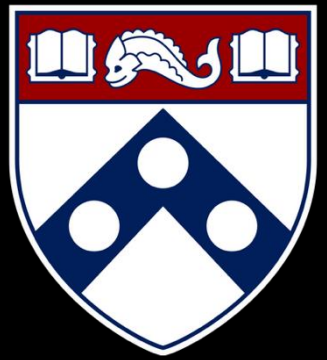
Secure Software Engineering and Management

UPenn CIS 7000-010

Michael Hicks



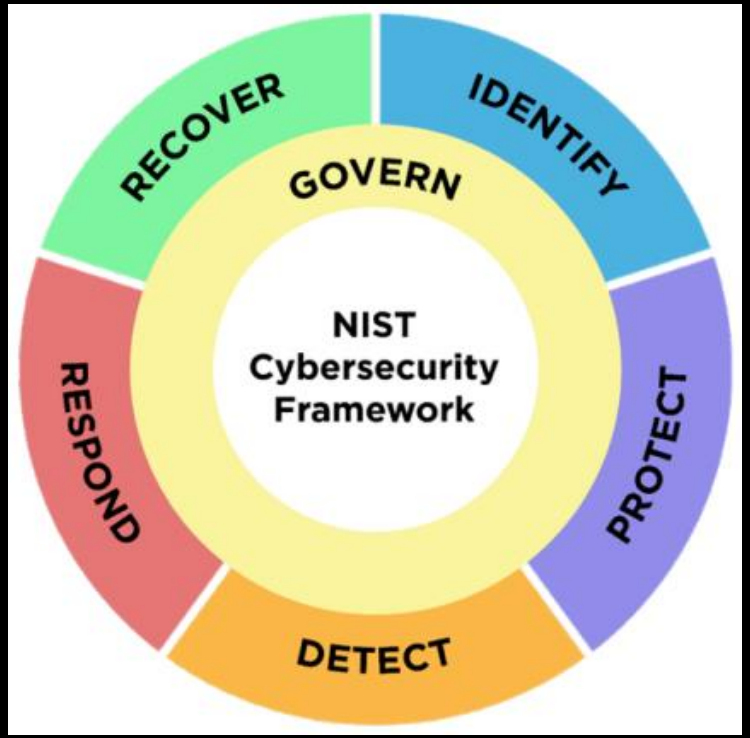
Cybersecurity Risk Management

The Big Question

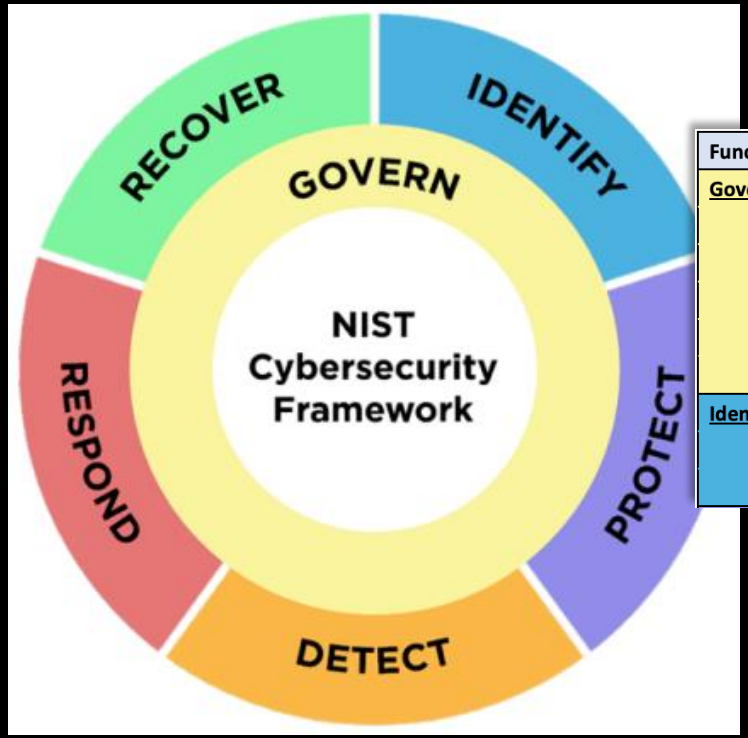
You are building and operating a cloud-hosted service with many customers and valuable data.

How do you decide what to spend on security — and on *which* security activities?

NIST CSF 2.0: What You *Should* Do

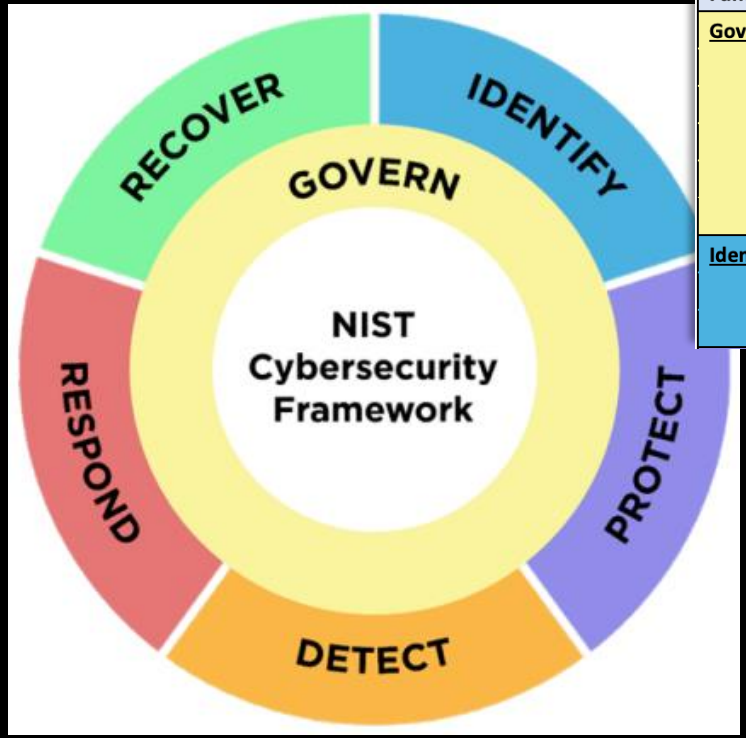


NIST CSF 2.0: What You *Should* Do



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM

NIST CSF 2.0: What You *Should* Do



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM

Under **Govern** → **Risk Management (GV.RM)**:

- GV.RM-02: Establish **risk appetite and tolerance**
- GV.RM-06: Establish a standardized method for **calculating and prioritizing** risks

Under **Identify** → **Risk Assessment (ID.RA)**:

- ID.RA-03: Identify and record threats
- ID.RA-04: Identify potential **impacts and likelihoods**
- ID.RA-05: Use these to **prioritize** risk responses

What We Know So Far

From earlier lectures:

- **Anderson**: Misaligned incentives distort security markets
- **Grigg**: The market rewards the *appearance* of security ("silver bullets")
- **Herley & van Oorschot**: Security as a scientific pursuit faces fundamental measurement challenges
- **Breen, Herley & Redmiles**: Even estimating cybercrime victimization rates is surprisingly hard

Today: Given these problems, how do we make rational security investment decisions?

Outline

1. The case for quantitative risk assessment
2. Why cyber risk is so hard to quantify
3. Giving it a shot!
4. Communicating risk

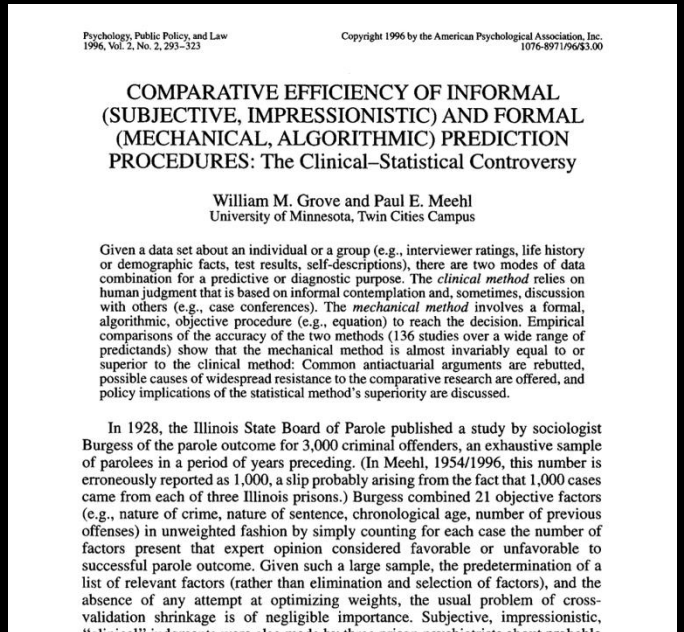
Part 1: The Case for Quantitative Risk Assessment

Clinical vs. Statistical Prediction

Across **136 studies** in medicine, psychology, and other fields, mechanical/algorithmic prediction **equals or beats** expert judgment in virtually every case

- Parole decisions
- Medical diagnoses
- Academic success predictions

Why should cybersecurity be exempt?



Psychology, Public Policy, and Law
1996, Vol. 2, No. 2, 293–323

1076-8971/96/$3.00

COMPARATIVE EFFICIENCY OF INFORMAL (SUBJECTIVE, IMPRESSIONISTIC) AND FORMAL (MECHANICAL, ALGORITHMIC) PREDICTION PROCEDURES: The Clinical–Statistical Controversy

William M. Grove and Paul E. Meehl
University of Minnesota, Twin Cities Campus

Given a data set about an individual or a group (e.g., interviewer ratings, life history or demographic facts, test results, self-descriptions), there are two modes of data combination for a predictive or diagnostic purpose. The *clinical method* relies on human judgment that is based on informal contemplation and, sometimes, discussion with others (e.g., case conferences). The *mechanical method* involves a formal, algorithmic, objective procedure (e.g., equation) to reach the decision. Empirical comparisons of the accuracy of the two methods (136 studies over a wide range of predictands) show that the mechanical method is almost invariably equal to or superior to the clinical method: Common antiactuarial arguments are rebutted, possible causes of widespread resistance to the comparative research are offered, and policy implications of the statistical method's superiority are discussed.

In 1928, the Illinois State Board of Parole published a study by sociologist Burgess of the parole outcome for 3,000 criminal offenders, an exhaustive sample of parolees in a period of years preceding. (In Meehl, 1954/1996, this number is erroneously reported as 1,000, a slip probably arising from the fact that 1,000 cases came from each of three Illinois prisons.) Burgess combined 21 objective factors (e.g., nature of crime, nature of sentence, chronological age, number of previous offenses) in unweighted fashion by simply counting for each case the number of factors present that expert opinion considered favorable or unfavorable to successful parole outcome. Given such a large sample, the predetermination of a list of relevant factors (rather than elimination and selection of factors), and the absence of any attempt at optimizing weights, the usual problem of cross-validation shrinkage is of negligible importance. Subjective, impressionistic,

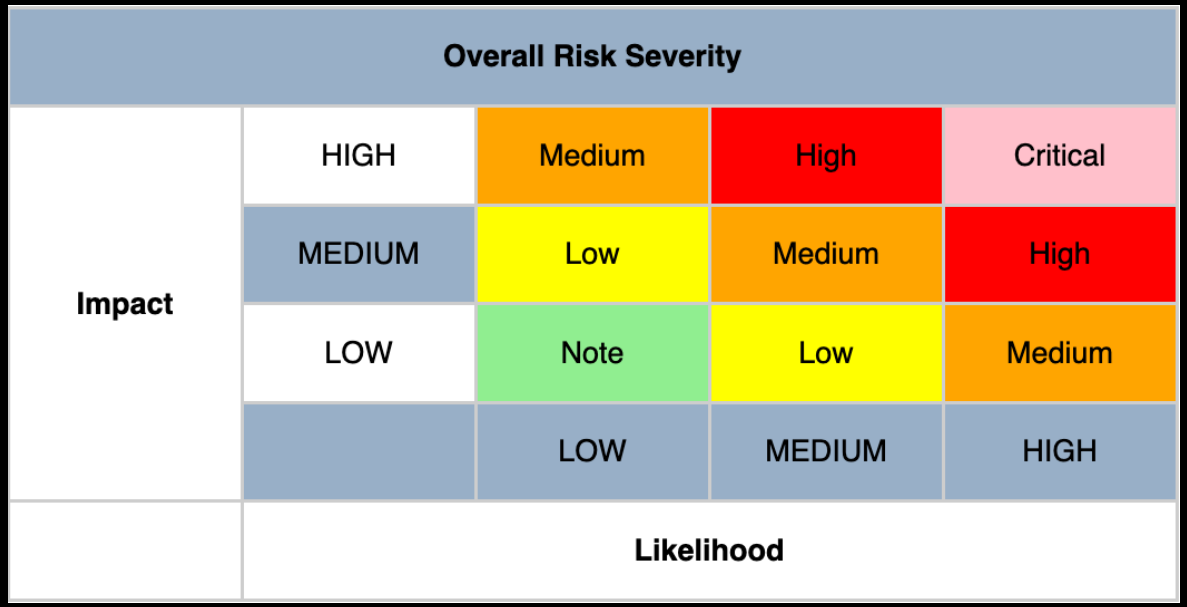
Why Quantify Risk?

