Questions)

EXAMPLE: Assume that you have a portfolio of systems for which you have observed no security events in the past year that resulted in a monetary or productivity loss, which of the following statements is true?

	Answer Options	Response Percent
✗	If no events were observed, then we have no data about the likelihood of these events.	2.2%
✓ !	The fact that no events were observed tells us something about the likelihood of these events.	37.0%
✗	One year is not long enough time to gather enough observations to make an inference.	4.4%
✗	Since some events may not have been observed, the lack of observed losses tells us nothing.	31.9%
✗	There is insufficient information to answer the question.	17.8%
	I don't know	6.7%

Bayesian Methods: Node Probability Tables



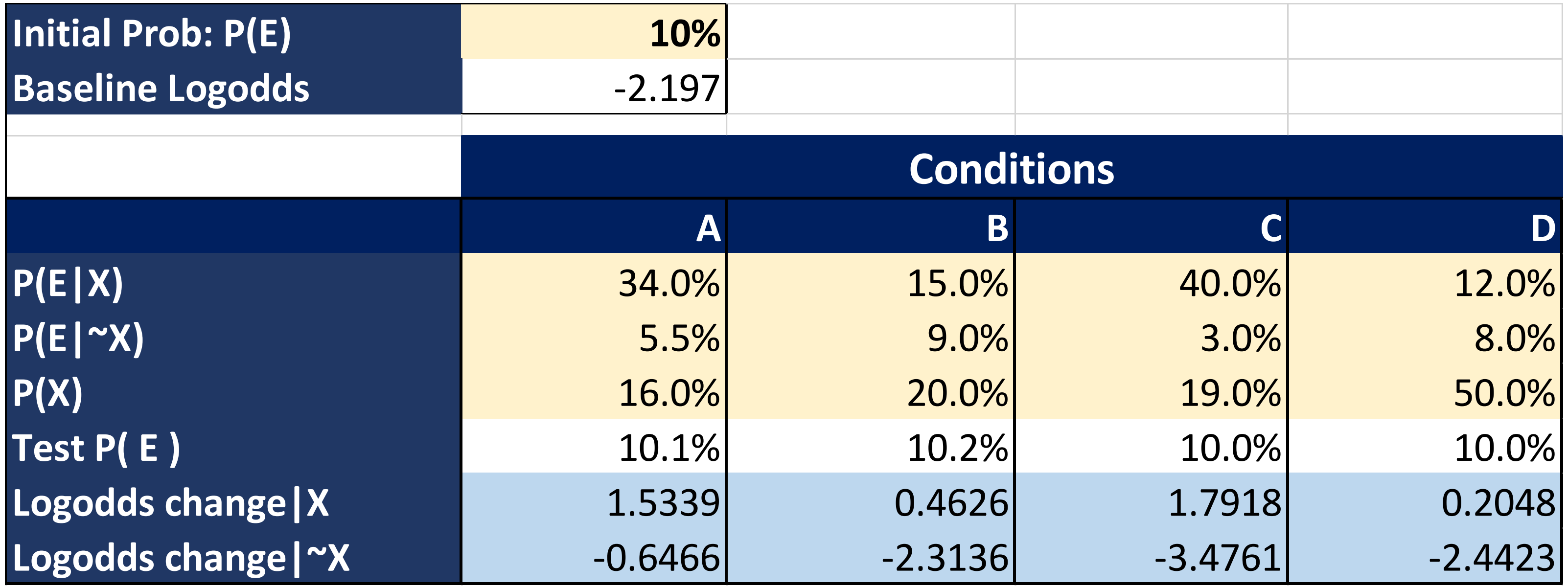
Node Probability Table

Condition				
A	B	C	D	P(E|A,B,C,D)
Yes	Yes	Yes	Yes	86%
No	Yes	Yes	Yes	40%
Yes	No	Yes	Yes	1%
No	No	Yes	Yes	2%
Yes	Yes	No	Yes	75%
No	Yes	No	Yes	40%
Yes	No	No	Yes	2%
No	No	No	Yes	1%
Yes	Yes	Yes	No	90%
No	Yes	Yes	No	35%
Yes	No	Yes	No	2%
No	No	Yes	No	1%
Yes	Yes	No	No	80%
No	Yes	No	No	40%
Yes	No	No	No	2%
No	No	No	No	2%

- Conditional probabilities with combinations of conditions are recorded with an NPT
- With more than a few conditions and conditions that are more than binary, it will become unwieldly
- (Recent models we created would have had thousands of rows)

Rasch (Logodds) Model

- A Rasch Model is a relatively simple approximation to “add up” a number of parameters that modify a probability when NPTs would be large.
- Logodds of X=LO(X)=ln(P(X)/(1-P(X))
- Adjustment due to condition Y=A(Y) =LO(P(X|Y))– LO(P(X))
- P(X|A,B,..)=A(Sum of (LO(A),LO(B),…)+LO(P(X)))
- The more independent the parameter are, the better the Rasch approximation.

