



Breaking Out of Optimised Failure

Is There a Case for a Post-Risk Cyber World?

Who am I

Head of Information Security - Numan

Fractional Head of Product - DevArmor

OWASP Project Contributor CycloneDX TM-BOM

OWASP Project Co-Leader Threat Model Library

*LF AI -Data Security and Compliance - Threat Model Use Cases
Workgroup Co-chair*

Technology, Machine learning and AI enthusiast

Public speaker - OWASP Global AppSec, Teiss, Podcast guest...

Inventor (0 day malware detection patent)

Threat Modeling enthusiast

Competitive athlete / volleyball player



This Is a Thought Exercise, Not a Manifesto

What This Session Is NOT Saying

- Risk management is pointless

What This Session IS Proposing

- Critical examination of the risk centric approach in cyber

- We should stop all our current practices

- Questioning some foundational assumptions
- Exploration of alternatives
- Assessment of outcomes vs theoretical benefits

The Uncomfortable ~~Year~~ Decade ?

M&S

Jaguar

Airport Attacks

Supply Chain Attacks

Mythos

The Oversight Illusion

2X Incident Growth

-NCSC Annual Review

The Existential Crisis Moment

Last year at OWASP Global AppSec, a cyber security thought leader, practitioner, expert - Adam Shostack challenged us all to stop managing risk.



The Evolution of Cyber Risk Management

1974

1993–1995

2002

2005

FIPS PUB 31 explicitly links computer security with "risk management."

UK DTI/BSI Code of Practice (BS 7799) forms the foundation for later ISO standards.

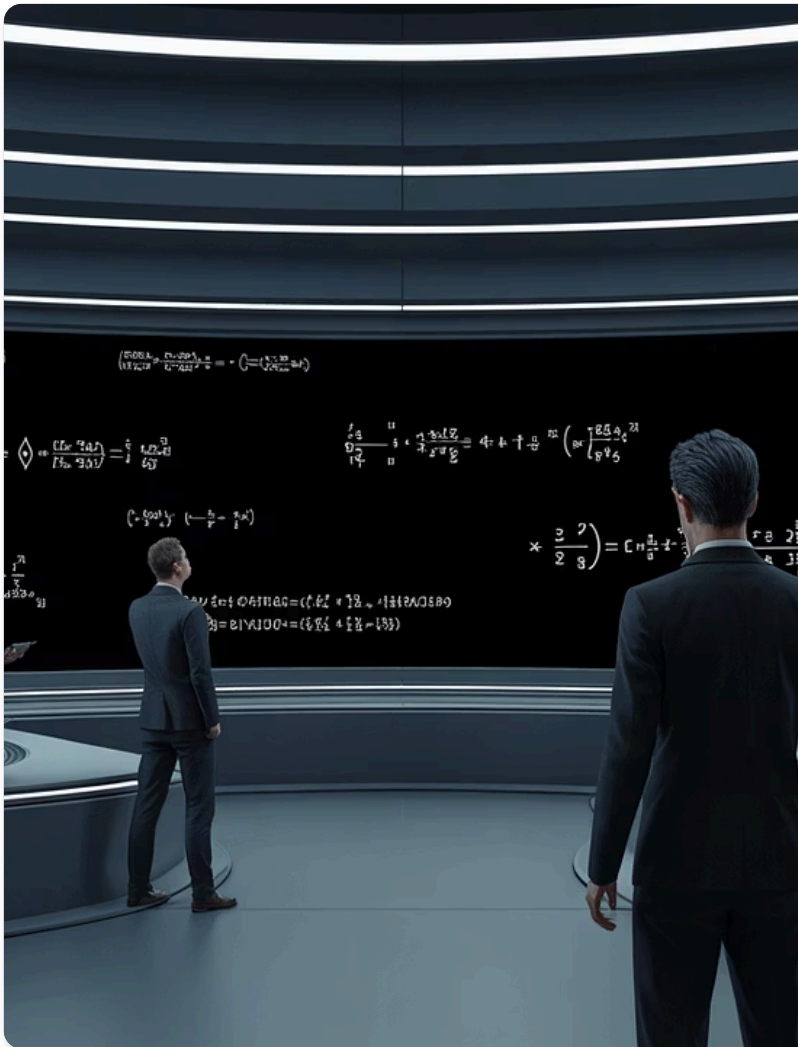
FISMA passed, and NIST SP 800-30 publishes a formal "risk management guide" for IT systems.

ISO/IEC 27001 first published, introducing a risk-based Information Security Management System (ISMS).



Vibe Check





ERM Language, Not ERM Maths

ERM Concepts

We adopted ERM concepts (appetite, registers, residual risk) for organisational governance and spending decisions.

Cyber Risk is not like Financial Risk!

Cybersecurity is adversarial and non-stationary; systems and threats evolve faster than data can stabilise for true quantification.

"Casino Math"

Many "risk numbers" are structured judgement, not calibrated measurement, leading to rigorous-looking but unreliable simulations (Brook Schoenfeld).