- “We need more security” is not actionable
- “We face $2M in expected annual loss from ransomware; a $200K investment in backup testing reduces that by 60%” — *that’s* actionable

So we need an algorithm. What does one look like?

The OWASP Risk Rating Methodology (2010s)

A widely used approach: rate **likelihood** and **impact** on 0–9 scales, average them, plot on a heat map



The OWASP Risk Rating Methodology (2010s)

A widely used approach: rate **likelihood** and **impact** on 0–9 scales, average them, plot on a heat map.

Likelihood = average of 8 factors:

- *Threat agent*: skill level, motive, opportunity, size
- *Vulnerability*: ease of discovery, ease of exploit, awareness, intrusion detection

Impact = average of 4 factors:

- Technical: confidentiality, integrity, availability, accountability
- (Or business: financial, reputation, compliance, privacy)

Example: Ransomware Hits Our SaaS Company

Threat agent factors (0–9 each):

Factor	Score	Reasoning
Skill level	6	Ransomware-as-a-service lowers the bar
Motive	9	Direct financial gain
Opportunity	5	Need initial access (phishing, vuln)
Size	7	Large criminal ecosystem

Average: **(6 + 9 + 5 + 7) / 4 = 6.75**

OWASP Example: Vulnerability

Vulnerability factors (0–9 each):

Factor	Score	Reasoning
Ease of discovery	5	Scanning tools find exposed services
Ease of exploit	6	Known CVEs, phishing kits available
Awareness	7	Ransomware is well-known
Intrusion detection	4	We have EDR, some logging

Average: **(5 + 6 + 7 + 4) / 4 = 5.5**

Overall likelihood = (6.75 + 5.5) / 2 = 6.125 → HIGH

OWASP Example: Technical Impact

Technical impact factors (0–9 each):

Factor	Score	Reasoning
Confidentiality	7	Data exfiltration before encryption
Integrity	9	All data encrypted
Availability	9	Service completely down
Accountability	3	Attackers usually identifiable as group

Average: **(7 + 9 + 9 + 3) / 4 = 7.0 → HIGH**

OWASP Result: The Heat Map

Risk Severity	**LOW impact**	**MEDIUM impact**	**HIGH impact**
HIGH likelihood	Medium	High	**Critical**
MEDIUM likelihood	Low	Medium	High
LOW likelihood	Note	Low	Medium

Our ransomware scenario: **HIGH likelihood** × **HIGH impact** = **Critical**

So… now what?

What's Wrong with Risk Matrices?

1. Correctly rank **less than 10%** of randomly selected hazard pairs
2. Can assign **higher** ratings to **smaller** risks
3. Can be **"worse than useless"** when frequency and severity are negatively correlated

Risk Analysis, Vol. 28, No. 2, 2008 DOI: 10.1111/j.1539-6924.2008.01030.x

What's Wrong with Risk Matrices?

Louis Anthony (Tony) Cox, Jr.*

Risk matrices—tables mapping "frequency" and "severity" ratings to corresponding risk priority levels—are popular in applications as diverse as terrorism risk analysis, highway construction project management, office building risk analysis, climate change risk management, and enterprise risk management (ERM). National and international standards (e.g., Military Standard 882C and AS/NZS 4360:1999) have stimulated adoption of risk matrices by many organizations and risk consultants. However, little research rigorously validates their performance in actually improving risk management decisions. This article examines some mathematical properties of risk matrices and shows that they have the following limitations. (a) *Poor Resolution*. Typical risk matrices can correctly and unambiguously compare only a small fraction (e.g., less than 10%) of randomly selected pairs of hazards. They can assign identical ratings to quantitatively very different risks ("range compression"). (b) *Errors*. 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. (c) *Suboptimal Resource Allocation*. Effective allocation of resources to risk-reducing countermeasures cannot be based on the categories provided by risk matrices. (d) *Ambiguous Inputs and Outputs*. Categorizations of severity cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g., frequency and severity categorizations) and resulting outputs (i.e., risk ratings) require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks. These limitations suggest that risk matrices should be used with caution, and only with careful explanations of embedded judgments.

KEY WORDS: AS/NZS 4360; decision analysis; enterprise risk management; Military Standard 882C; qualitative risk assessment; risk matrix; semiquantitative risk assessment; worse-than-useless information

1. INTRODUCTION

A *risk matrix* is a table that has several categories of "probability," "likelihood," or "frequency" for its rows (or columns) and several categories of "severity," "impact," or "consequences" for its columns (or rows, respectively). It associates a recommended level of risk, urgency, priority, or management action with each row-column pair, that is, with each cell. Table I shows an example of a standard 5 × 5 risk matrix developed by the Federal Highway Administration for assessing risks and setting priorities in addressing issues as diverse as unexpected geotechnical problems at bridge piers and unwillingness of landowners to sell land near critical road junctions.

The green, yellow, and red cells indicate low, medium, and high or urgent risk levels based on ratings of probability (vertical axis) and impact (horizontal axis) ranging from "VL" (very low) to "VH" (very high).

Table II shows a similar example of a 5 × 5 risk matrix from a 2007 Federal Aviation Administration (FAA) Advisory Circular (AC) introducing the concept of a safety management system for airport operators. The accompanying explanation states: "Hazards are ranked according to the severity and the likeli-

* Address correspondence to Louis Anthony (Tony) Cox; Cox Associates and University of Colorado, 503 Franklin St., Denver, CO 80218; tel: 303-388-1778; fax: 303-388-0609; tcoxdenver@aol.com.

Example 5x5 Risk Matrix

Score	Likelihood (annual)	Impact
1 Very Low	<1%	<$10K
2 Low	1–5%	$10K–$100K
3 Medium	5–20%	$100K–$1M
4 High	20–50%	$1M–$10M
5 Very High	>50%	**>$10M** *(unbounded!)*

Inspired in part by NIST 800-30

Risk score = Likelihood × Impact. **“Critical”** = score ≥ 20.

Each bucket spans **~5–10× in real values.** Bucket 5 for impact has **no upper bound at all.** That’s where Cox’s reversal comes from.

Example of Cox's Reversal

Our SaaS company assesses two risks.

Risk A — Major PII breach *(Marriott-class event)*

- Analyst: Likelihood **3 (Medium)**, Impact **5 (Very High)**
- Cell: 3 × 5 = **15** → "High" *(not Critical)*

Risk B — Business Email Compromise (BEC) / O365 account takeover

- Analyst: Likelihood **5 (Very High)**, Impact **4 (High)**
- Cell: 5 × 4 = **20** → **Critical** *(upper-right)*

The Risk Matrix

Bold cells = “Critical” (score ≥ 20).
B lands in the Critical corner.
A lands one cell below.

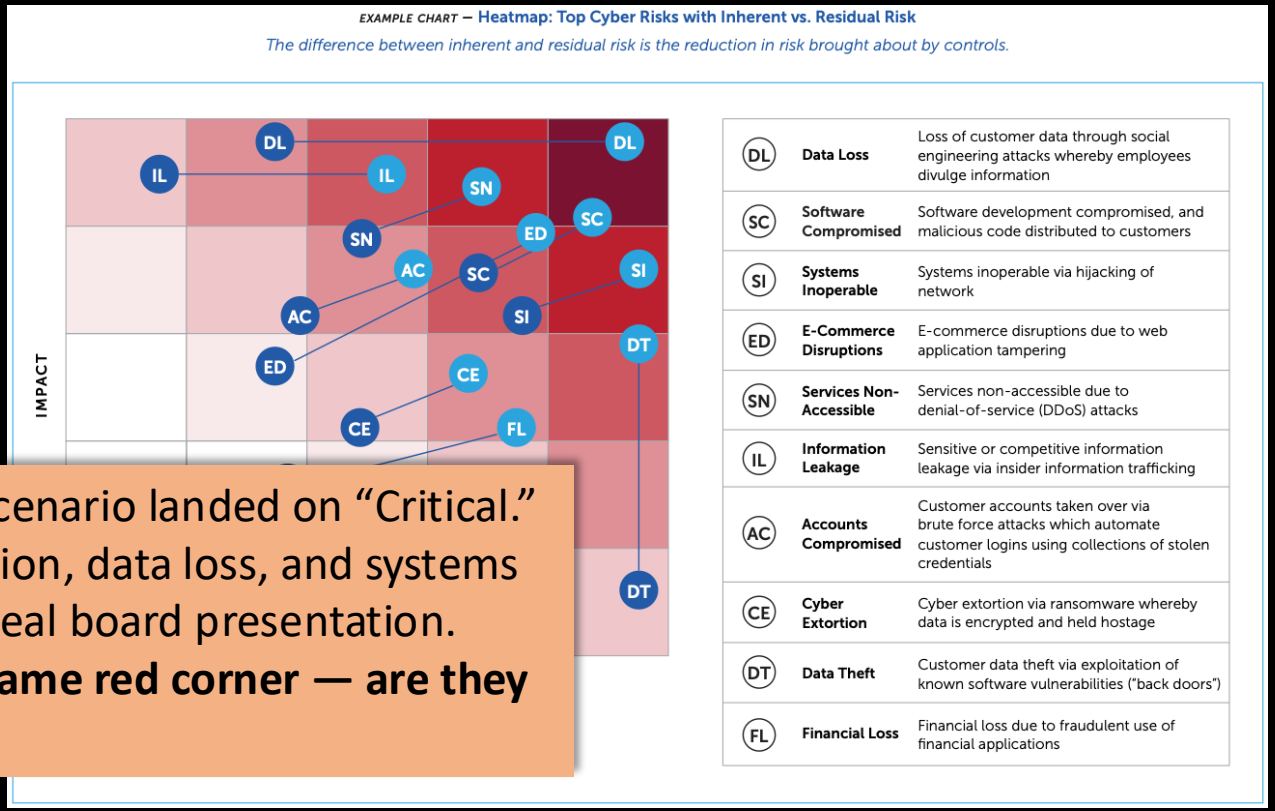
	I=1	I=2	I=3	I=4	I=5
L=5	5	10	15	20 ← **B**	25
L=4	4	8	12	16	20
L=3	3	6	9	12	15 ← **A**
L=2	2	4	6	8	10
L=1	1	2	3	4	5

Risk A’s expected loss is **~87× larger** than Risk B’s.
The matrix has the ranking reversed.

Risk	Actual likelihood	Actual impact	Expected annual loss
A (breach)	15% (top of bucket 3)	**$40M**	**$6,000,000**
B (BEC)	60% (bottom of bucket 5)	$115K	$69,000

Exhibit A: CISOs Use Heatmaps Too

From an actual Fortune 1000 CISO board presentation (RSAC ESAF, 2022)



Our ransomware scenario landed on "Critical." So did cyber extortion, data loss, and systems inoperable in this real board presentation. **They're all in the same red corner — are they the same risk?**

We Need Something Better

The standard method (risk matrices) is **mathematically broken**

But CISOs at the world's largest companies **still use it**

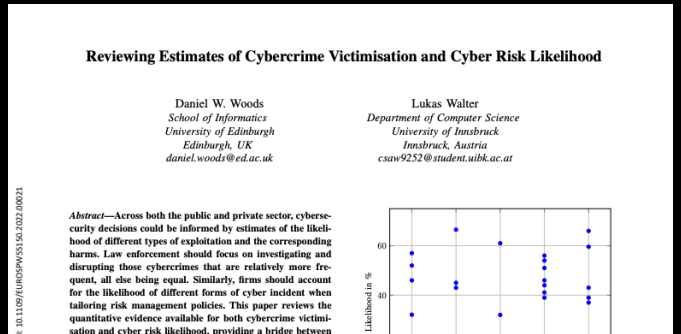
Why? And what should we use instead?

First: let's understand *why* cyber risk is so hard to quantify.