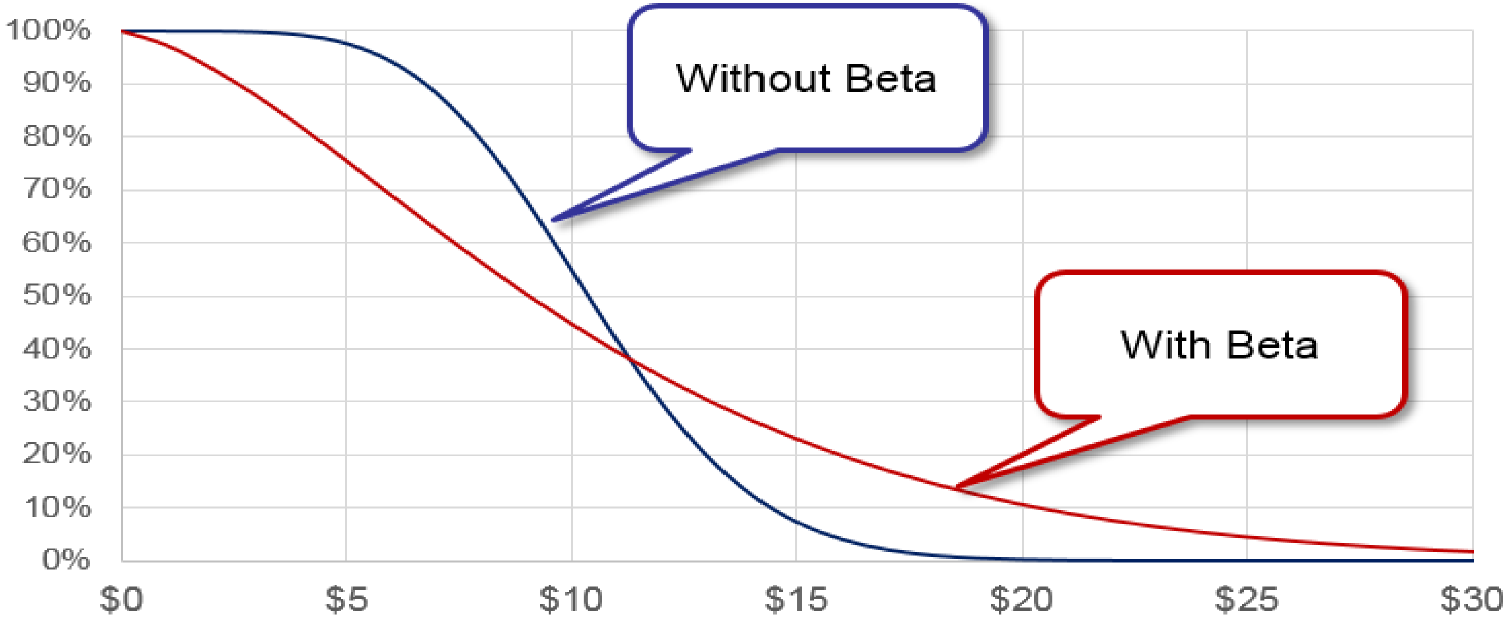


Initial Prob: P(E)	**10%**
Baseline Logodds	-2.197

	Conditions			
	A	**B**	**C**	**D**
P(E|X)	34.0%	15.0%	40.0%	12.0%
P(E|~X)	5.5%	9.0%	3.0%	8.0%
P(X)	16.0%	20.0%	19.0%	50.0%
Test P(E)	10.1%	10.2%	10.0%	10.0%
Logodds change|X	1.5339	0.4626	1.7918	0.2048
Logodds change|~X	-0.6466	-2.3136	-3.4761	-2.4423

Beta Distribution and the LEC

- Consider a portfolio of systems, each with chance of monetary loss event and a range of loss amount if it occurs.
- If we consider the possibility of systemic under/overestimation of P(Event), the LEC is rotated so that expected loss is constant but extreme loss.es are more likely



Effects of Ordinal Scales and Matrices of Ordinal Scales

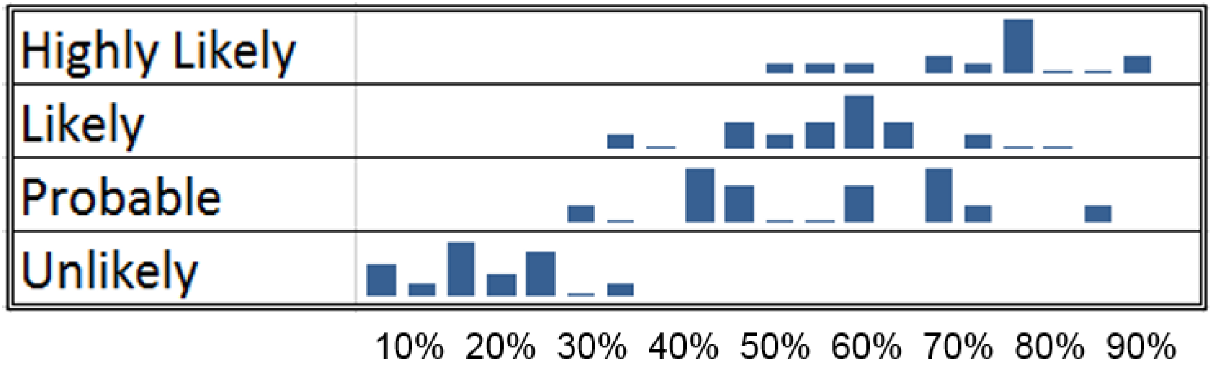
- Bob Clemen and Craig Fox paper on ordinal scales for general decision analysis, Management Science, 2004
  - "Analysts typically assume that the particular choice of intervals does not unduly influence assessed probabilities. Unfortunately, our experimental results demonstrate that this assumption is unfounded: assessed probabilities can vary substantially with the particular partition that the analyst chooses."
- Tony Cox "What's wrong with Risk Matrices" investigates various mathematical consequences of ordinal scales on a matrix.
  - "Risk matrices can mistakenly assign higher qualitative ratings to quantitatively smaller risks. For risks with negatively correlated frequencies and severities, they can be "worse than useless," leading to worse-than-random decisions."

The “Illusion of Communication”

- Budescu et. al. *Psychological Science,* 2009 on the use of verbal, qualitative scales for likelihoods:

  “[Verbal terms] induce an illusion of communication People assume that everyone interprets the terms consistently and similarly, and fail to appreciate the variance in the interpretations of these words. The high level of potential miscommunication has been widely documented in many contexts.”

  - Richards Heuer, *The Psychology of Intelligence Analysis,* Center for the Study of Intelligence, CIA, 1999



23 NATO officers estimates of probabilities for events described using common terms used in communicating likelihoods in intelligence reports (e.g. “War between X and Y is…”

The State of Cybersecurity

James B. Comey, Director FBI, made the following statement before the Senate Committee on Homeland Security and Government Affairs on Nov 14, 2013:

“The diverse threats we face are increasingly cyber-based. Much of America’s most sensitive data is stored on computers. We are losing data, money, and ideas through cyber intrusions. This threatens innovation and, as citizens, we are also increasingly vulnerable to losing our personal information. ***That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.***

Methods of Measurement

- Most real-world scientific measurements are based on random samples of some kind.
- There are a variety of methods for many situations but they all come down to one simple idea: What is being measured has some effect on the likelihood of a particular observation.
- This means that you don’t have to:
  - Count everything
  - Eliminate or even *know* all sources of error
- “Exception anxiety” is where you think of a possible source of error and assume this means the measurement tells you nothing. This is itself a hypothesis that requires evidence. It assumes a measured quantity of error smothers the “signal.”

Practical Assumptions

- Its been measured before
- You have more data than you think
- You need less data than you think

“It’s amazing what you can see when you look”
Yogi Berra

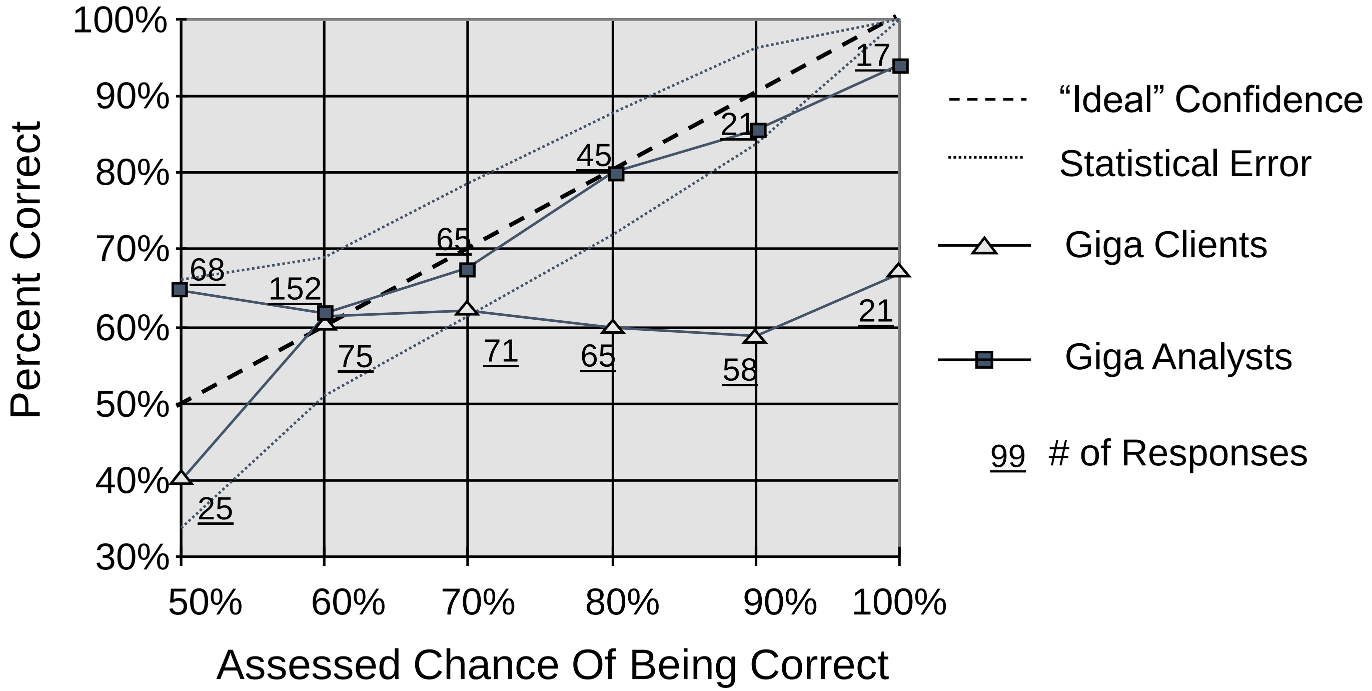
Common Misconceptions Corrected by Bayes

