Making Risk Understandable

(Bridging Knowledge, Wisdom & Everyday Understanding)

The Goal:
To create a shared understanding of risk that speaks to **everyone** —
From technical experts to business leaders, and from practitioners to new learners

- **I share knowledge:** using familiar models and clear, simple language
- **I apply wisdom:** through stories and relatable analogies to simplify complex ideas
- **I connect with common sense:** using everyday examples everyone can relate to

“Wisdom is not a gift of history, but the acts of memory, caution, and deliberate design.
It is not a privilege, but an architecture built on knowledge and experience.” – Roshan Sequeira

What is Risk? (Made Simple)

Risk means something **“might go wrong."**

You’re not sure it will happen — but it **“could”**.
So, you try to **“be careful”** and **“prepare just in case”**.

Simple Example:

" If the sky is cloudy , there’s a chance it might rain, and you’ll get wet.
You carry an umbrella — that’s managing risk!”

The Basic Formula:

Risk = Chance of it happening × How bad it could be
(This is called: Likelihood × Impact)

What is Likelihood?

It means how likely something is to happen.
A number between 0 (won’t happen) and 1 (will happen)
It sits between **impossible** and **certain**

What is Impact?

It means how bad things could get if something goes wrong — like losing money, trust, or access.
It’s about the damage or trouble it can cause —to ***people, money, reputation, systems, or services***.

How We Measure Cybersecurity or Business Risk (In Simpler Terms)

In cybersecurity or business, risk is calculated using a slightly modified formula — but the idea stays the same.

Risk Score =
💰 *How important the thing is **(asset value)***
⚠️ *How serious the threat is **(threat impact)***
🔓 *How weak the defenses are* **(vulnerability severity)**

So, Risk Score =
Asset Value × Threat Impact X Vulnerability Severity

"It's like leaving your house unlocked with valuables inside
— and a thief is nearby watching."

Example:
The company stores sensitive customer data (💰 valuable)
Hackers want to steal it (⚠️ serious threat)
The system has weak security (🔓 vulnerability)
👉 **That's a high-risk situation**

That's why knowing your risks helps you stay one step ahead.

Simple vs. Structured Risk Models — What's the Difference?

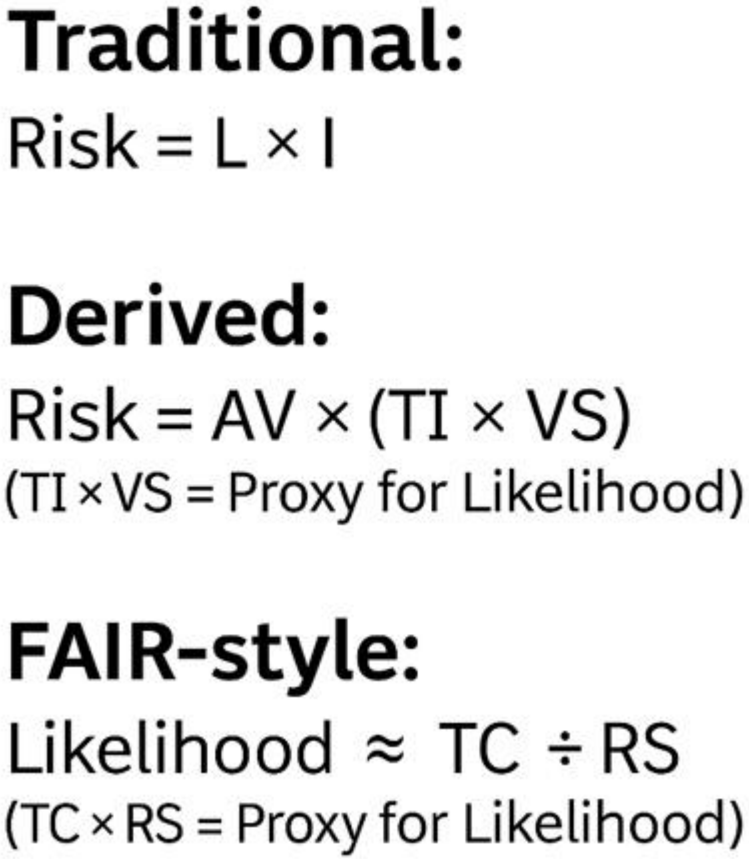
Simplified Model = Satellite View

- Shows where the risk clouds are forming
- Gives the big picture — good for planning, prioritizing, and board-level decisions
- ***You know there's a storm coming — but not how strong it is yet***
- **Risk = Likelihood × Impact**
- In these models, **'Impact'** is sometimes treated as how important the asset is
- So **'Impact'** is often treated the same as **"Asset Value"**
- Often used when Threat Impact and Vulnerability Severity aren't scored separately
- Primarily used in **top-down enterprise risk,** basic risk charts or awareness training