Part 2: Why Cyber Risk Is So Hard to Quantify

The Fundamental Data Problem

- Different studies show **unstable, contradictory trends**
- Measurement methodologies are **incomparable** across studies
- We can't even reliably estimate **victimization rates**



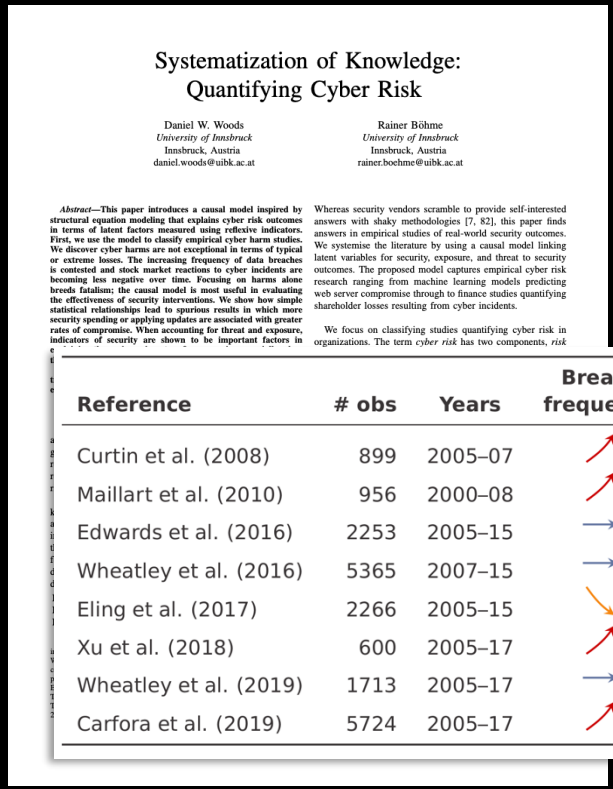
Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood

Daniel W. Woods
School of Informatics
University of Edinburgh
Edinburgh, UK
daniel.woods@ed.ac.uk

Lukas Walter
Department of Computer Science
University of Innsbruck
Innsbruck, Austria
csaw9252@student.uibk.ac.at

***Abstract*—Across both the public and private sector, cybersecurity decisions could be informed by estimates of the likelihood of different types of exploitation and the corresponding harms. Law enforcement should focus on investigating and disrupting those cybercrimes that are relatively more frequent, all else being equal. Similarly, firms should account for the likelihood of different forms of cyber incident when tailoring risk management policies. This paper reviews the quantitative evidence available for both cybercrime victimisation and cyber risk likelihood, providing a bridge between**

10.1109/EuroSPW55150.2022.00021



Systematization of Knowledge:
Quantifying Cyber Risk

Daniel W. Woods
University of Innsbruck
Innsbruck, Austria
daniel.woods@uibk.ac.at

Rainer Böhme
University of Innsbruck
Innsbruck, Austria
rainer.boehme@uibk.ac.at

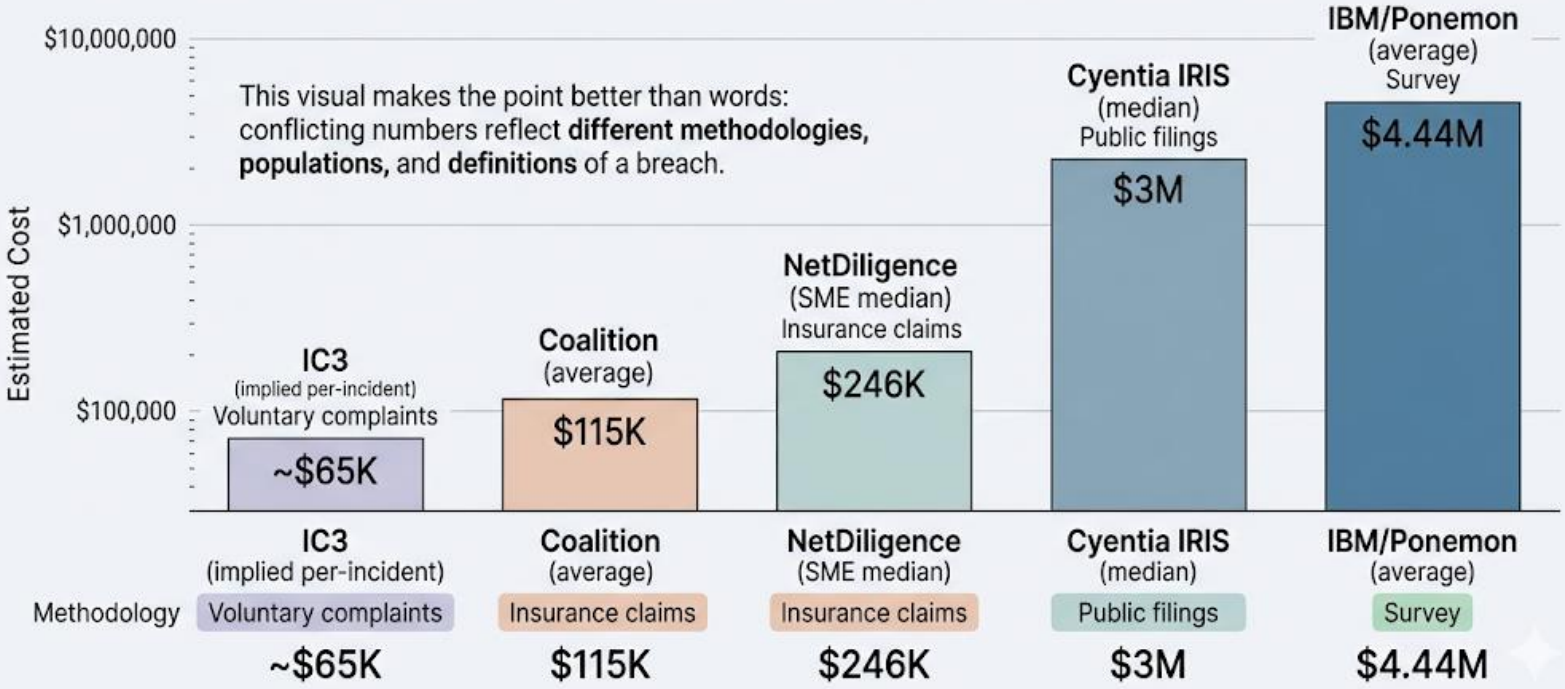
***Abstract*—This paper introduces a causal model inspired by structural equation modeling that explains cyber risk outcomes in terms of latent factors measured using reflexive indicators. First, we use the model to classify empirical cyber harm studies. We discover cyber harms are not exceptional in terms of typical or extreme losses. The increasing frequency of data breaches is contested and stock market reactions to cyber incidents are becoming less negative over time. Focusing on harms alone breeds fatalism; the causal model is most useful in evaluating the effectiveness of security interventions. We show how simple statistical relationships lead to spurious results in which more security spending or applying updates are associated with greater rates of compromise. When accounting for threat and exposure, indicators of security are shown to be important factors in**

Whereas security vendors scramble to provide self-interested answers with shaky methodologies [7, 82], this paper finds answers in empirical studies of real-world security outcomes. We systemise the literature by using a causal model linking latent variables for security, exposure, and threat to security outcomes. The proposed model captures empirical cyber risk research ranging from machine learning models predicting web server compromise through to finance studies quantifying shareholder losses resulting from cyber incidents.

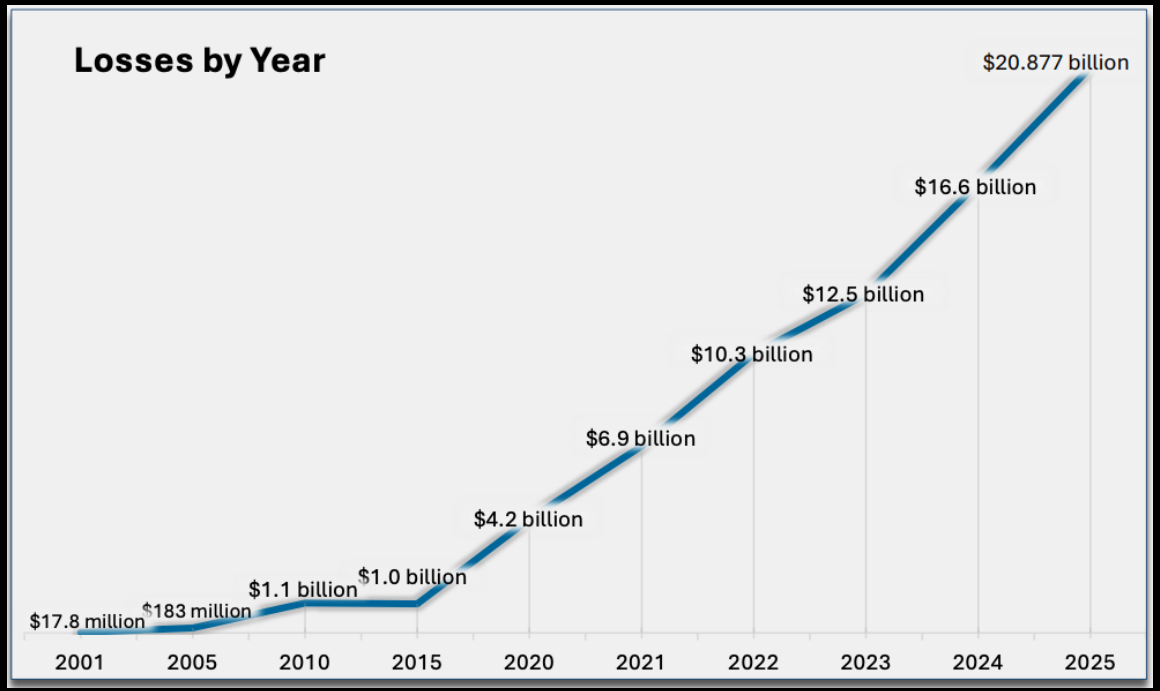
We focus on classifying studies quantifying cyber risk in organizations. The term *cyber risk* has two components, *risk*

Reference	# obs	Years	Breach frequency	Breach size
Curtin et al. (2008)	899	2005–07	↗	?
Maillart et al. (2010)	956	2000–08	↗	→
Edwards et al. (2016)	2253	2005–15	→	→
Wheatley et al. (2016)	5365	2007–15	→	↗
Eling et al. (2017)	2266	2005–15	↘	→
Xu et al. (2018)	600	2005–17	↗	→
Wheatley et al. (2019)	1713	2005–17	→	→
Carfora et al. (2019)	5724	2005–17	↗	?

Cost of a Data Breach: 1-2 Order of Magnitude Variation Across Industry Reports



FBI IC3: The Floor Estimate



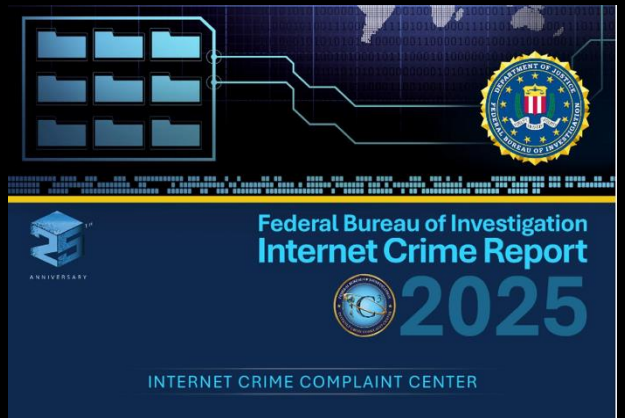
FBI IC3: The Floor Estimate

FBI Internet Crime Complaint Center, 2025:

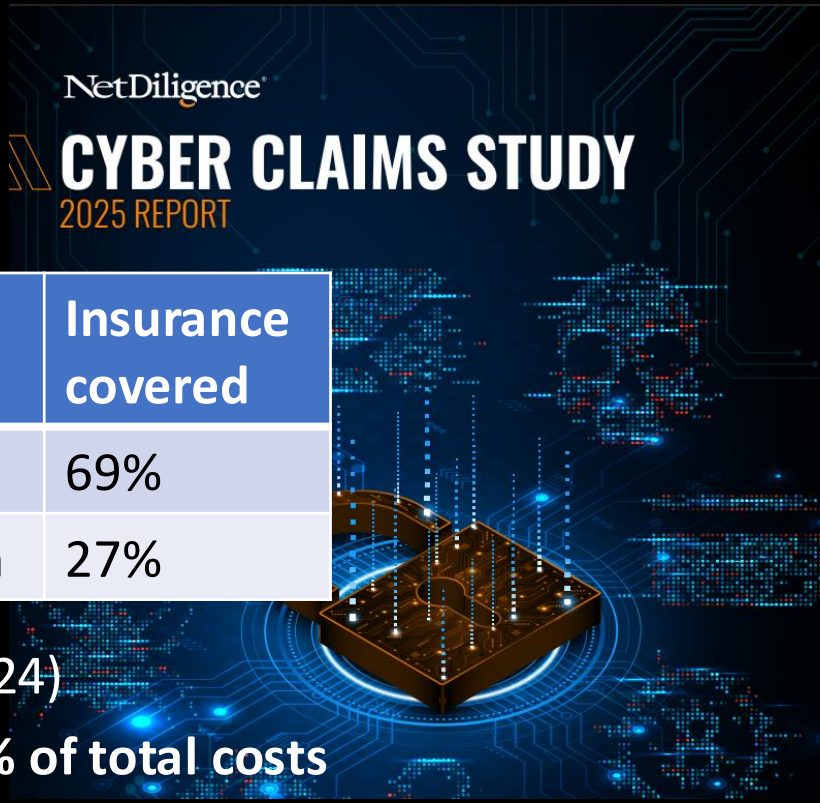
- Total reported losses: **$20.9 billion**
- BEC alone: **$3.05 billion**
- Ransomware: **$32.3 million** (!)

excludes downtime, remediation, and lost business.