- “A positive result on a test can tell us something but a negative result tells us nothing”
- “If nothing occurred, I have no data about the rate of occurrence” OR “Absence of evidence is not evidence of absence”
- “A few data points tell us nothing” OR “We need more data to be statistically significant”

For each of 10 systems, you estimate an 8% chance per year of a loss due to integrity breaches. The following year you observe no breaches in any of the 10 systems. Is this sufficient data to change the chance of this loss?

Calibrated Probabilities: A 1997 Experiment

- In January 1997, I conducted a calibration training experiment with 16 IT Industry Analysts and 16 CIO's to test if calibrated people were better at putting odds on uncertain future events.
- The analysts were calibrated and all 32 subjects were asked To Predict 20 IT Industry events
- Example: Steve Jobs will be CEO of Apple again, by Aug 8, 1997 - True or False? Are you 50%, 60%...90%, 100% confident?

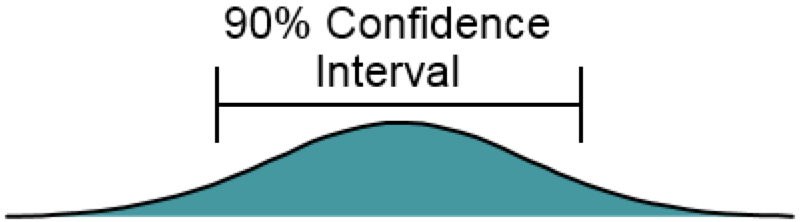


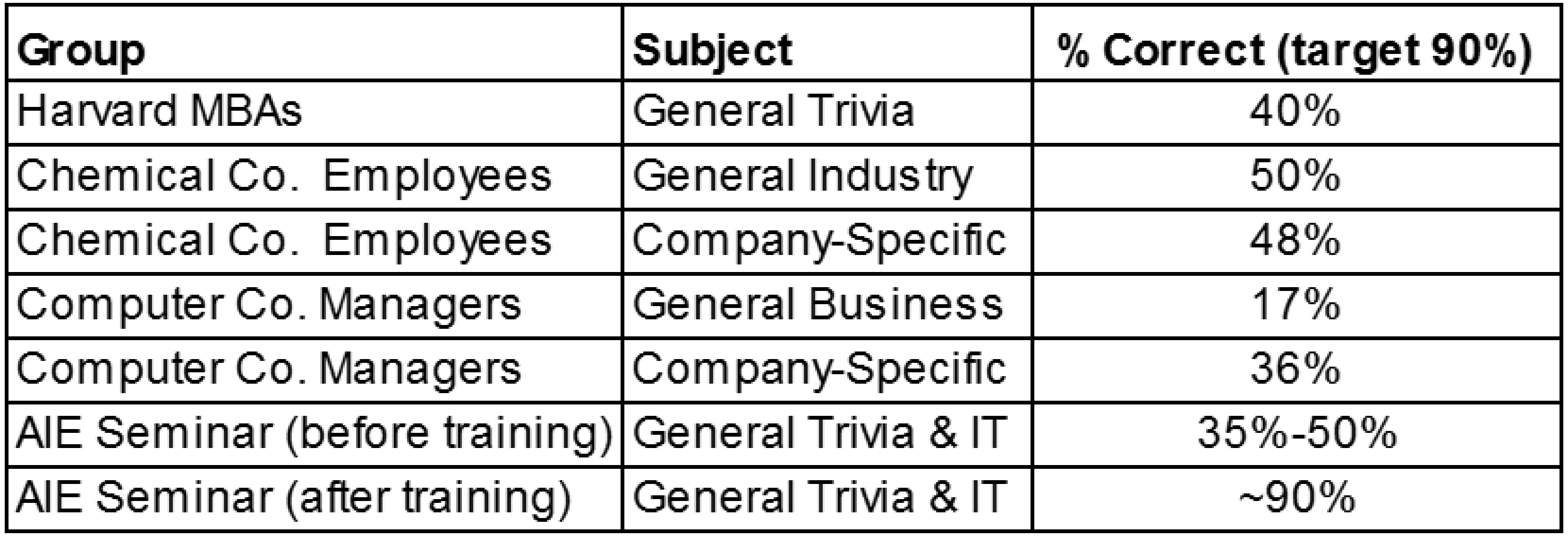
Source: Hubbard Decision Research

© Hubbard Decision Research, 2012

Overconfidence in Ranges

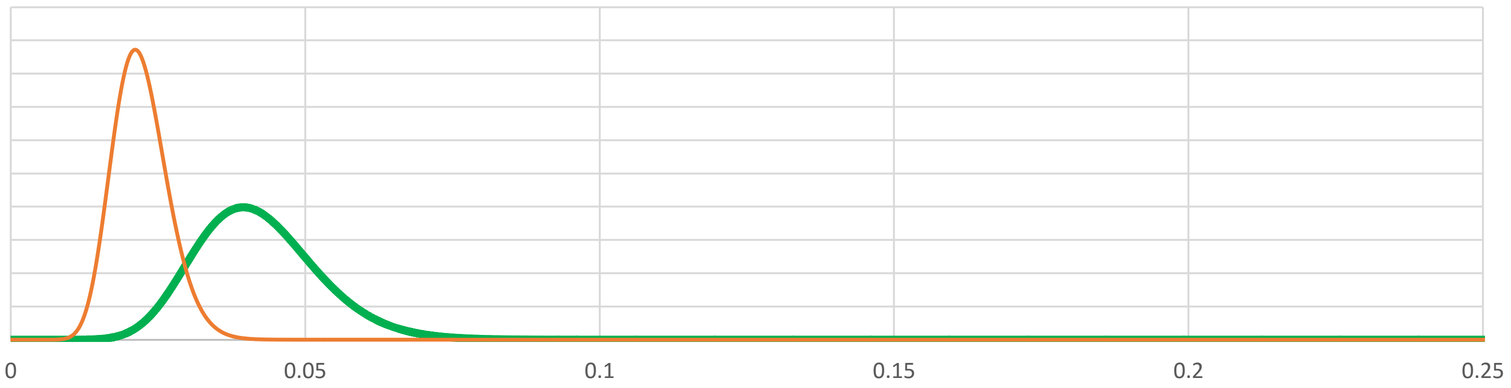
- The same training methods apply to the assessment of uncertain ranges for quantities like the duration of a future outage, the records compromised in a future breach, etc.