The Practical Challenges Undermining Cyber Risk Management



Data That Doesn't Drive Action



Business Buy-In



Lack of Real-World Data



Computationally Expensive Modelling

The Prioritisation Game





ERM cyber risks aren't judged in isolation. They compete against a wide array of categories like technology, commercial, clinical, and operational.

- more tangible impacts of other risk categories:
 - commercial risks are derived directly from revenue and have direct business impact
 - clinical and safety carry regulatory and moral weights
 - cyber risks are often abstract, probabilistic, and hard to quantify.
- lack of data driven quantification across the board



Why are we so bad at managing risk?

*Because humans don't "calculate" risk - we **feel** it.*

- **We remember stories, not base rates** (Tversky & Kahneman)
- **Emotion overrides probability** (Slovic; Sunstein)
- **Metrics get gamed** (Campbell / Goodhart "measure → target")

Industry opinions?

Ross Young

former CIA officer; former enterprise CISO (Caterpillar Financial); CISO in Residence at Team8; co-host of CISO Tradecraft

Skepticism towards cyber risk quantification as it's practiced today - he recommends we should make security decisions with scenario evidence, and optimise for outcomes per pound spent.

Adam Shostack

threat modeling expert; author of Threat Modeling: Designing for Security; nearly a decade at Microsoft working on threat modeling in the SDL;

Adam wants us to stop managing risk altogether "Risk management... has been given... an axiomatic truth. It doesn't deserve it."

Bruce Schneier

security technologist and author; longtime commentator on security economics and risk

The problem in the security world is we often lack the data to do risk management well.

Industry opinions?

Shannon Lantzy, Ph.D., PMP

Medtech thought leader, ex-Booz Allen Chief Scientist

Shannon says we should kill the risk matrix.

"Not because risk assessment is wrong. But because the way we're using risk matrices in health tech is quietly distorting decisions."

What Would a Post-Risk World Look Like?



"We do not anticipate the world with our dogmas but instead attempt to discover the new world through the critique of the old."

Author

Karl Marx

Vibe Check



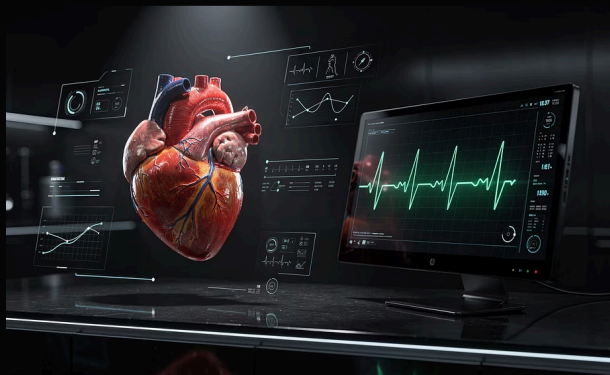
The 25% Rule

“A sufficiently large committed minority can trigger a tipping point in social convention.” - *Centola et al., Science (2018)*

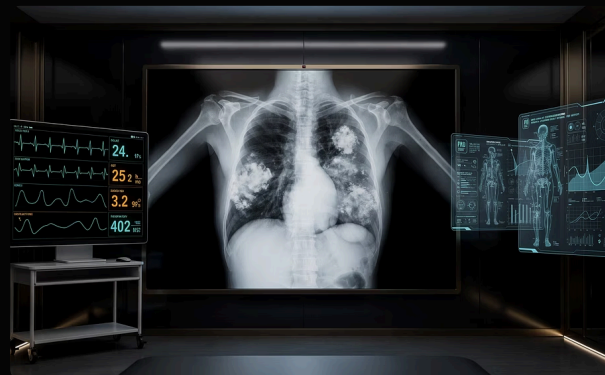


How to enable decision-making and prioritisation then?

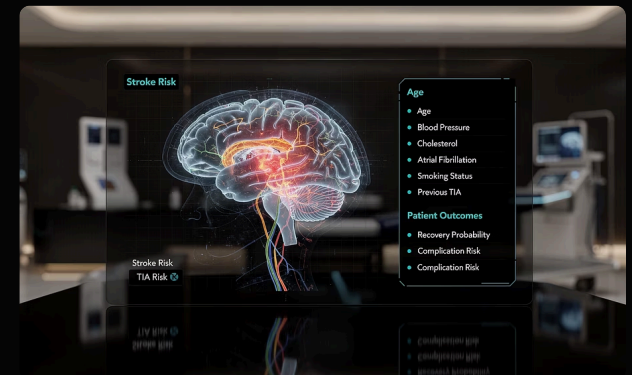
A Medical Perspective: Evidence based approach



HEART Score



CURB-65 Score



ABCD² Score

Quantifies risk of major adverse cardiac events in chest pain patients.

Based on statistical prediction from real-world data, considering EKG, age, and other risk factors.

Assesses pneumonia severity and mortality risk.

Factors include Confusion, Urea, Respiratory rate, Blood pressure, and Age over 65, derived from extensive population studies.

Predicts stroke risk after a transient ischemic attack (TIA).

Evaluates Age, Blood pressure, Clinical features, Duration of TIA symptoms, and Diabetes, based on statistical analysis of patient outcomes.



