ACRQ

vs

VaR

| The “FAIR” Model

A revolution in cyber risk management

VaR

Value at Risk | The”FAIR” Model

Let's start by explaining what VaR is to understand why it shouldn’t be used in cyber risk management.

Value at Risk (VaR) measures the risk of loss of investment/capital. It estimates how much a set of investments might lose (with a given probability), given normal market conditions, in a set time period such as a day.

VaR is typically used by firms and regulators in the financial industry to gauge the amount of assets needed to cover possible losses.

It’s not FAIR to use VaR in cyber. Here’s why!

VaR

Value at Risk | The"FAIR" Model

To simplify this understanding,
Nassim Nicholas Taleb speaks against VaR on:

the reliability of VaR models:
"The problem with the VAR is that it tries to estimate something that is not scientifically possible, namely the maximum loss over a fixed horizon, with a given confidence interval, usually 95% or 99%."

Nassim Nicholas Taleb is a Lebanese-American essayist, mathematical statistician, former option trader, risk analyst, and aphorist. His work concerns problems of randomness, probability, and uncertainty.
Taleb is the author of The Incerto, a five-volume philosophical essay on uncertainty published between 2001 and 2018 (notably, The Black Swan and Antifragile). He has been a professor at several universities, serving as a Distinguished Professor of Risk Engineering at the New York University Tandon School of Engineering since September 2008. Learn more>

It's not FAIR to use VaR in cyber. Here's why!

VaR

Value at Risk | The”FAIR” Model

Nassim Nicholas Taleb on:

the limitations of VaR: “Value-at-Risk is charlatanism. It assumes that we know what volatility is, but the distribution of extreme events cannot be predicted from past data.”

the risk of relying on VaR: "The tragedy of VaR is that it creates the illusion of control and precision, leading to a false sense of security among risk managers.”

the role of VaR in financial crises: "VaR is like an airbag that works all the time, except when you have a car accident.“

It’s not FAIR to use VaR in cyber. Here’s why!

VaR

Value at Risk | The"FAIR" Model

Nassim Nicholas Taleb's key points against VaR Risk Management Practices:

Underestimation of Tail Risk: VaR models often fail to adequately account for extreme events, or "tail risk," low-probability but high-impact occurrences. These rare events can lead to significant losses not predicted by VaR models, as they focus on the central part of the probability distribution.

Misleading Sense of Security: VaR gives decision-makers a false sense of security by providing a single risk metric, leading to complacency, as it oversimplifies the complexity of risk and encourages the belief that risk is fully understood and controlled.

It's not FAIR to use VaR in cyber. Here's why!

VaR

Value at Risk | The"FAIR" Model

Nassim Nicholas Taleb's key points against VaR Risk Management Practices:

Inappropriate Distribution Assumptions: VaR models assume a normal distribution of returns, which is inappropriate for financial markets that exhibit fat tails and skewed distributions. Taleb criticizes these assumptions, which ignore the true nature of market behavior, leading to inaccurate risk assessments.

Historical Data Limitations: VaR relies heavily on historical data to predict future risks, but this data does not always indicate future results. This reliance can lead to significant underestimation of risk during market stress or structural changes.

It's not FAIR to use VaR in cyber. Here's why!

VaR

Value at Risk | The"FAIR" Model

Nassim Nicholas Taleb's key points against VaR Risk Management Practices:

Lack of Robustness: VaR models lack robustness because they do not account for the full range of potential outcomes, especially under extreme conditions. He argues that this lack of robustness makes VaR models fragile and unreliable in the face of unforeseen events.

Encourages Risk-Taking Behavior: Because VaR focuses on average risk within a confidence interval, institutions may underestimate the potential for large losses, prompting them to take on more risk than is prudent.

It's not FAIR to use VaR in cyber. Here's why!

SUMMARY:

VaR

is dangerous for Cyber Risk Management

1. Underestimation of Extreme Events
2. Historical Data Reliance
3. Model Risk
4. Lack of Robustness
5. Static Nature
6. Ignores Liquidity Risk
7. Complacency and Over-Reliance
8. Regulatory and Capital Misallocation

What should you use for cyber risk instead...

ACRQ

Actuarial science is better at managing cyber risk because it:

- provides a **comprehensive, quantitative, and adaptable** risk assessment and management approach.

- incorporates **detailed statistical modeling, scenario analysis, and long-term risk evaluation**, making it well-suited for addressing cyber threats' complex and evolving nature.

Special access to this revolution in cyber risk...

ArxNimbus

JULY 18, 12 NOON ET
SPECIAL RISK CALL

ACRQ

VS

VaR

The "FAIR" Model

PLUS, learn from our dynamic duo about **special access to our patented ACRQ technology, Thrivaca™ until July 31.**

LIVE, ONLINE! Grab your VIP seat:
https://crowdcast.io/c/julriskcall