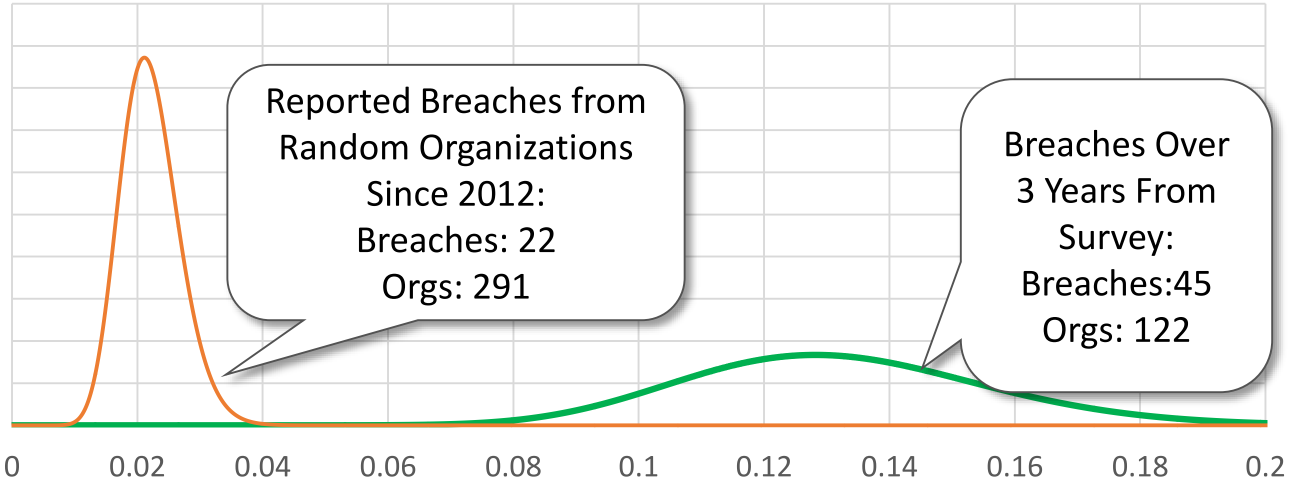




Group	Subject	% Correct (target 90%)
Harvard MBAs	General Trivia	40%
Chemical Co. Employees	General Industry	50%
Chemical Co. Employees	Company-Specific	48%
Computer Co. Managers	General Business	17%
Computer Co. Managers	Company-Specific	36%
AIE Seminar (before training)	General Trivia & IT	35%-50%
AIE Seminar (after training)	General Trivia & IT	~90%

Don’t Do The Math In Your Head: Breach Probability





Reported Breaches from Random Organizations Since 2012:
Breaches: 22
Orgs: 291

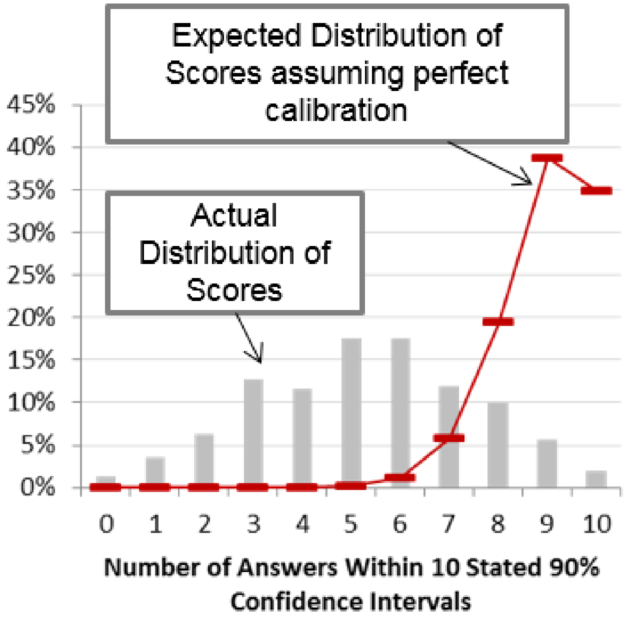
Breaches Over 3 Years From Survey:
Breaches:45
Orgs: 122

- What’s the REAL Breach frequency?
- In the survey we asked respondents whether they had a breach in the last three years.
- If they had a breach, we also asked whether they reported the breach or not.

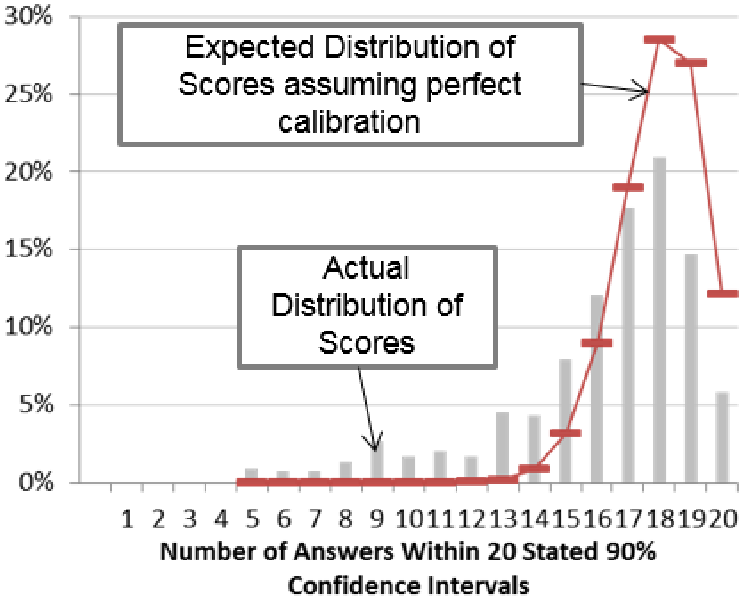
More Data on the Effects of Calibration Training

- With nearly 1,000 subjects who have taken the same calibration tests, and over 100,000 individual responses, HDR has more calibration data than all academic literature combined.
- A clear pattern emerges: Training has a major impact; 15% don’t quite reach calibration