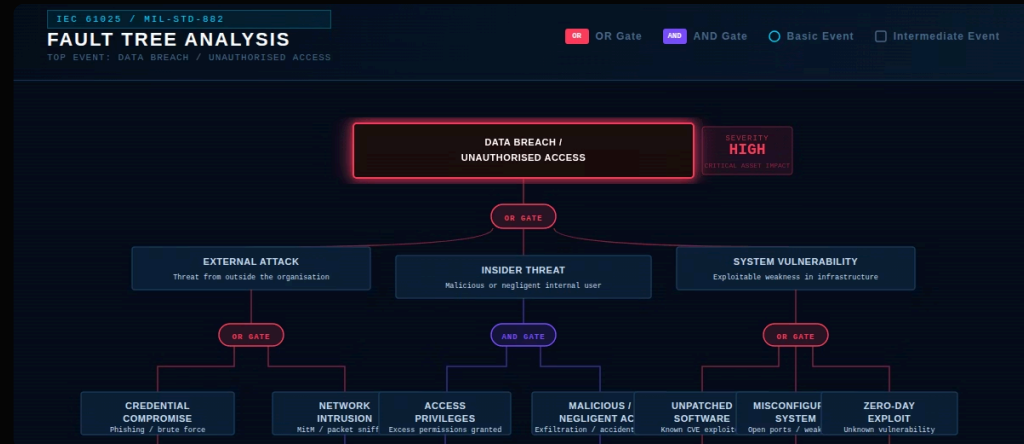
The above comes from year of research and abundance of data - is what we are doing just pseudoscience?

Or is the lack of data a solvable problem we should focus on?



Safety Engineering

- Cyber incidents are chains of small failures




“The primary objective of risk management is accident prevention ... achieved by proactively identifying, assessing, and eliminating or mitigating ... hazards.”

— FAA, *Aviation Instructor's Handbook*

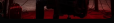
Other Considerations...





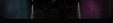
Chaos Engineering

Instead of relying on theoretical attacks for prioritisation, focusing on continuously breaking systems to test resilience



Threat-Centric Approaches

By creating threat models and attack trees we can try to identify key controls to focus on (what are we building, what can go wrong, what will we do about it)



Early warning scores → key risk indicators

Medicine tracks vital signs and uses early warning scores to trigger action early.

Cyber equivalent: a small set of Key Risk Indicators (KRIs) that are:

leading (they move before incidents),

objective (measured from systems of record),

actionable (each has a predefined response),

trend-based (direction matters more than a one-off number).



FAIR

FAIR (Factor Analysis of Information Risk) is an international standard for quantifying cyber risk in financial terms - giving organisations a consistent, defensible framework for measuring and communicating risk.

*If our cyber risk approach isn't delivering,
do we have the **courage to reimagine it** —
or will we keep optimising **a failing
system?***

We should either
define acceptable methods —
or, à la Adam, **let's stop pretending.**

// AUTHOR

**Brook
Schoenfield**

Former CISO
Security-Architecture Leader
Securing Systems
Secrets of a Cyber Security Architect

Your Challenge: Return and Reassess

1

Question Your Core Risk Centric Assumptions

2

Let's work together as an industry and share / publish more data!

3

Explore Alternative Approaches

4

Have the Difficult Conversation



Questions

References

Campbell, Donald T. 1979. "Assessing the Impact of Planned Social Change." *Evaluation and Program Planning* 2 (1): 67–90.

[https://doi.org/10.1016/0149-7189\(79\)90048-X](https://doi.org/10.1016/0149-7189(79)90048-X).

Rozenblit, Leonid, and Frank Keil. 2002. "The Misunderstood Limits of Folk Science: An Illusion of Explanatory Depth." *Cognitive Science* 26 (5): 521–562.

Slovic, Paul, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor. 2004. "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality." *Risk Analysis* 24 (2): 311–322. <https://doi.org/10.1111/j.0272-4332.2004.00433.x>.

Sunstein, Cass R. 2002. "Probability Neglect: Emotions, Worst Cases, and Law." *Yale Law Journal* 112: 61–107.

Tversky, Amos, and Daniel Kahneman. 1973. "Availability: A Heuristic for Judging Frequency and Probability." *Cognitive Psychology* 5: 207–232.

Goodhart, Charles A. E. 1975. "Problems of Monetary Management: The UK Experience." In *Papers in Monetary Economics*, Vol. 1. Sydney: Reserve Bank of Australia.

Marx, Karl. 1843. "Letter to Arnold Ruge" (Kreuznach, September 1843). In *Marx-Engels Collected Works*, vol. 3. Online version at Marxists Internet Archive. Accessed February 8, 2026.

U.S. Department of Transportation, Federal Aviation Administration. 2020. *Aviation Instructor's Handbook (FAA-H-8083-9B)*, chap. 1, "Risk Management and Single-Pilot Resource Management." Washington, DC. Accessed February 8, 2026.

Centola, Damon, Robb Willer, and Michael Macy. 2018. "Experimental Evidence for Tipping Points in Social Convention." *Science* 360 (6393): 1116–1119. <https://doi.org/10.1126/science.aas8827>.