IC3 is voluntary self-reporting — captures ~10–15% of actual incidents



Insurance Claims: The Most Credible Source



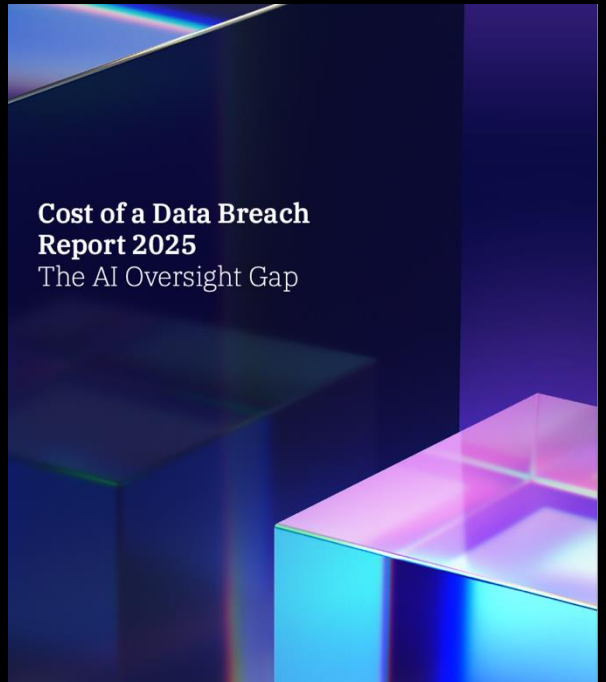
Company size	Average incident cost	Insurance covered
SME (<$2B revenue)	**$264,000**	69%
Large (>$2B revenue)	**$10.3 million**	27%

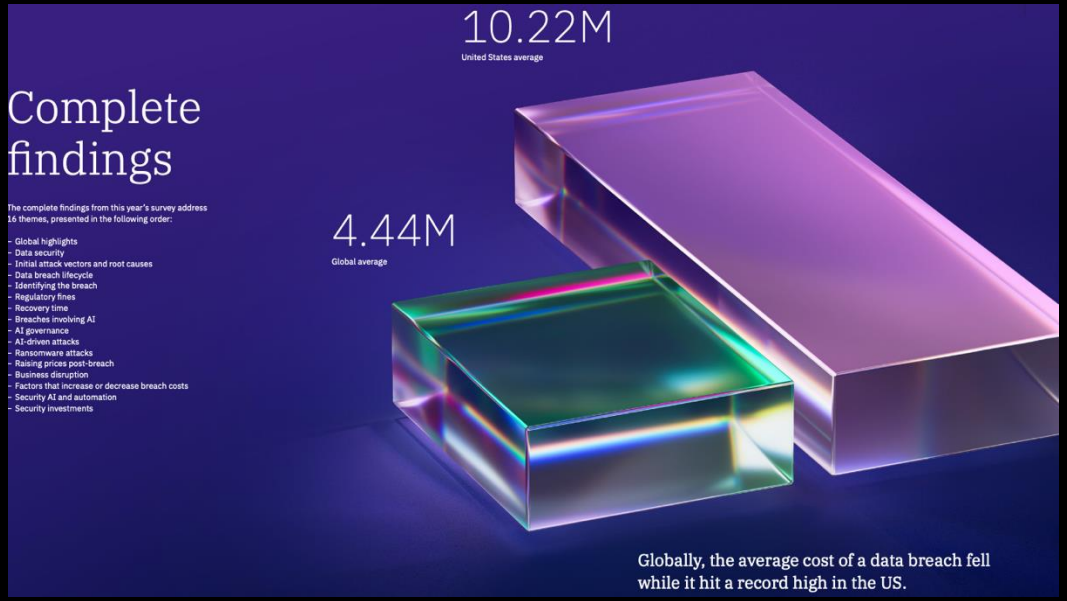
(10,402 actual insurance claims. 2020-2024)

Large companies = **2% of claims** but **>50% of total costs**

The Widely-Cited Number: $10M

IBM/Ponemon Cost of a Data Breach 2025





The Widely-Cited Number (Why It's Weak)

IBM/Ponemon Cost of a Data Breach 2025:

- Global average: **$4.44 million**
- U.S. average: **$10.22 million**

Methodology problems:

- **Survey-based**: executives *estimate* costs, not verified data
- **Excludes mega-breaches** (>113K records)
- Per-record cost model explains only **2–13% of variance**
- **Sponsored by IBM**, which sells security products

The Loss Distribution: Fat Tails

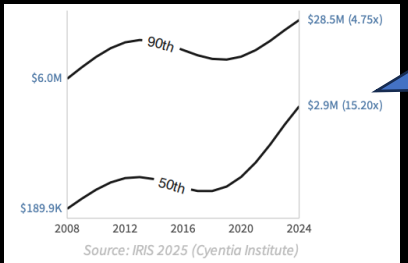


Figure 10: Trend analysis of median and 90th percentile losses

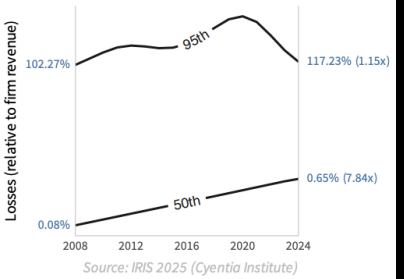


Figure 11: Trend analysis of median and 95th percentile losses as a percent of revenue

$2.9M in 2024

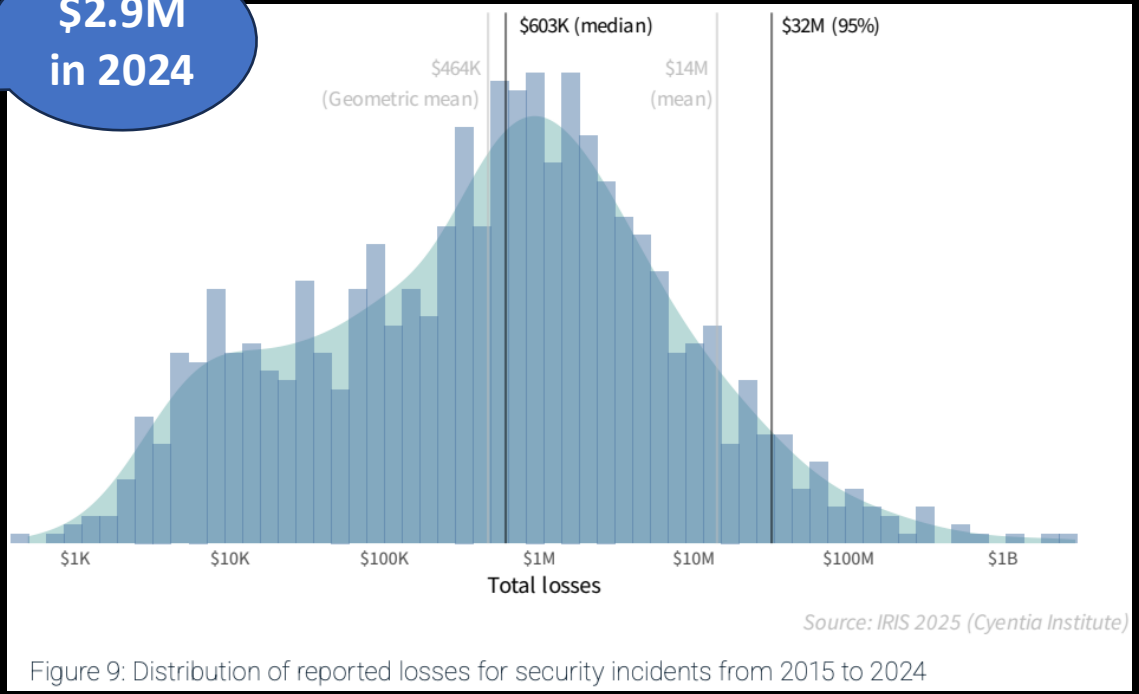


Figure 9: Distribution of reported losses for security incidents from 2015 to 2024

Cyentia IRIS 2025 (150,000+ incidents, 2008–2024)

Where Risk Quantification Works: Building Codes

Why Cybersecurity Breaks the Pattern

	Structural engineering	Cybersecurity
Governing laws	Stable physics	No “physics” of attacker behavior
Adversary	Nature — no intent	Active, intelligent, adaptive
Failure modes	Catalogued from centuries	Constantly evolving
Historical data	Abundant, systematic	Sparse, proprietary
Landscape change	Codes evolve over decades	Every update changes the attack surface

The Aviation Paradox

Downer (2017): Aviation's safety record **cannot be explained** by the testing and modeling the industry credits

- Can't validate claims like 10^{-9} failures/flight hour — would need **billions of test hours**
- Same problem applies to nuclear safety

Minerva (2017) 55:229–248
DOI 10.1007/s11024-017-9322-4

CrossMark

The Aviation Paradox: Why We Can 'Know' Jetliners But Not Reactors

John Downer[1]

Published online: 7 June 2017

Abstract Publics and policymakers increasingly have to contend with the risks of complex, safety-critical technologies, such as airframes and reactors. As such, 'technological risk' has become an important object of modern governance, with state regulators as core agents, and 'reliability assessment' as the most essential metric. The Science and Technology Studies (STS) literature casts doubt on whether or not we should place our faith in these assessments because predictively calculating the ultra-high reliability required of such systems poses seemingly insurmountable epistemological problems. This paper argues that these misgivings are warranted in the nuclear sphere, despite evidence from the aviation sphere suggesting that such calculations can be accurate. It explains why regulatory calculations that predict the reliability of new airframes cannot work in principle, and then it explains why those calculations work in practice. It then builds on this explanation to argue that the means by which engineers manage reliability in aviation is highly domain-specific, and to suggest how a more nuanced understanding of jetliners could inform debates about nuclear energy.

Keywords Engineering · Reliability · Risk · Safety · Regulation · Technology assessment · Nuclear energy · Civil aviation · Jetliners · Reactors

If politics means anything today it must become 'the art of the impossible.'
~Lewis Mumford (1954: 7)

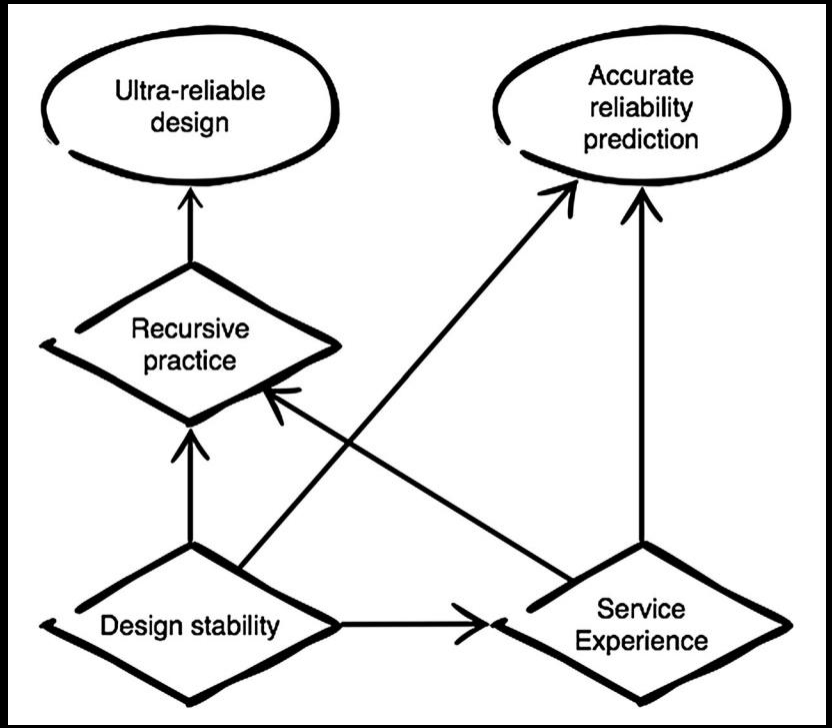
Ultra-high reliability assessments

- Reliability like security – a negative property.
  - Forces it to be contextual: You have to define the circumstances under which you agree the bad thing can't happen, and you have to carefully define the parameters of the bad thing
- Predictive reliability assessment goal: 1B hours of failure-free service
- Approach: Model-based analysis
  - Assess individual components **inductively**
  - Reason about their combined reliability **deductively**, using a model
- Example: Redundant engines
  - Single engine failure probability P, based on measurements
  - Total engine failure of two engines = P^2
    - Assuming engine failures are independent

Ultra-high reliability assessments, questioned

- Epistemically dubious!
  - “There is no way that experts should be able to deduce from tests and models that a yet-unrealized jetliner or reactor will be reliable to the extraordinary levels that they claim.”
  - Why? We cannot observe the tech in action long enough, or draw on other prior evidence, to extrapolate to the hoped-for conclusion.
    - 1B hours is 114,000(ish) years! Long time to run to test directly
- Nevertheless: “A stubbornly suicidal traveler would have to take a random airline flight every day for 19,000 years to stand a better-than-even chance of succumbing to a fatal crash.”