Initial 10 Question 90% CI Test



Final 20 Question 90% CI Test



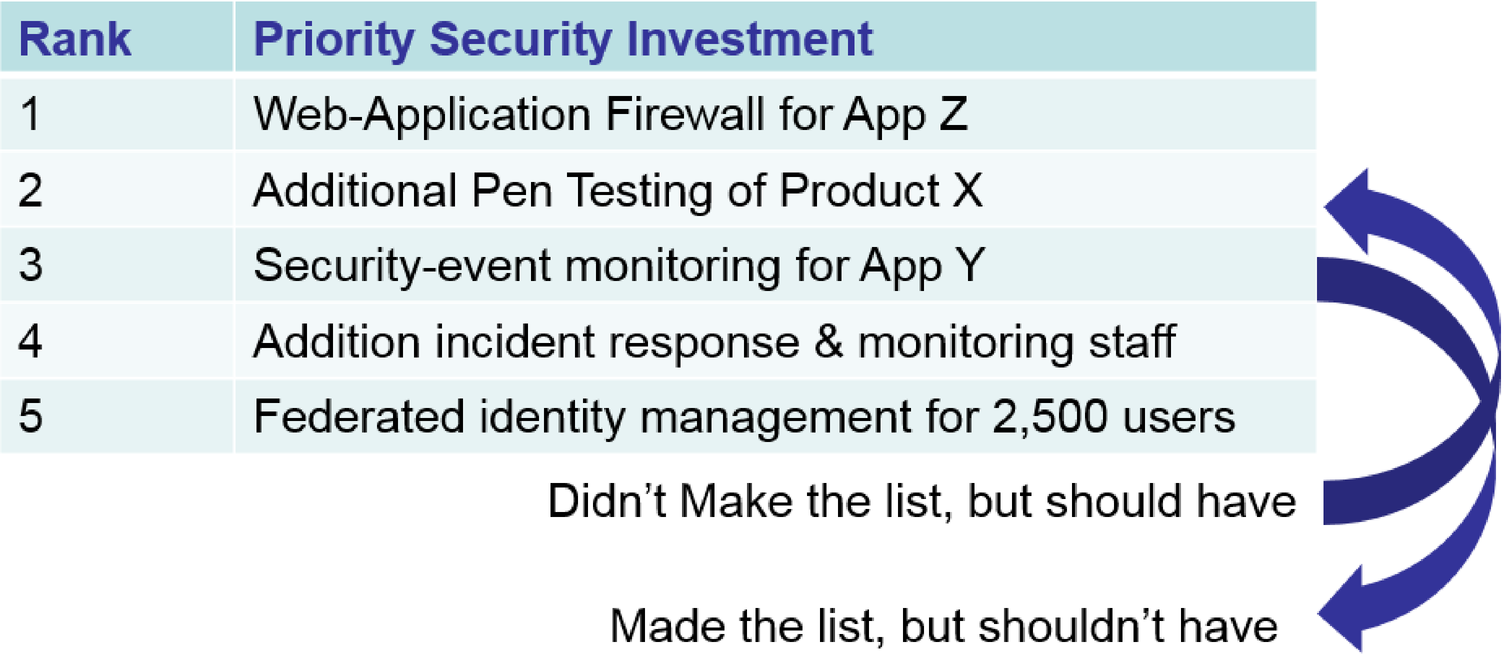
Irrelevant Influences

- Studies have shown risk aversion changes due to what should be irrelevant external factors including:

Factor	Risk Aversion
Being around smiling people	⬇
Recalling an event causing fear	⬆
Recalling an event causing anger	⬇
A recent win in an unrelated decision	⬇
A recent loss in an unrelated decision	⬆

How Much Difference Does This Make?

- If 21% of the variation of your judgments comes from random inconsistency, not the information you were given, how much of your Top 5 are there by chance?
- How many things are not in the Top 5 that should be?
- If it is a “tight race” the answer may be most…or *all*.



Rank	Priority Security Investment
1	Web-Application Firewall for App Z
2	Additional Pen Testing of Product X
3	Security-event monitoring for App Y
4	Addition incident response & monitoring staff
5	Federated identity management for 2,500 users

Didn’t Make the list, but should have

Made the list, but shouldn’t have

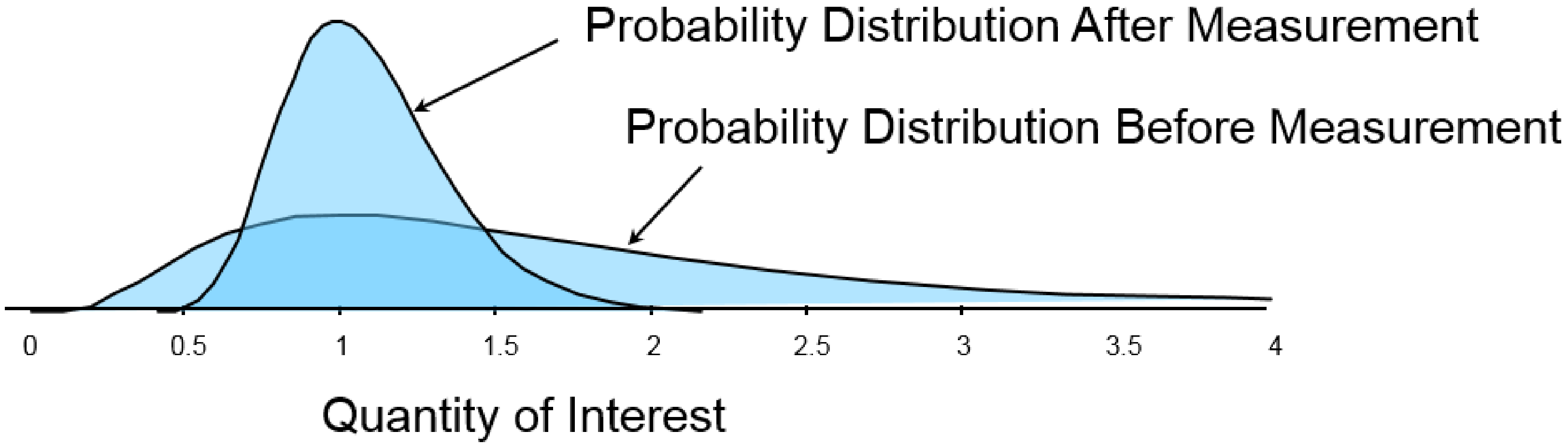
Applied Information Economics

- AIE is a practical application of quantitative methods to decision analysis problems
- Goal: Optimizing Uncertainty Reduction –Balancing measurably improved decisions and analysis effort
- It answers two questions:
  - Given the current uncertainty, what is the best decision?
  - What additional analysis or measurements are justified?

The Value of a Measurement

In big, risky decisions, even small uncertainty reductions can have considerable value.

- Most business decisions have a cost of being wrong and a chance of being wrong.
- Information reduces uncertainty in decisions.
- Less decision risk improves the chance of better decisions.



© Hubbard Decision Research, 2012

The Value of Information*

The Formula For The Value of Information:

$$EVI = \sum_{i=1}^{k} p(r_i) \max\left[\sum_{j=1}^{z} V_{1,j}\, p(\Theta_j|r_i), \sum_{j=1}^{z} V_{2,j}\, p(\Theta_j|r_i), \ldots \sum_{j=1}^{z} V_{l,j}\, p(\Theta_j|r_i),\right] - EV^*$$

OR, in its simplest form:

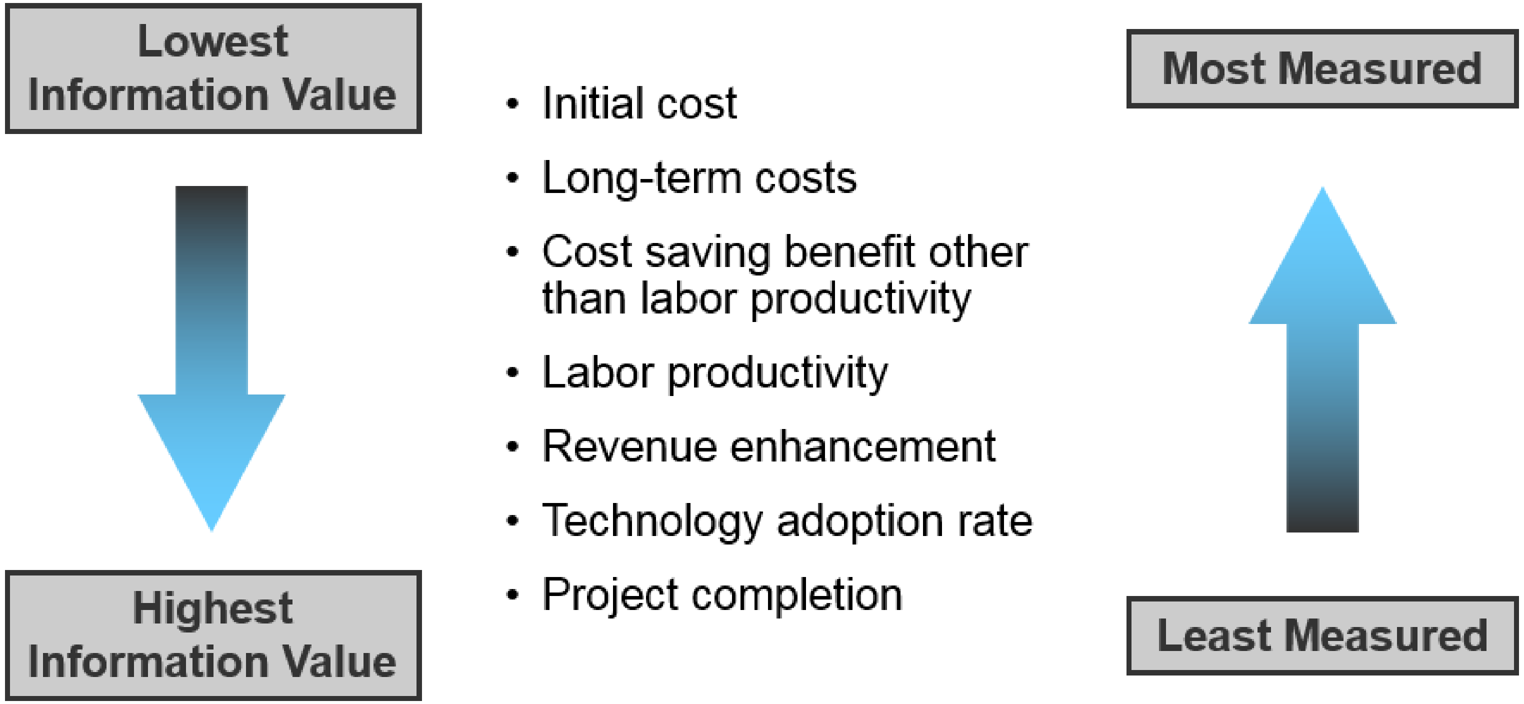
"The cost of being wrong times the chance of being wrong"

- The formula for the value of information has been around for almost 60 years but still mostly unheard of in the parts of business where it might do the most good.
- Using the formula resolves two major problems
  - Often, the most valuable measurements are ignored while time is spent on less valuable measurements.
  - Measurements are often not attempted because of misconceptions about the cost and value (fewer and simpler measurements may be required than expected).

*Covered More in Modules A-1 and A-2

The Measurement Inversion

In a business case, the economic value of measuring a variable is usually inversely proportional to the measurement attention it typically gets.



Lowest Information Value

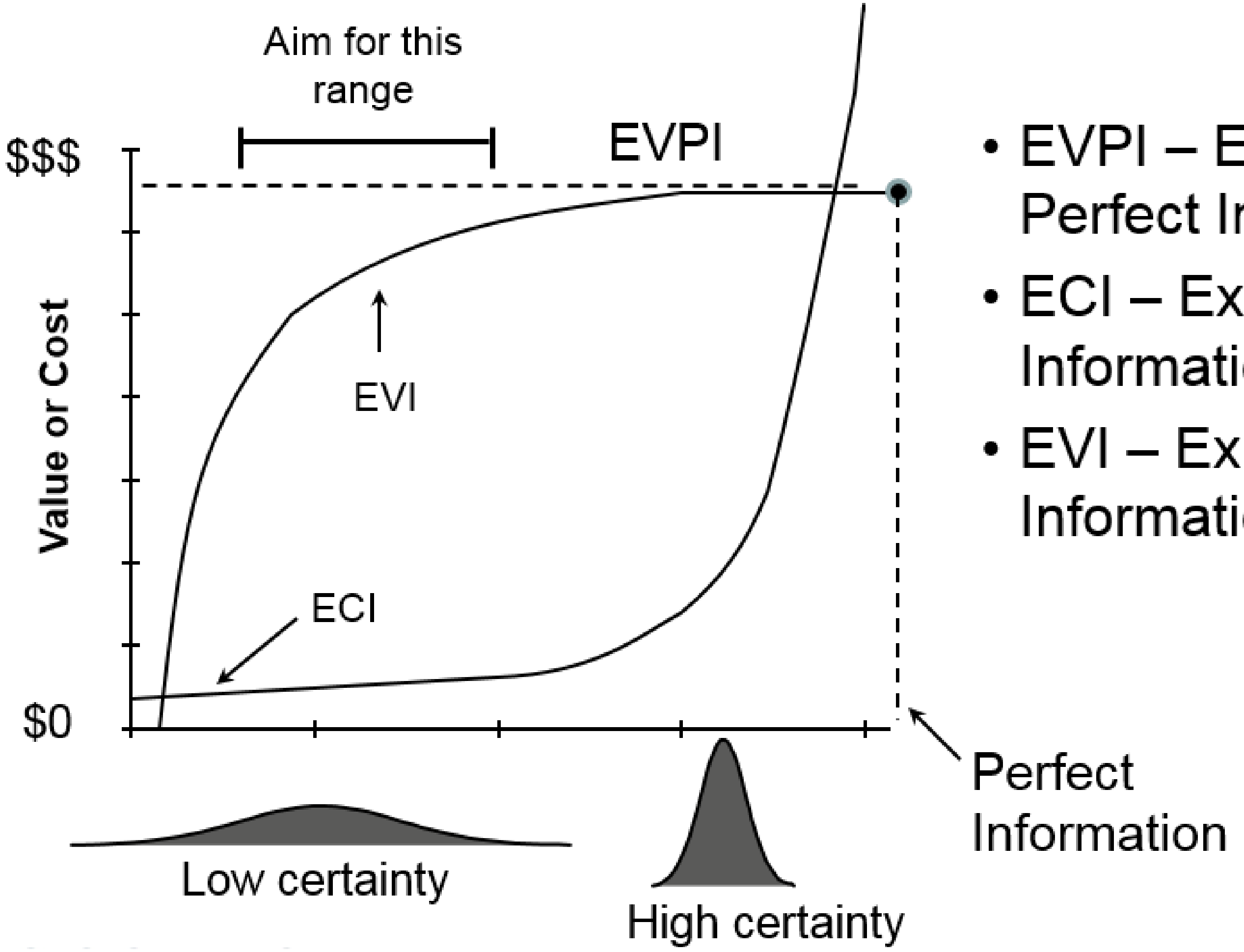
Highest Information Value

- Initial cost
- Long-term costs
- Cost saving benefit other than labor productivity
- Labor productivity
- Revenue enhancement
- Technology adoption rate
- Project completion

Most Measured

Least Measured

Increasing Value & Cost of Info.



- EVPI – Expected Value of Perfect Information
- ECI – Expected Cost of Information
- EVI – Expected Value of Information

© Hubbard Decision Research, 2012

The Fallacies Regarding the Use of Quantitative Methods vs. Current Standards

- Cybersecurity is too complex or lacks sufficient data for quantitative analysis…

  …yet can be analyzed with unaided expert intuition or soft scales.
- Probabilities can't be used explicitly because _______ ….

