GRC Engineering Club

01 / 10

RISK QUANTIFICATION

Put a number on it.

FAIR, Factor Analysis of Information Risk, in 10 slides.
No spreadsheet required to start.

SWIPE

@ajyawn

grcengclub.com

STEP ONE

Risk is a sentence.

> A **threat** does something to an **asset** and produces a **loss.**

> "An external attacker uses a stolen credential to pull customer data from the production database."

> If you cannot write the sentence, you cannot quantify the risk.

@ajyawn

THE MODEL

Two numbers decide everything.

Risk = Loss Event Frequency × Loss Magnitude

> How often it happens in a year.

> How much it costs when it does.

> Every other factor exists to estimate one of these two.

@ajyawn

FREQUENCY

Frequency splits in two.

LEF = Threat Event Frequency × Vulnerability

> **Threat event frequency:** how often someone tries.

> **Vulnerability:** the probability a try succeeds.

> Your controls live in the vulnerability number. That is what MFA actually changes.

@ajyawn

GRC Engineering Club

05 / 10

MAGNITUDE

Magnitude has two halves.

Primary loss: response, replacement, lost productivity.

Secondary loss: fines, customer churn, legal, reputation.

Secondary is usually where the money is, and the half most registers skip.

SWIPE

ESTIMATION

Ranges, never points.

> Minimum. Most likely. Maximum.

> "Between 2 and 6 times a year, most likely 3" beats "High."

> Calibration test: would you bet your own money on the range? Widen it until you would.

@ajyawn

THE MATH

Run it. Do not average it.

> Sample each range thousands of times. That is a Monte Carlo simulation, and a spreadsheet can do it.

> You get a distribution of annual loss, not one number.

> Report the 90th percentile, the year that hurts, next to the median.

@ajyawn

THE TRANSLATION

What the board hears.

> Before: "Credential theft is a High."

> After: "Credential theft. About 3 events a year. 9 years in 10 we lose under $1.4M."

> Second one gets a budget decision. The numbers are illustrative; yours will differ.

@ajyawn

GRC Engineering Club

09 / 10

THE RULE

Make the model yours.

> FAIR is a vocabulary and a structure, not a mandate.

> Keep the terms so your estimates mean the same thing to everyone.

> Set your own ranges, your own loss tables, your own thresholds for action.

SWIPE

GRC Engineering Club

10 / 10

START TODAY

One risk. Two estimates. One reason written down.

Pick the risk your board asks about most. Estimate frequency and magnitude as ranges. Write down why. Shape the model around your organization from there.