Why it works for (most) civil aviation



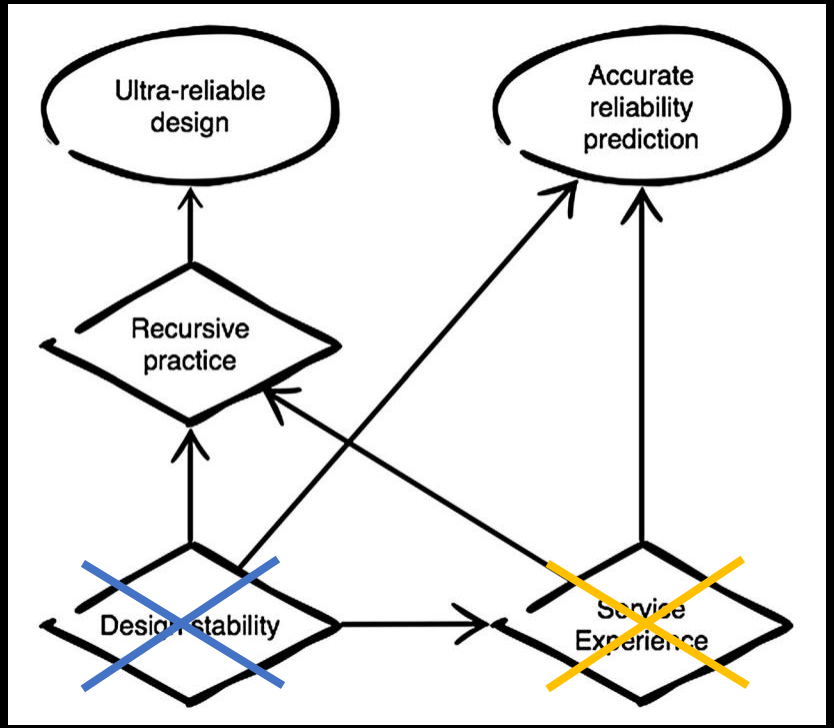
But not the Concorde

But not the Concorde

1 catastrophic failure, July 25, 2000

Very different design

- 1354 mph cruising speed
- ‘Double delta’ wing shape
- Unorthodox landing gear and a nose that moved
- Special heat-resistant alloys

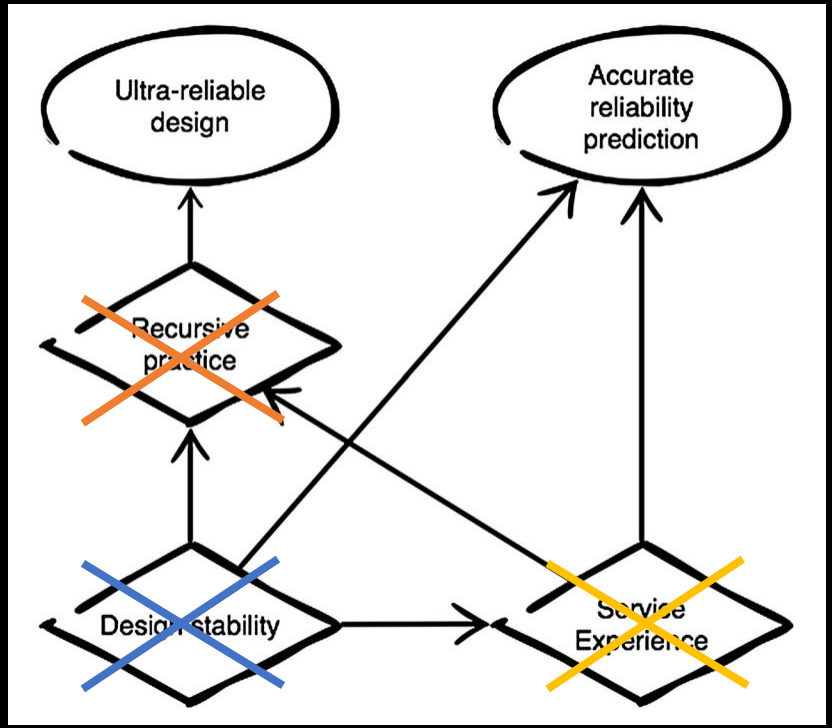


Only 14 planes in operation totaling 50,000 flights over 27 years

And not Nuclear

Lessons are learned and improvements made, but do not generalize

Reactor designs broadly dissimilar



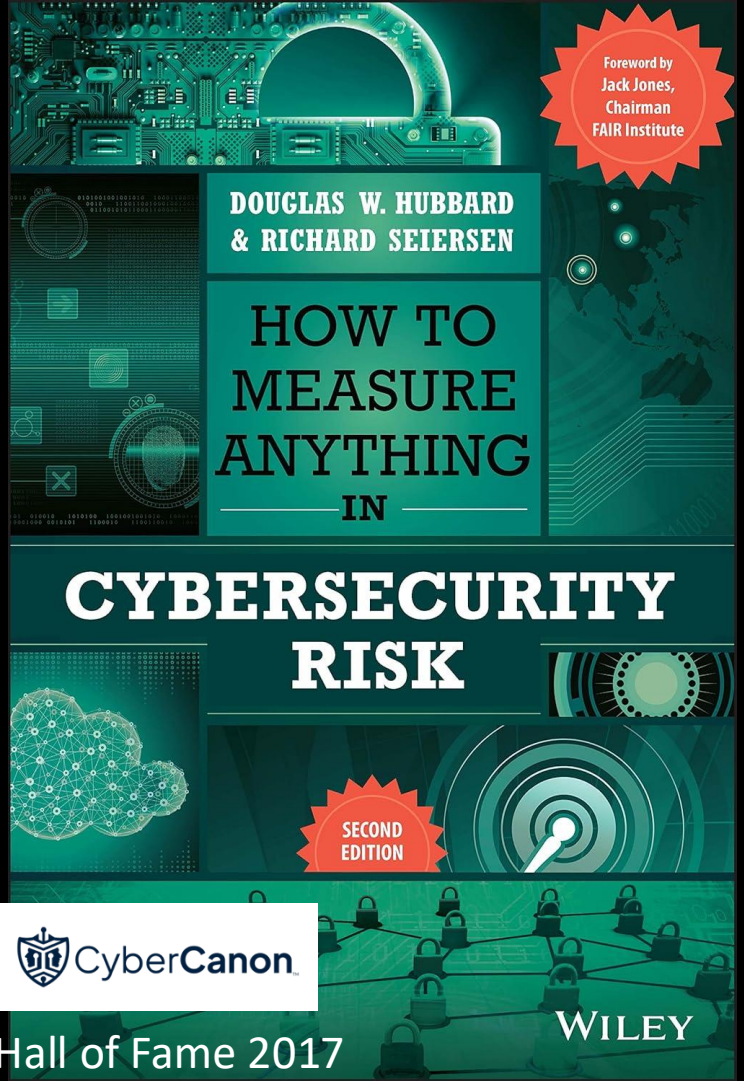
Not enough reactors, not enough service time for each

The Layered Implication

1. **Civil engineering**: Risk quantification works — stable physics, abundant data, no adversary
2. **Aviation**: Even with stable physics, safety depends on **institutional culture**, not just models (thus: doesn't apply to **nuclear reactors**)
3. **Cybersecurity**: All of aviation's modeling problems **plus** an adaptive adversary

⇒ We can't rely on risk models alone. We also need institutional infrastructure for learning (more later).

Part 3: Trying to Quantify Risk



CyberCanon

Hall of Fame 2017

6 Truths of Cyber Risk Quanti

philvenables.com/post/6-truths-of-cyber-risk-quantification

Ask Gemini

New Chrome available

RISK & CYBERSECURITY

Thoughts from the Field

HOME ABOUT EVENTS AND PUBLICATIONS

All Posts Leadership Risk Cybersecurity Technology

Phil Venables · Sep 7, 2024 · 8 min read

6 Truths of Cyber Risk Quantification

I wrote the original version of this post over 4 years ago. In revisiting this it is interesting to note that not much has actually advanced in the field. Yes, there have been more products and tools developed to apply FAIR or FAIR-like quantitative methods - some successful and some less so, usually indexed on the degree of effort it takes to set up the tooling to get more value out than you put in.

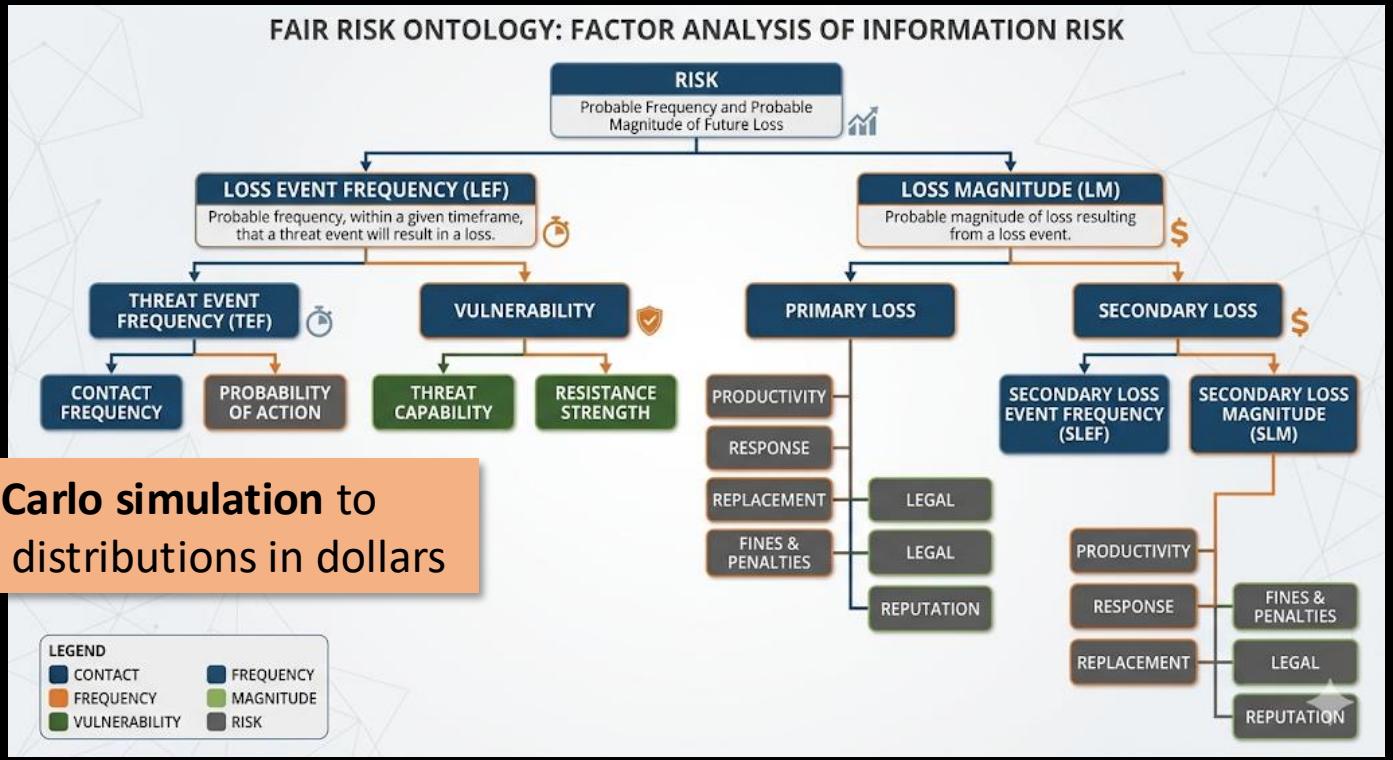
As with other areas of risk there's a Heisenberg-like quality to much of the approaches. That is the act of measuring often changes the situation, often positively. Although the *Breaking Bad* use of the term Heisenberg might also apply given the mix of confusion and euphoria that often results from excess use of risk quantification.

There have also been significant advances in the world of cyber-risk insurance particularly in insurers fine tuning their actuarial models, having more data available from the insured parties, and from industry sources like research teams, intelligence units and some cyber scoring services. Some cloud providers and cybersecurity companies have also partnered to stimulate capacity and provide risk-adjusted pricing.

But overall, I think there has been the most progress in the effective use of data, analytics

FAIR: The Prominent Quantitative Framework

Factor
Analysis
of
Information
Risk



Uses **Monte Carlo simulation** to produce loss distributions in dollars

https://www.fairinstitute.org/

FAIR: What's Sound, What's Missing

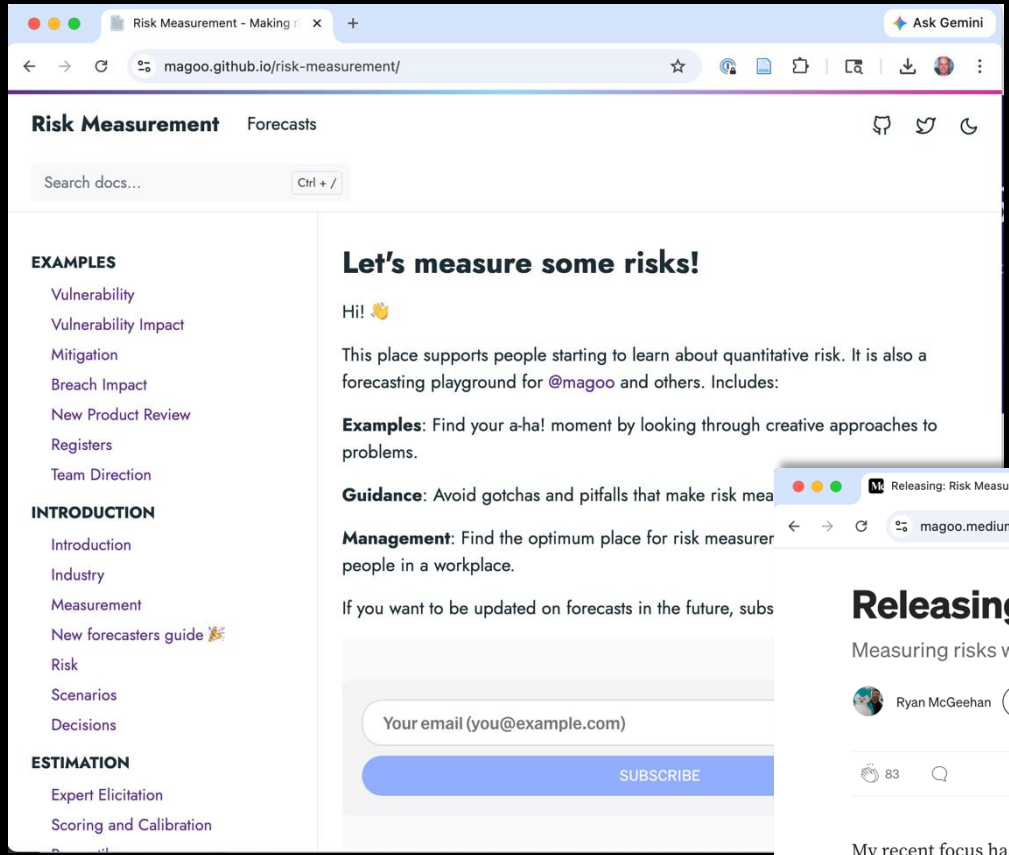
FAIR's **structure is sound**:

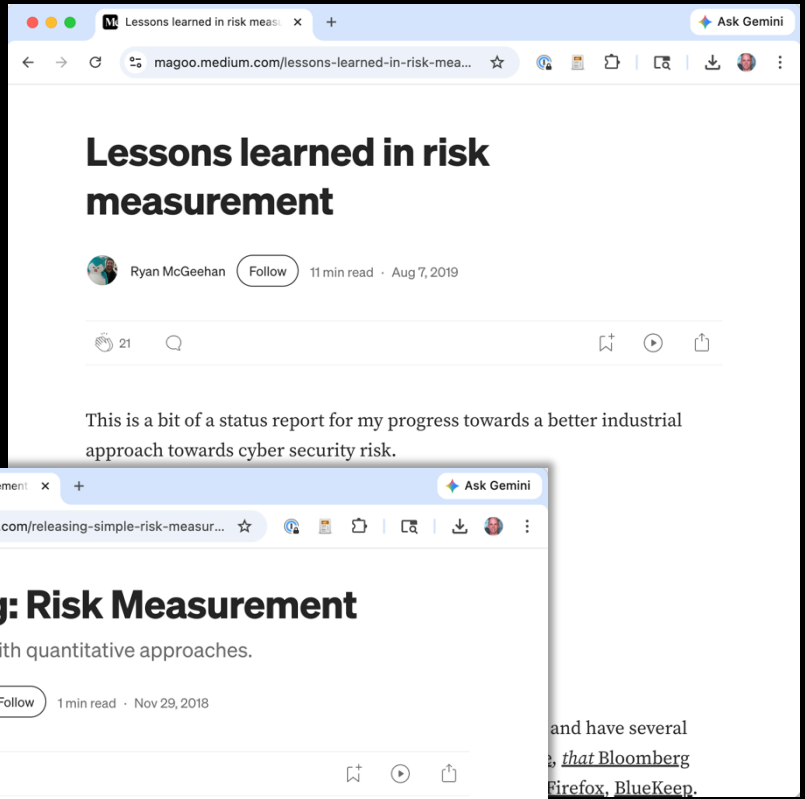
- Decompose risk into measurable sub-factors
- Express inputs as ranges (not point estimates)
- Aggregate via Monte Carlo to get loss distributions in dollars

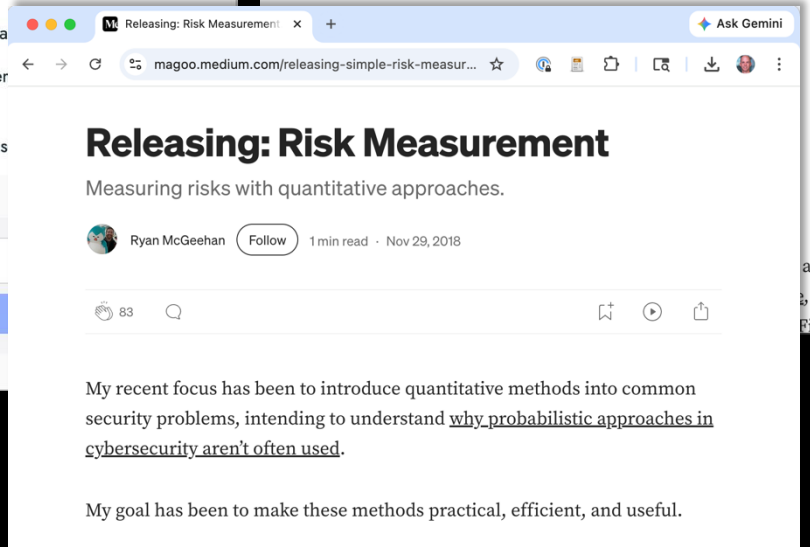
The real critique is about inputs, not structure:

- Hubbard: practitioners often feed FAIR uncalibrated gut estimates
- Venables: the hard problem is **communication and calibration**, not quantification itself — FAIR works when done well

What FAIR needs: a discipline for producing calibrated inputs.


Risk Measurement - Making
Ask Gemini
magoo.github.io/risk-measurement/
Risk Measurement
Forecasts
Search docs...
Ctrl + /
EXAMPLES
Vulnerability
Vulnerability Impact
Mitigation
Breach Impact
New Product Review
Registers
Team Direction
INTRODUCTION
Introduction
Industry
Measurement
New forecasters guide
Risk
Scenarios
Decisions
ESTIMATION
Expert Elicitation
Scoring and Calibration
Let's measure some risks!
Hi!
This place supports people starting to learn about quantitative risk. It is also a forecasting playground for @magoo and others. Includes:
Examples: Find your a-ha! moment by looking through creative approaches to problems.
Guidance: Avoid gotchas and pitfalls that make risk mea
Management: Find the optimum place for risk measurer
people in a workplace.
If you want to be updated on forecasts in the future, subs
Your email (you@example.com)
SUBSCRIBE


Lessons learned in risk meas
Ask Gemini
magoo.medium.com/lessons-learned-in-risk-mea...
Lessons learned in risk measurement
Ryan McGeehan
Follow
11 min read · Aug 7, 2019
21
This is a bit of a status report for my progress towards a better industrial approach towards cyber security risk.
and have several
, that Bloomberg
Firefox, BlueKeep.


Releasing: Risk Measurement
Ask Gemini
magoo.medium.com/releasing-simple-risk-measur...
Releasing: Risk Measurement
Measuring risks with quantitative approaches.
Ryan McGeehan
Follow
1 min read · Nov 29, 2018
83
My recent focus has been to introduce quantitative methods into common security problems, intending to understand why probabilistic approaches in cybersecurity aren't often used.
My goal has been to make these methods practical, efficient, and useful.

Forecasting: The Calibration Discipline FAIR Needs

Treat risk inputs as forecasts, not scores.

Instead of “ransomware = High risk,” commit to a specific falsifiable prediction:

> “A ransomware event causes >24h of downtime within the next 12 months”

Then attach:

- A **probability** (Brier-scored after the timeframe)
- Separately, a **cost interval** if it occurs (feeds FAIR/Gordon-Loeb)

Calibration is tracked **over many forecasts**, not one.

What Makes a Good Forecast?

A forecast is a **structured, scorable commitment** about a future event:

1. **Scenario**: An unambiguous statement of an undesirable future event, with a timeframe — the "impact" is built into the scenario itself (downtime, disclosure, lawsuit, etc.)
2. **Probability**: Your stated confidence the scenario will occur
3. **Scoring plan**: Judge the outcome after the timeframe using a Brier score (0-1, lower is better):

$$\text{Brier} = (\text{forecast} - \text{outcome})^2$$

Scoping note: Dollar costs and investment decisions come *afterwards*, when we act on forecasts we're confident in.

Let’s Try It: Writing a Scenario (Step 1)

Bad scenario: “Ransomware hits our company” ← vague, no timeframe, no defined outcome

Good scenario:

> *Our mid-sized SaaS company (~$50M revenue, ~200 employees) publicly discloses a ransomware incident that causes >24 hours of service downtime within the next 12 months.*

- **Unambiguous event**: clear trigger (public disclosure + >24h downtime)
- **Timeframe**: next 12 months
- **Judgment**: Did we file a public disclosure? Was downtime >24h?

Step 2: Commit to a Probability

Before I show you any data:

Write down your estimate. What probability do you assign to this scenario?

This is your **forecast**. Own it.

SOPHOS

THE STATE OF RANSOMWARE 2025

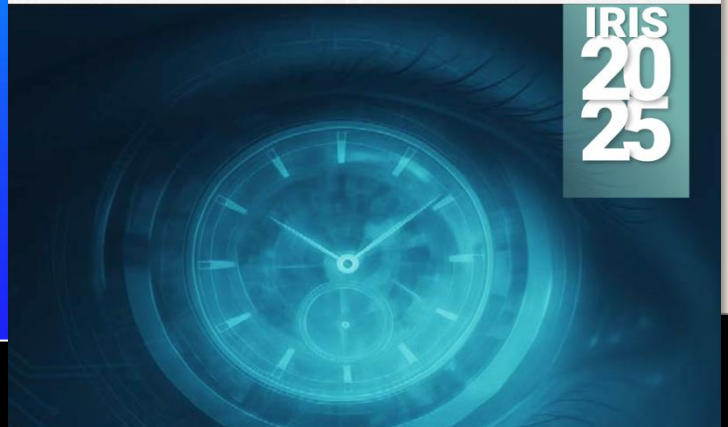
Findings from an independent survey of 3,400 IT and cybersecurity leaders across 17 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. June 2025

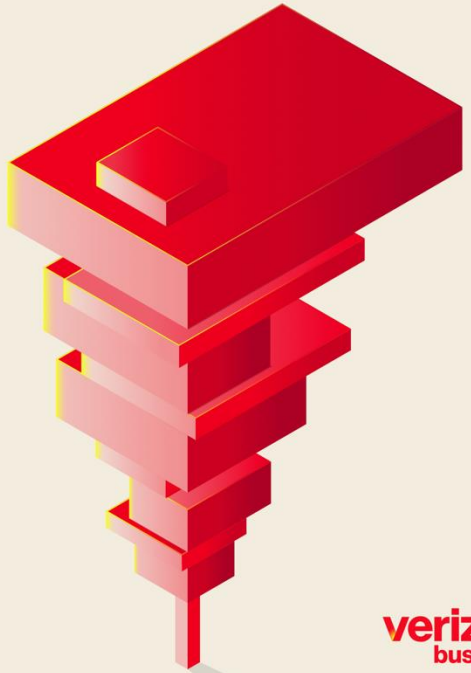
Cyentia INSTITUTE

Information Risk Insights Study

It's About Time



2025 Data Breach Investigations Report



verizon business

Coalition

2025 Cyber Claims Report

An in-depth look at cyber claims data and the state of Active Insurance

NetDiligence

CYBER CLAIMS STUDY

2025 REPORT

CONSTANGY Brooks Smith & Prophete · experian · RSM · SUREFIRE CYBER

What the Data Says: Probability

Now let's calibrate your probability estimate against available data:

- **Coalition 2025**: Ransomware claims frequency = **0.31%** of policyholders (industry avg ~4x higher → ~1.1%)
- **Cyentia IRIS 2025**: Overall incident probability ~9.3%; ransomware is ~30% of incidents → ~3%
- **Verizon DBIR 2025**: Ransomware in 44% of *confirmed breaches*; 88% among SMBs — but this is composition, **not** probability

Triangulating: roughly **1–5%** for a mid-sized firm per year

Step 3: Score It

$$\text{Brier} = (\text{forecast} - \text{outcome})^2$$

After 12 months, check: did the scenario occur?

Your forecast	Outcome	Brier score
3%	Did not occur (0)	$(0.03 - 0)^2 = 0.0009$
3%	Occurred (1)	$(0.03 - 1)^2 = 0.9409$
30%	Did not occur (0)	$(0.30 - 0)^2 = 0.0900$

A single Brier score tells you little. Over **many** forecasts, your average Brier score reveals **calibration**: are your probabilities trustworthy?

Now What?

We have a forecast:

> **~3% probability** that a ransomware incident causes >24h downtime and public disclosure in the next 12 months.

The CISO's next questions:

1. *If it happens, what would it cost us?*
2. *What should we do to mitigate this risk?*

What Would It Cost? (If It Occurs)

Don’t estimate a single cost. Estimate a **range**:

> *“I’m 90% confident that if this scenario occurs, our total direct losses will fall between $___ and $___.”*

Direct losses = downtime revenue loss + forensics + legal + ransom (if paid) + notification

Write down your 90% confidence interval.

What the Data Says: Cost

Source	What it measures	Amount
Coalition 2025	Avg insurance claim (ransomware)	$292K
Sophos 2025	Avg recovery cost (survey, excl. ransom)	$1.53M
Sophos 2025	Avg recovery, 100–250 employees	$639K
Coalition 2025	Avg business interruption loss	$102K
Coalition 2025	Avg forensic vendor cost	$58K
DBIR 2025	Median ransom payment (if paid)	$115K
Sophos 2025	Median ransom payment (if paid)	$1M

A reasonable **90% CI** for our scenario: **$50K – $3M**

So: Expected Annual Loss?