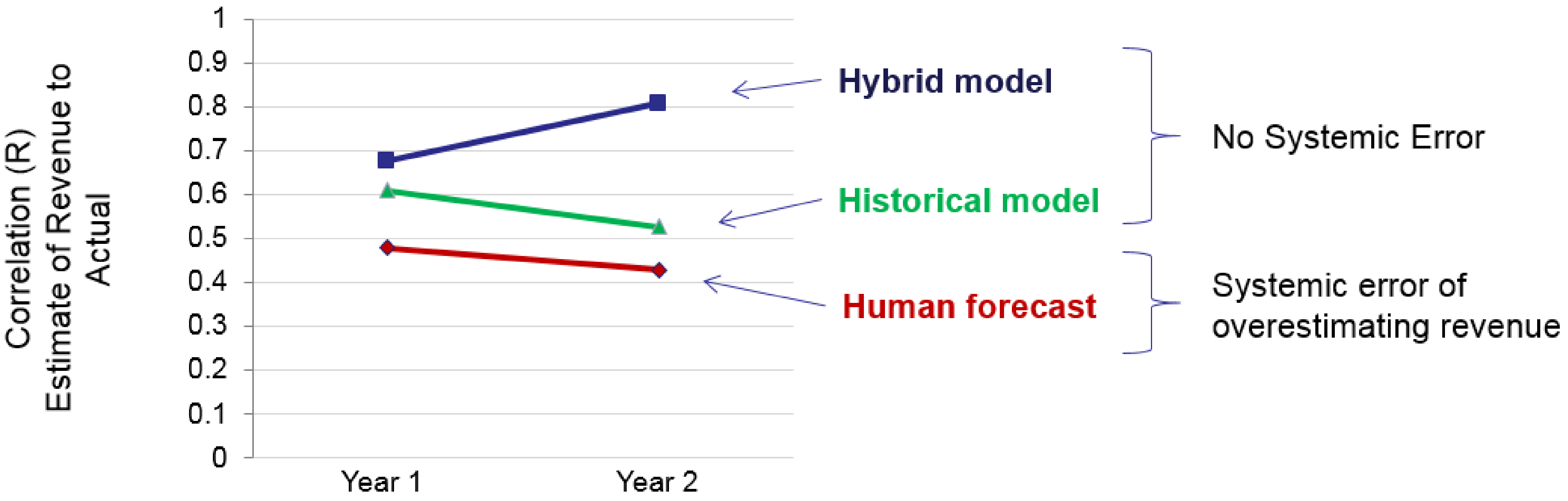
  …yet we can *imply* probabilities with ambiguous labels.

Remember, softer methods never *alleviate* a lack of data, complexity, rapidly changing environments or unpredictable human actors…

…they can only *obscure* it.

Measuring the Impact of Analysis Example (Cont.)

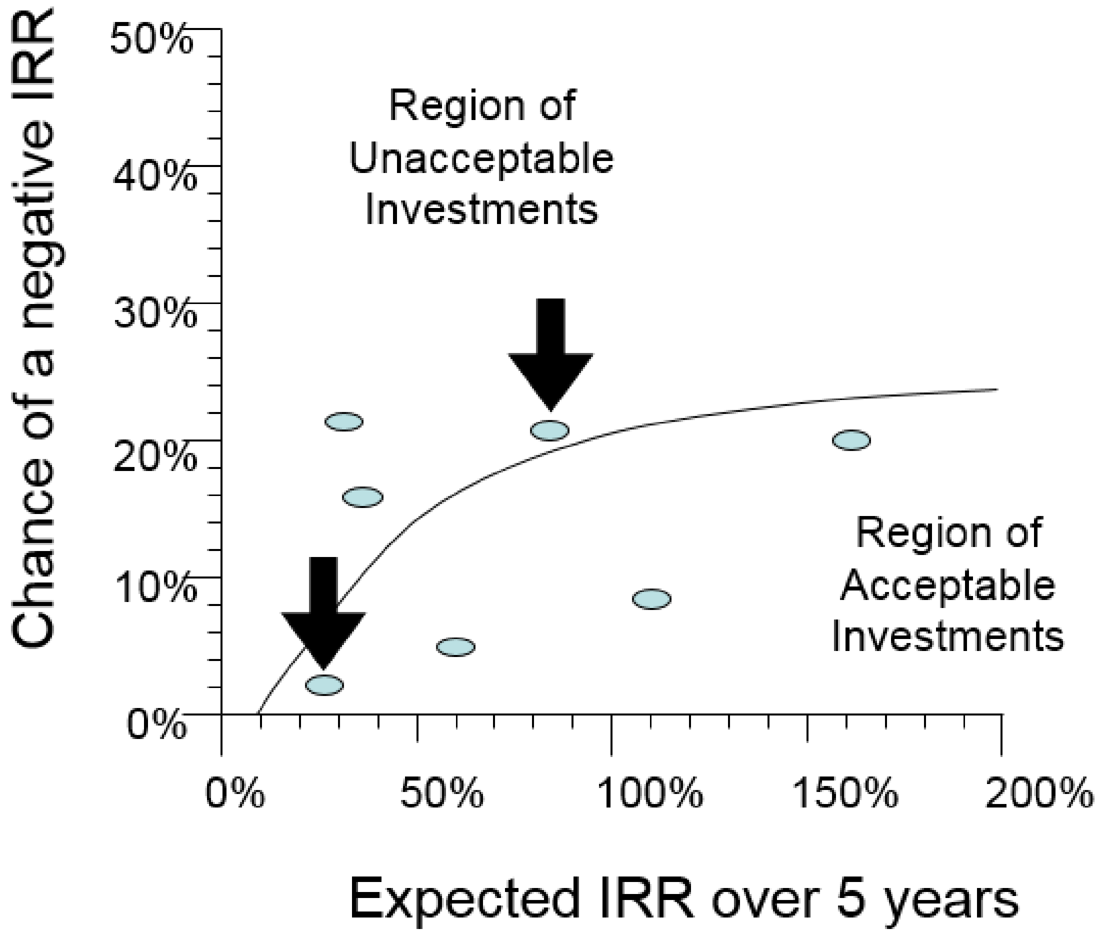
- The client was forecasting first and second year revenue of new products in the biotech lab equipment industry.
- Given both the improved correlation *and* the elimination of the systemic overestimation error, the overall forecasting error was reduced by 76%.



No Systemic Error

Systemic error of overestimating revenue

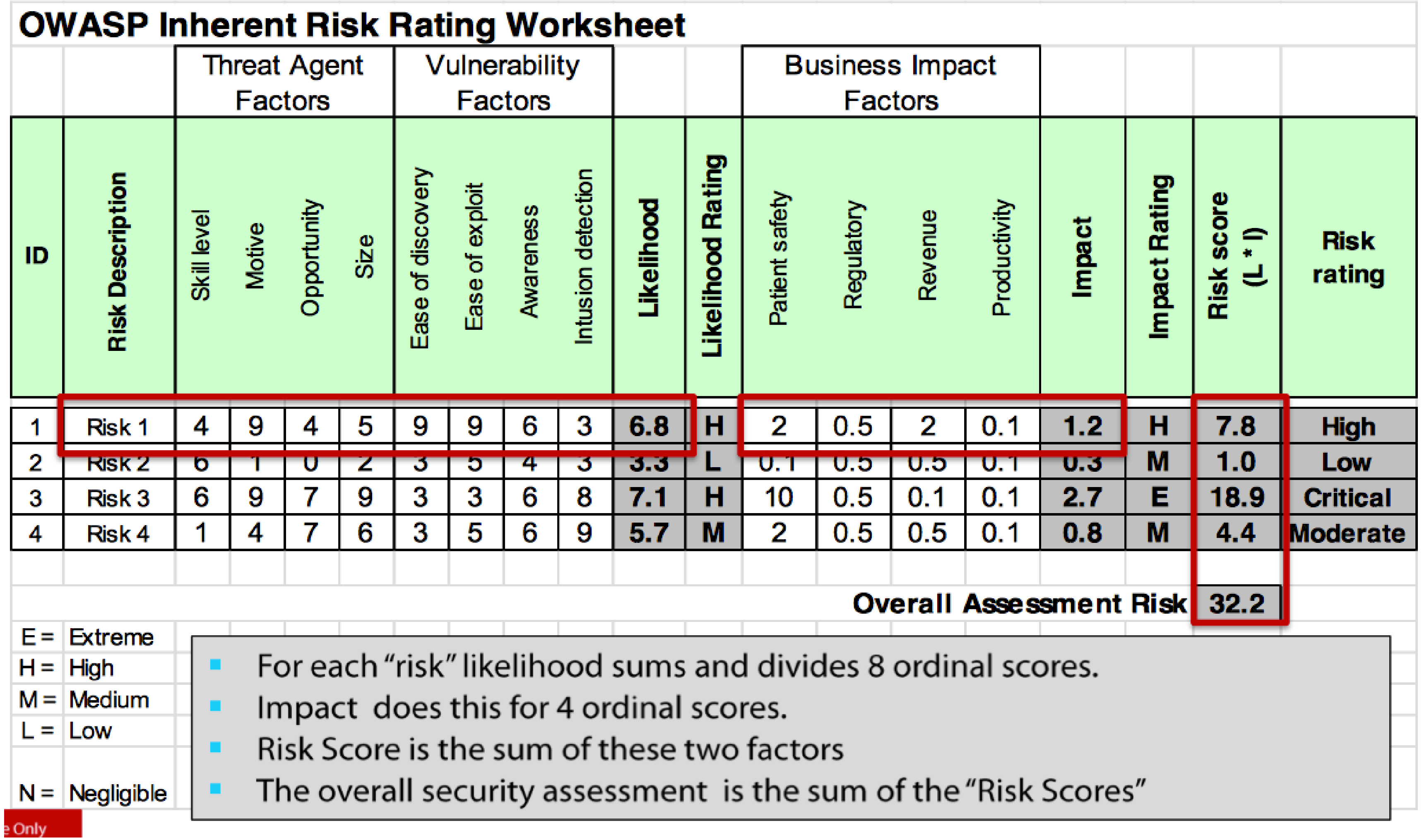
Example of Risk Effects



- These are real IT investments of $2M-$3M plotted against a client's investment boundary
- The 27% ROI investment is actually preferred to the 83% ROI investment

SECURE360

Is This the Best We Can Do?



OWASP Inherent Risk Rating Worksheet

		Threat Agent Factors				Vulnerability Factors						Business Impact Factors							
ID	**Risk Description**	Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intusion detection	**Likelihood**	**Likelihood Rating**	Patient safety	Regulatory	Revenue	Productivity	**Impact**	**Impact Rating**	**Risk score (L * I)**	**Risk rating**
1	Risk 1	4	9	4	5	9	9	6	3	**6.8**	**H**	2	0.5	2	0.1	**1.2**	**H**	**7.8**	**High**
2	Risk 2	6	1	0	2	3	5	4	3	**3.3**	**L**	0.1	0.5	0.5	0.1	**0.3**	**M**	**1.0**	**Low**
3	Risk 3	6	9	7	9	3	3	6	8	**7.1**	**H**	10	0.5	0.1	0.1	**2.7**	**E**	**18.9**	**Critical**
4	Risk 4	1	4	7	6	3	5	6	9	**5.7**	**M**	2	0.5	0.5	0.1	**0.8**	**M**	**4.4**	**Moderate**

Overall Assessment Risk **32.2**

E =	Extreme
H =	High
M =	Medium
L =	Low
N =	Negligible

e Only

- For each "risk" likelihood sums and divides 8 ordinal scores.
- Impact does this for 4 ordinal scores.
- Risk Score is the sum of these two factors
- The overall security assessment is the sum of the "Risk Scores"

Hubbard Decision Research

© Hubbard Decision Research, 2012

Selected Sources

- Tsai C., Klayman J., Hastie R. “Effects of amount of information on judgment accuracy and confidence” *Org. Behavior and Human Decision Processes,* Vol. 107, No. 2, 2008, pp 97-105
- Heath C., Gonzalez R. “Interaction with Others Increases Decision Confidence but Not Decision Quality: Evidence against Information Collection Views of Interactive Decision Making” *Organizational Behavior and Human Decision Processes,* Vol. 61, No. 3, 1995, pp 305-326
- Andreassen, P.” Judgmental extrapolation and market overreaction: On the use and disuse of news” *Journal of Behavioral Decision Making*, vol. 3 iss. 3, pp 153-174, Jul/Sep 1990
- Williams M. Dennis A., Stam A., Aronson J. “The impact of DSS use and information load on errors and decision quality” *European Journal of Operational Research,* Vol. 176, No. 1, 2007, pp 468-81
- Knutson et. al. “Nucleus accumbens activation mediates the influence of reward cues on financial risk taking” *NeuroReport*, 26 March 2008 - Volume 19 - Issue 5 - pp 509-513
- A small study presented at Cognitive Neuroscience Society meeting in 2009 by a grad student at U. of Michigan showed that simply being briefly exposed to smiling faces makes people more risk tolerant in betting games.
- Risk preferences show a strong correlation to testosterone levels – which change daily (Sapienza, Zingales, Maestripieri, 2009).
- Recalling past events that involved fear and anger change the perception of risk (Lerner, Keltner, 2001).

Uses of Applied Information Economics

AIE was applied initially to IT business cases. But over the last 20 years it has also been applied to other decision analysis problems in all areas of Business Cases, Performance Metrics, Risk Analysis, and Portfolio Prioritization.

IT

- Prioritizing IT portfolios
- Risk of software development
- Value of better information
- Value of better security
- Risk of obsolescence and optimal technology upgrades
- Value of infrastructure
- Performance metrics for the business value of applications

Business

- Movie / film project selection
- New product development
- Pharmaceuticals
- Medical devices
- Publishing
- Real estate

Engineering

- Risks of major engineering projects
- Risk of mine flooding

Government & Non Profit

- Environmental policy
- Sustainable agriculture
- Procurement methods
- Grants management

Military

- Forecasting battlefield fuel consumption
- Effectiveness of combat training to reduce roadside bomb / IED casualties
- R&D portfolios

Questions?

Contact:

Doug Hubbard

Hubbard Decision Research

dwhubbard@hubbardresearch.com

www.hubbardresearch.com

630 858 2788

- If you want electronic copies of this presentation and copies of supporting articles I mention, please leave me a business card with “Presentation” written on the back