With probability p and a 90% CI on cost $[L, H]$: Either

1. Use **Monte Carlo simulation** (FAIR) to estimate losses, or
2. Use the **geometric mean** for right-skewed distributions:

$$\text{Central cost} = \sqrt{L \times H} = \sqrt{\$50\text{K} \times \$3\text{M}} \approx \$387\text{K}$$

Annualized expected loss $= p \times$ central cost $= 3\% \times \$387\text{K} \approx \$12\text{K}$

Tail-weighted (95th percentile of cost): $3\% \times \$3\text{M} = \$90\text{K}$ annualized

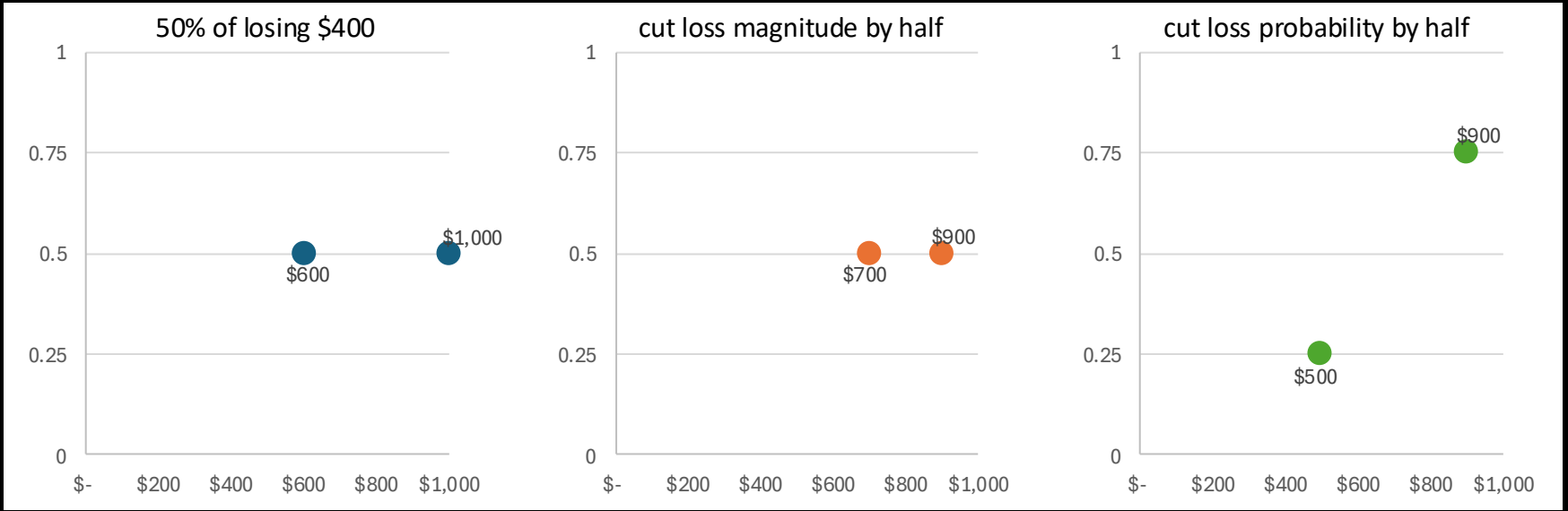
How Should We Mitigate the Risk?

- “Risk = Likelihood * Impact” is a lie. Pick one:
  - 1/10,000 chance of losing $100,000 or 1/1 chance of losing $10
    - … $20?
    - … $100?
    - … $1,000?
- **Risk is a distribution**, not a point. Risk management is the practice of shaping that distribution
  - **Reducing likelihood by 10x** has a different effect on the distribution than **reducing impact by 10x**
- Cost of risk mitigation must be explicit

Shaping risk distribution

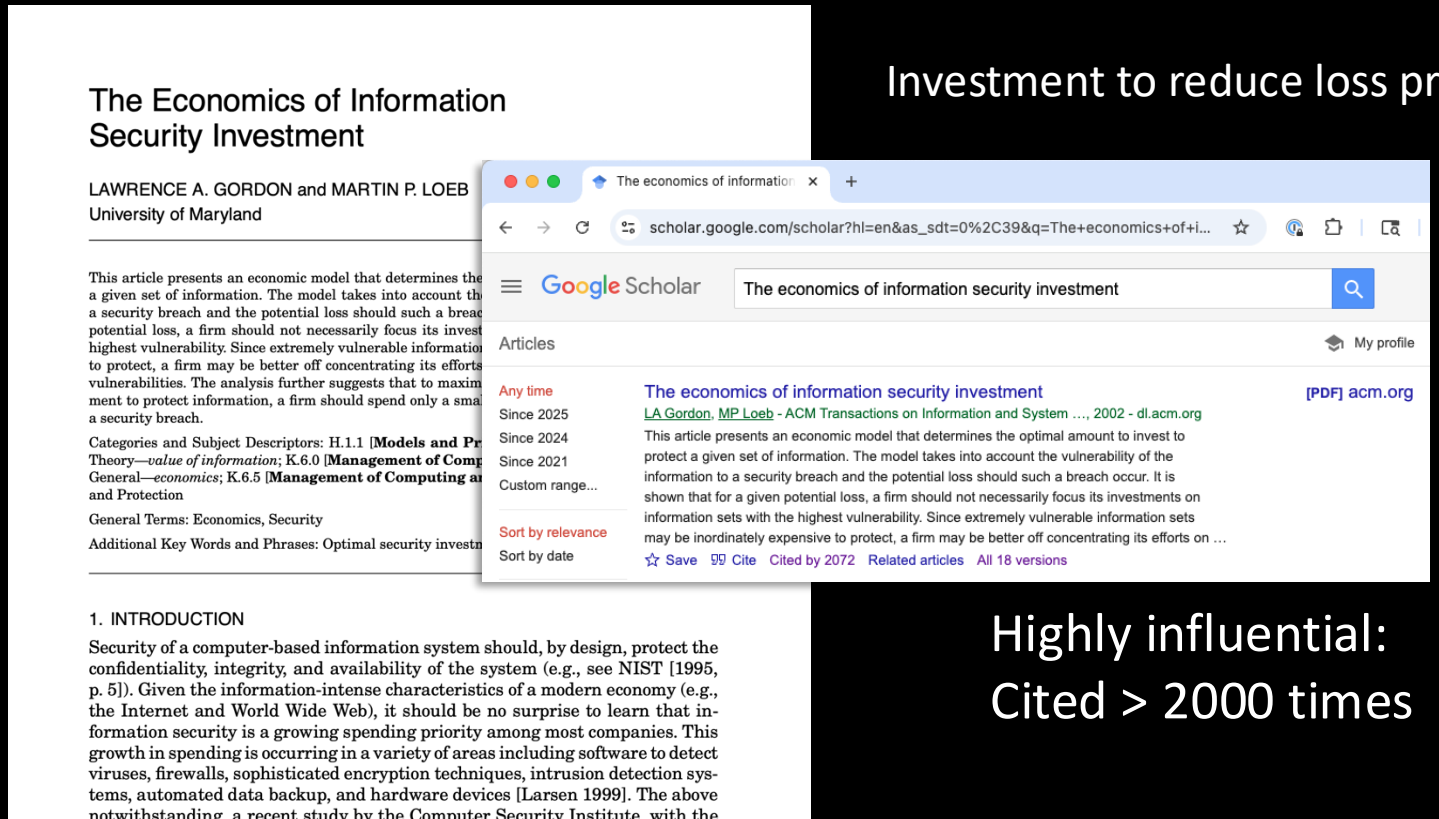
Starting with $1,000 …

… option to spend $100 to:



Mean final wealth is $800 in all three scenarios

Framing the Problem: Security as Investment



The Economics of Information Security Investment

LAWRENCE A. GORDON and MARTIN P. LOEB
University of Maryland

This article presents an economic model that determines the
a given set of information. The model takes into account th
a security breach and the potential loss should such a breac
potential loss, a firm should not necessarily focus its invest
highest vulnerability. Since extremely vulnerable informatio
to protect, a firm may be better off concentrating its efforts
vulnerabilities. The analysis further suggests that to maxim
ment to protect information, a firm should spend only a sma
a security breach.

Categories and Subject Descriptors: H.1.1 [**Models and Pr**
Theory—*value of information*; K.6.0 [**Management of Comp**
General—*economics*; K.6.5 [**Management of Computing a**
and Protection

General Terms: Economics, Security

Additional Key Words and Phrases: Optimal security investn

1. INTRODUCTION

Security of a computer-based information system should, by design, protect the confidentiality, integrity, and availability of the system (e.g., see NIST [1995, p. 5]). Given the information-intense characteristics of a modern economy (e.g., the Internet and World Wide Web), it should be no surprise to learn that information security is a growing spending priority among most companies. This growth in spending is occurring in a variety of areas including software to detect viruses, firewalls, sophisticated encryption techniques, intrusion detection systems, automated data backup, and hardware devices [Larsen 1999]. The above notwithstanding, a recent study by the Computer Security Institute, with the

Investment to reduce loss probability

Highly influential:
Cited > 2000 times

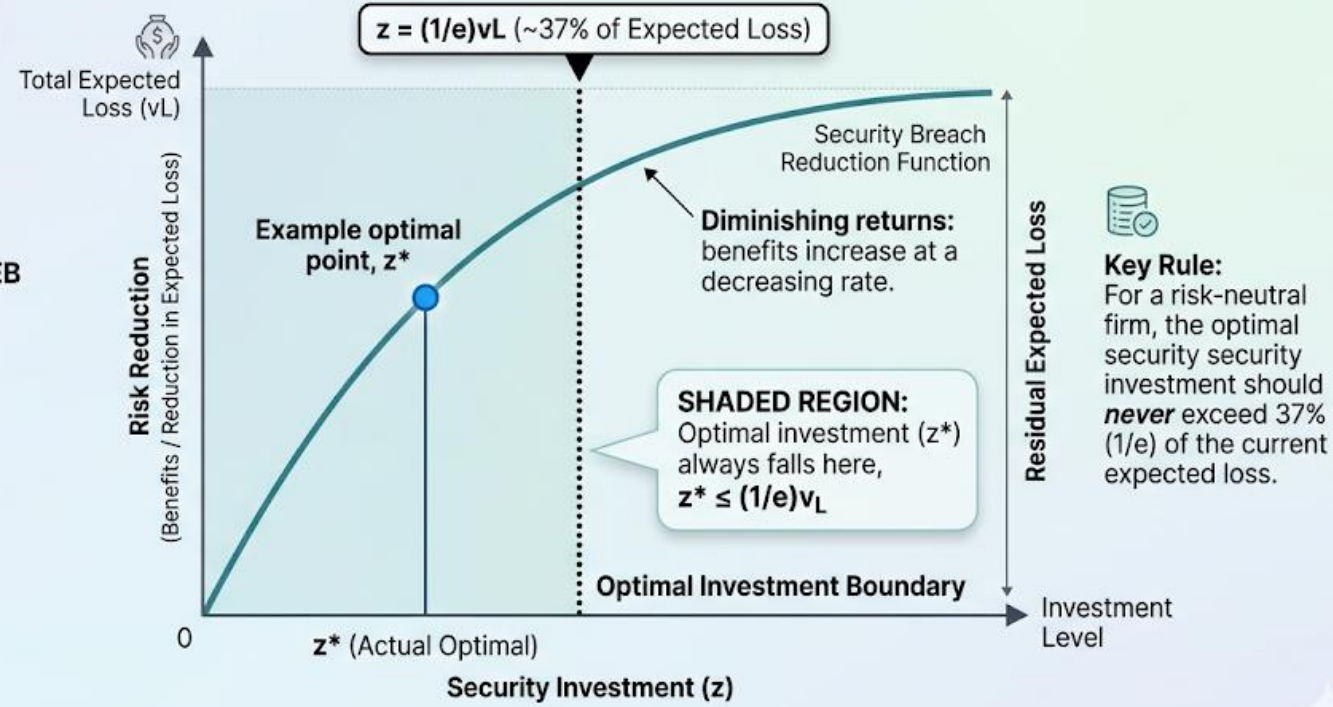
Cited Takeaway From This Paper

- it's often not worth investing heavily to protect highly vulnerable information sets, because the marginal returns to reducing an already-high vulnerability diminish quickly.

- The **optimal investment amount** z* could be **well below** the **expected loss** vL
  - Theorem: If the breach probability function S(z,v) is either of class I or class II, then $z* < (1/e)\ vL = .3679vL$
  - For class I, there are scenarios where $z* < .25vL$

THE GORDON-LOEB CURVE: OPTIMAL INVESTMENT & THE 1/e RULE

GORDON-LOEB MODEL:
Economical framework for optimal cybersecurity spending.



Key Rule:
For a risk-neutral firm, the optimal security security investment should ***never*** exceed 37% (1/e) of the current expected loss.

The 1/e rule is derived from general classes of security functions, emphasizing efficiency over complete elimination of risk.

The Investment Question: Defense

If we believe **Gordon-Loeb**: invest at most 37% of expected loss

Using the tail-weighted estimate ($90K):

$$37\% \times \$90\text{K} =\sim \$33\text{K/year}$$

Does that match what your company spends on:

- Endpoint detection?
- Backup testing?
- Incident response retainer?

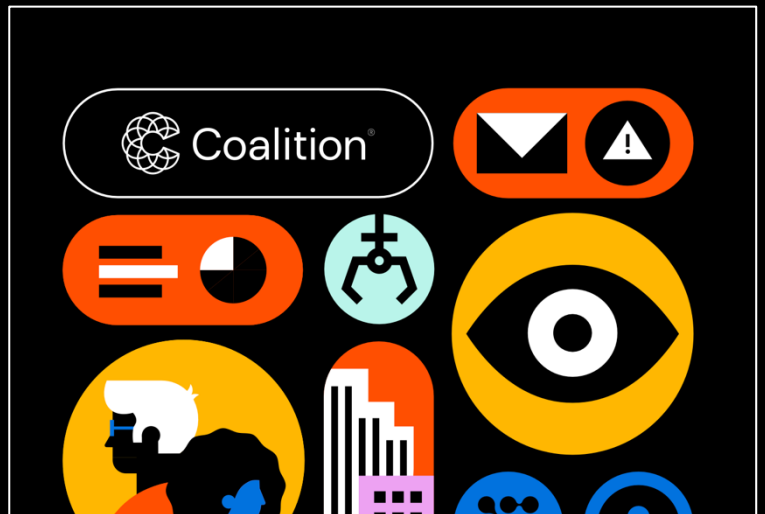
Are you over- or under-investing?

The Investment Question: Insurance?

Cyber insurance addresses the other part of risk: Reducing the impact

This affects the other part of the risk distribution

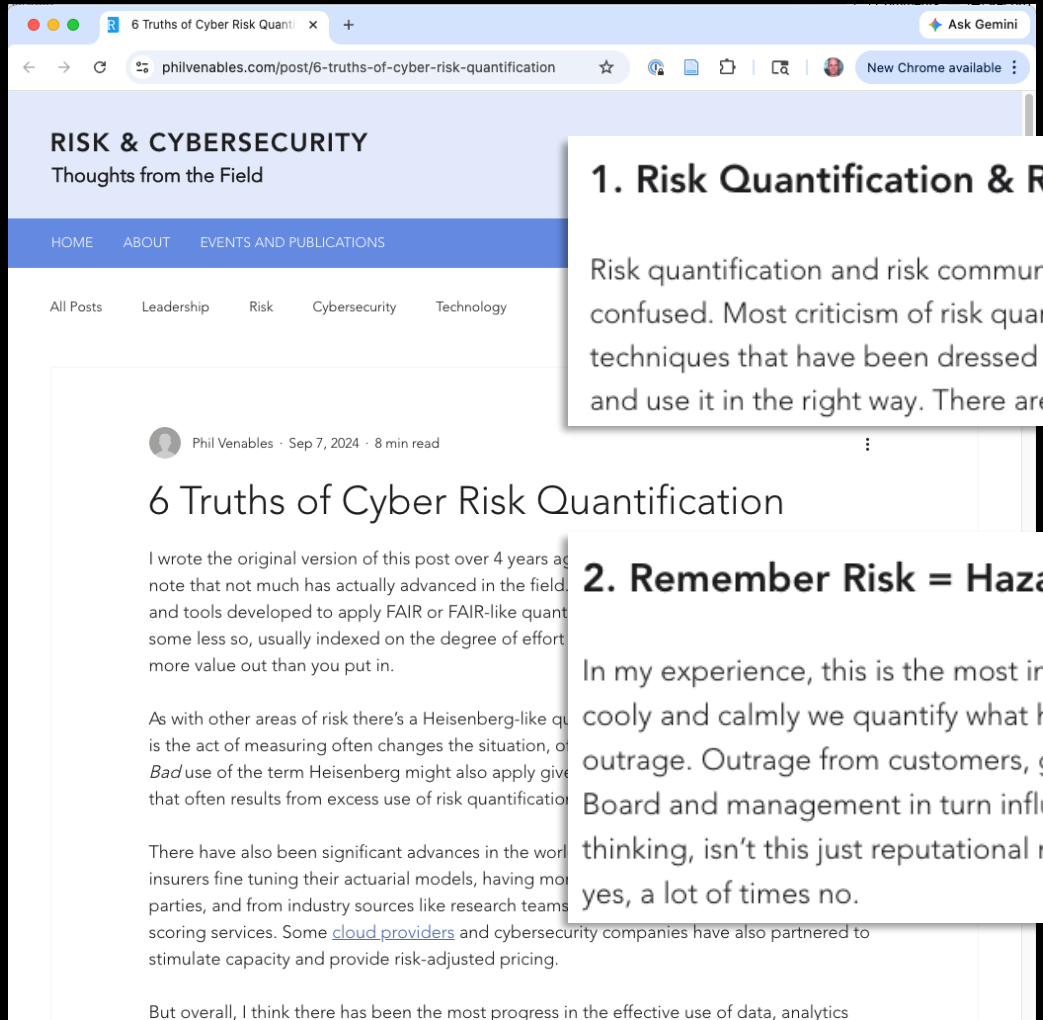
You (probably) want both



Why This Is Hard

- **Nobody wants to commit to numbers** — executives push back on probabilities
- Teams **argue about estimates** — but that’s the point! It surfaces hidden disagreements
- **Risk registers become compliance artifacts** — quantitative models used to justify decisions already made

Part 4: Communicating Risk



1. Risk Quantification & Risk Communication - Big Difference

Risk quantification and risk communication are two different disciplines but they're often confused. Most criticism of risk quantification is actually criticism of risk communication techniques that have been dressed up or misinterpreted as risk quantification. Pick your tool and use it in the right way. There are a variety of quantification mechanisms ranging from

2. Remember Risk = Hazard + Outrage

In my experience, this is the most important equation in risk management. No matter how cooly and calmly we quantify what hazard we are subject to it can still be overwhelmed by outrage. Outrage from customers, governments, regulators, media, auditors and one's own Board and management in turn influenced by that external outrage. You may well be thinking, isn't this just reputational risk that should be included in the hazard. Sometimes, yes, a lot of times no.

What CISOs Present to Boards

Surveyed Fortune 1000 CISOs on their actual board updates

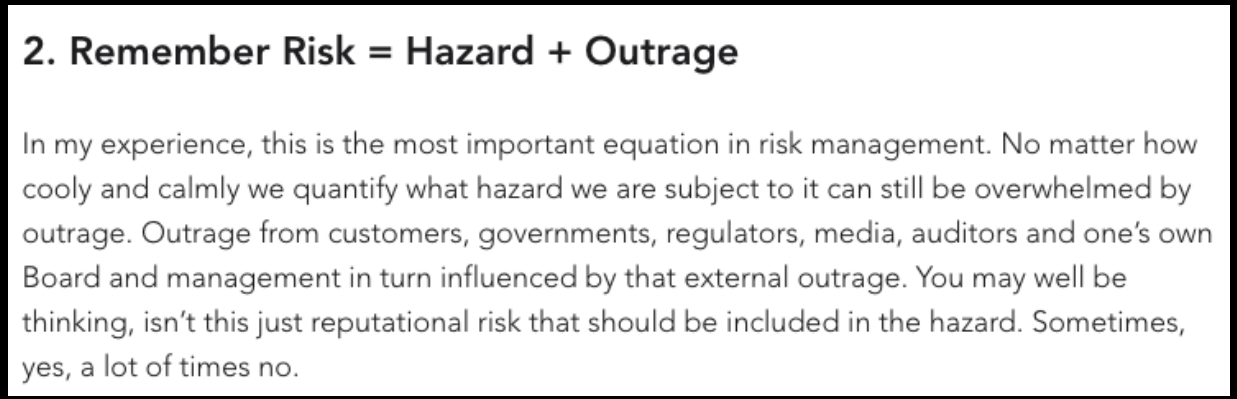
All include:

- Changes to the **risk landscape**
- **Maturity scores**
- **Security initiatives** progress
- **Significant incidents**

Why They Present This Way: Hazard + Outrage

Boards respond to **outrage**, not expected value

A $300K ransomware incident that makes the news is “worse” than a $3M BEC loss nobody hears about



2. Remember Risk = Hazard + Outrage

In my experience, this is the most important equation in risk management. No matter how cooly and calmly we quantify what hazard we are subject to it can still be overwhelmed by outrage. Outrage from customers, governments, regulators, media, auditors and one’s own Board and management in turn influenced by that external outrage. You may well be thinking, isn’t this just reputational risk that should be included in the hazard. Sometimes, yes, a lot of times no.

What CISOs *Don't* Present: Dollar Estimates

> "The board updates in our sample did not present cyber risks quantified in financial terms"

— RSAC ESAF Report, p. 9

But wait — is the board presentation the whole story?

The Nuance: Communication vs. Analysis

Some organizations do quantitative work internally:

> "Security teams use risk scoring systems internally to prioritize their efforts but **do not find it useful to share those numbers** with the board" (p. 8)
>
> CISOs "do a detailed assessment each year on a severe-but-plausible risk scenario and **quantify the financial losses**… primarily for insurance purposes" (p. 9)

But many haven't built the capability at all:

> "Most CISOs who have evaluated building a capability to quantify cyber risk in dollar values found that the **resources required would be prohibitive**" (p. 9)

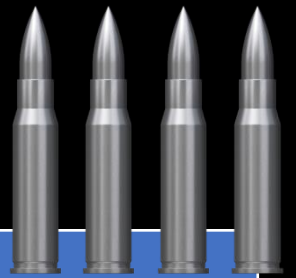
What Boards Actually Want to Know

- Is the risk landscape being **monitored**?
- Are risks being **analyzed and prioritized**?
- Is risk appetite being **factored in**?
- Is the CISO providing adequate **oversight**?

The board's primary concern: **legal defensibility**

> "Board members need to be able to show that they were adequately overseeing cyber risk management"

The Silver Bullets Connection



What boards see	What it measures	The worry
Risk heatmaps	Cox: broken by construction	Is there real analysis underneath?
Maturity scores	Process, not outcomes	Or is the heatmap *all there is*?
Compliance status	Checkbox, not efficacy	
Security initiatives	Activity, not risk reduction	

Simplifying for boards is fine — if there's rigorous analysis underneath

Grigg's silver bullets: the danger is when signaling *replaces* analysis, not just *simplifies* it

Discussion

Given everything we've discussed:

- The **data problems**
- The **practitioner reality** (social, not technical)
- The **competing pressures** (compliance, signaling, cost)
- The **missing institutional infrastructure**

Is quantitative cyber risk assessment genuinely achievable, or is it another "silver bullet"?

Three Mechanisms, Three Limitations

Mechanism	Promise	Limitation
Risk models	Rational investment	Data problems, no stable physics
Regulation	Minimum standards	Compliance ≠ security
Insurance	Markets price risk	Same data limitations

Next lecture: **Regulation and Compliance** — do mandates help?

Guest lecture (Apr 23): **Cyber Insurance** — can markets price what regulators can’t measure?

Readings for This Lecture

Required:

- Downer, “The Aviation Paradox,” *Minerva* 2017
- Romanosky, “Examining the Costs and Causes of Cyber Incidents,” *J. Cybersecurity* 2016

Optional:

- Hubbard & Seiersen, *How to Measure Anything in Cybersecurity Risk*, 2nd ed. 2023 (esp. Chapters 5, 6, 9, 12)
- Cox, “What’s Wrong with Risk Matrices?”, *Risk Analysis* 2008
- Cyentia Institute, IRIS 2025: *It’s About Time* (papers/IRIS-2025.pdf)
- Knake, Shostack & Wheeler, “Learning from Cyber Incidents,” Belfer Center 2021

All References

Risk quantification:

- Woods & Böhme, “SoK: Quantifying Cyber Risk,” IEEE S&P 2021
- Woods, “Reviewing Estimates of Cybercrime Victimisation,” 2022
- Gordon & Loeb, “Economics of Information Security Investment,” 2002
- Grove & Meehl, “Comparative Efficiency of Prediction Procedures,” 1996
- Cox, “What’s Wrong with Risk Matrices?”, 2008

Frameworks & practice:

- NIST CSF 2.0 (2024)
- OWASP Risk Rating Methodology
- McGeehan, Simple Risk Measurement (magoo.github.io/risk-measurement)
- Venables, “6 Truths of Cyber Risk Quantification,” 2024
- Venables, “Risk = Hazard + Outrage,” 2021

Loss data:

- FBI IC3 Annual Report 2024
- NetDiligence Cyber Claims Study 2025
- Coalition 2025 Cyber Claims Report
- Cyentia IRIS 2025: *It’s About Time*
- Verizon DBIR 2025
- Romanosky, “Costs and Causes of Cyber Incidents,” 2016
- IBM/Ponemon Cost of a Data Breach 2025

Safety & institutional learning:

- Downer, “The Aviation Paradox,” 2017
- Knake, Shostack & Wheeler, “Learning from Cyber Incidents,” 2021
- RSAC ESAF, “What Top CISOs Include in Updates for the Board,” 2022
- Hubbard & Seiersen, *How to Measure Anything in Cybersecurity Risk*, 2nd ed. 2023