Structured (Derived) Model = Radar & Microscope

- **Radar →** reveals impact zones and threat patterns (like early warning systems)
- **Microscope →** zooms into **vulnerabilities, control weakness**
- For example:
  - Radar shows where and how strong the lightning may strike,
  - Microscope shows how exposed and fragile your systems really are.
- **Risk = Asset Value × Threat Impact × Vulnerability Severity**
- **Asset Value** → from CIA ratings (**Confidentiality, Integrity, Availability)**
- **Threat Impact** → How much damage if the attack succeeds
- **Vulnerability Severity** → How easy it is to exploit the weakness
- Used in enterprise-grade risk systems -**bottom-up or operational risk**

Evolution of Risk Formulas



Traditional:

Risk = L × I

Derived:

Risk = AV × (TI × VS)

(TI × VS = Proxy for Likelihood)

FAIR-style:

Likelihood ≈ TC ÷ RS

(TC × RS = Proxy for Likelihood)

How “Likelihood ≈ Threat Capability ÷ Resistance Strength” Fits In:
In Traditional/Simplified Models

Likelihood is a **standalone input**, often scored subjectively (e.g., "Likely", "Unlikely") or based on past events.
Formula: **Risk = Likelihood × Impact**

In Structured/Derived Models

Likelihood is **not entered manually** — it's ***derived***.

You calculate it based on ***two measurable components:***

- **Threat Capability (TC)** = strength, skill, resources of the attacker
- **Resistance Strength (RS)** = how well your controls resist the attack

Therefore: **Likelihood ≈ TC ÷ RS**
(The stronger the attacker and the weaker your defenses, the higher the likelihood)

Then plug this derived likelihood into:
Risk = Asset Value × Likelihood
or the expanded version:
Risk = Asset Value × Threat Impact × Vulnerability Severity = AV x (TI x VS)
Since **Threat Impact × Vulnerability Severity** can be interpreted as a ***proxy for Likelihood***, this all aligns.

Key Risk Terms —
What They Mean & How They’re Used

Term	**What It Means**	**How It's Used**
Threat	Who or what can cause harm	Defines attack scenarios
Vulnerability	Where you're exposed / weak	Shows where things can go wrong
Threat Impact	How bad it would be if the threat succeeds	Helps calculate risk severity
Vulnerability Severity	How easy it is for the attack to work	Affects how likely the threat will succeed
Likelihood (Is Model Dependent)	How likely it is to happen	**In the Traditional Model:** Likelihood is scored separately (e.g., probability based on history) **In the Derived Model:** Likelihood ≈ TI × VS (how serious the threat is × how easy it is to exploit) **Structured Model (e.g., STRIDE, STPA):** Likelihood ≈ Threat Capability ÷ Resistance Strength
Inherent Risk	Risk before controls are in place	Asset × TI × VS (which corresponds to: Inherent Risk = Impact × Likelihood — in traditional terms)
Risk Score	The final number or priority	Used in dashboards & reports

Likelihood Model explained

Model	Type	Where It Fits	Focus
STRIDE	Threat Modeling Framework	Before scoring risk (threat identification)	Identifies categories of threats
FAIR	Quantitative Risk Analysis Model	Used to calculate risk (especially financial loss)	Quantifies risk using probability and loss magnitude
Traditional/Simplified	Risk Scoring Formula	High-level or boardroom reporting	Uses Likelihood × Impact or Asset Value × Likelihood *Typically qualitative; lacks threat/vulnerability breakdown*
Structured (Derived)	Detailed Risk Formula **Risk = Asset × Threat Impact × Vulnerability Severity**	Operational & control-level assessments	Likelihood sometimes decomposed as Threat Capability ÷ Resistance Strength — esp. in FAIR)

In Structured/Derived Models - **Likelihood is not entered manually — it's derived.**
You calculate it based on two measurable components:

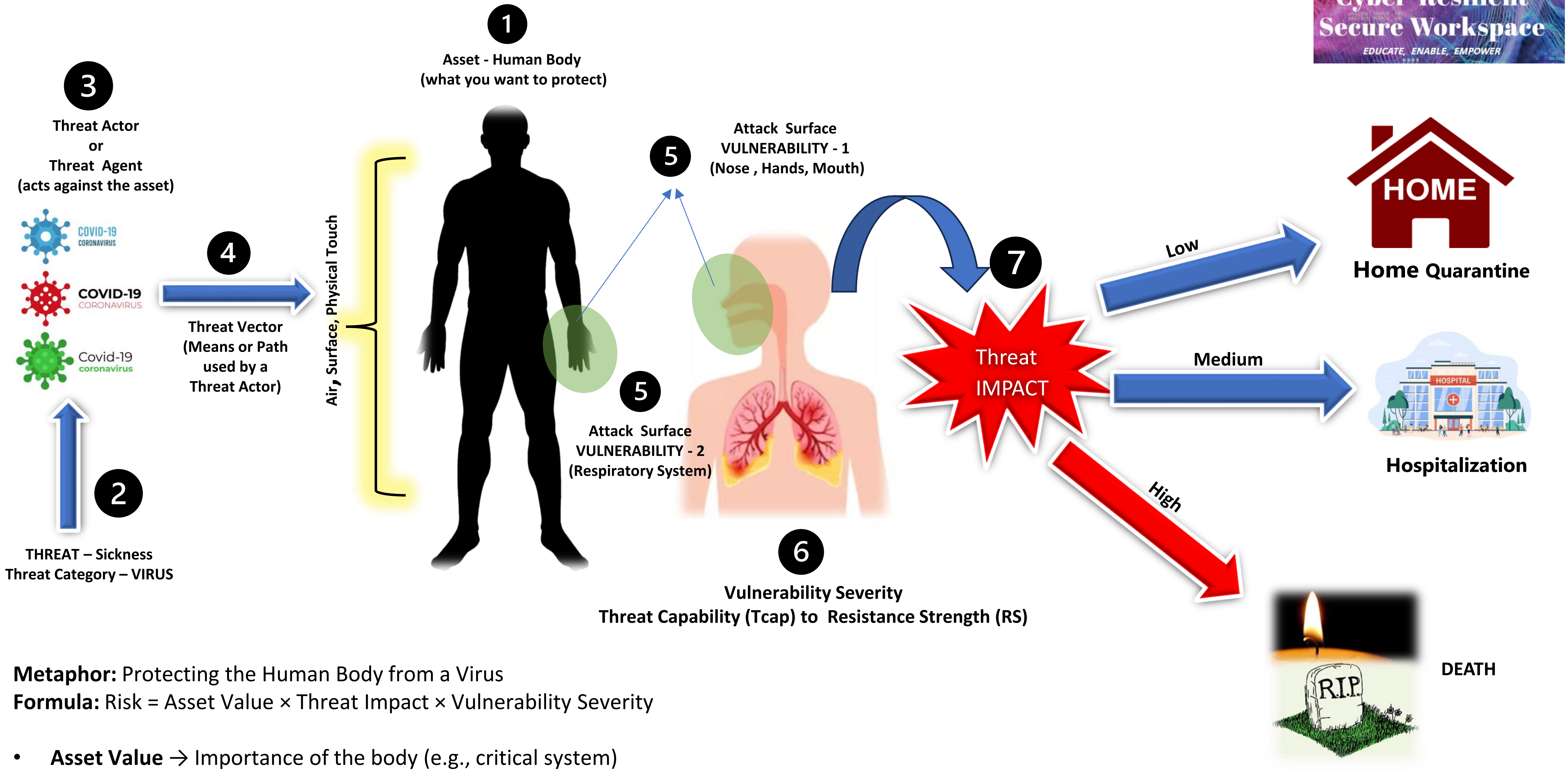
- **Threat Capability (TC)** = strength, skill, resources of the attacker
- **Resistance Strength (RS)** = how well your controls resist the attack

Therefore: **Likelihood ≈ TC ÷ RS**
(The stronger the attacker and the weaker your defenses, the higher the likelihood)

Note: Some Structured models go further by breaking **"Likelihood"** into **Threat Capability ÷ Resistance Strength** — especially in quantitative models like FAIR.

Structured modeling approach used in frameworks like:

- FAIR (Factor Analysis of Information Risk)
- Threat Modeling (STRIDE, PASTA)
- Bowtie Analysis (risk barrier modeling)



1 Asset - Human Body
(what you want to protect)

3 Threat Actor
or
Threat Agent
(acts against the asset)

2 THREAT – Sickness
Threat Category – VIRUS

4 Threat Vector
(Means or Path
used by a
Threat Actor)

Air, Surface, Physical Touch

5 Attack Surface
VULNERABILITY - 1
(Nose , Hands, Mouth)

5 Attack Surface
VULNERABILITY - 2
(Respiratory System)

6 Vulnerability Severity
Threat Capability (Tcap) to Resistance Strength (RS)

7 Threat
IMPACT

Low → Home Quarantine

Medium → Hospitalization

High → DEATH

Metaphor: Protecting the Human Body from a Virus
Formula: Risk = Asset Value × Threat Impact × Vulnerability Severity

- **Asset Value** → Importance of the body (e.g., critical system)
- **Threat Impact** → Severity if virus succeeds (e.g., hospitalization or death)
- **Vulnerability Severity** → How easily the virus can enter (e.g., no mask, weak immunity)

Image/Photo Credits – FREEPIK https://www.freepik.com/

The Human Body example :
Translating Risk Metaphor to Risk Formula

Risk Score = Asset Value × Threat Impact (T1) × Vulnerability Severity (VS)

Metaphor: Protecting the Human Body from a Virus
Formula: Risk = Asset Value × Threat Impact × Vulnerability Severity

- Asset Value → Importance of the body (e.g., critical system)
- Threat Impact → Severity if virus succeeds (e.g., hospitalization or death)
- Vulnerability Severity → How easily the virus can enter (e.g., no mask, weak immunity)

Example:

- Asset Value = 5 (Critical body system)
- Threat Impact = 4 (Hospitalization)
- Vulnerability Severity = 5 (No protection)
- **Inherent Risk = 5 × 4 × 5 = 100**

Mapping Presentation to Formal Risk Terminology

Formal Term	**Defined As**	**Presentation Mapping**
Asset	Anything of value to protect	Human body
Threat	A potential cause of an unwanted incident	Corona virus (sickness as the threat condition)
Threat Actor	Entity that executes the threat	Virus (Corona)
Threat Vector	Pathway through which threat acts	Air, physical touch, surface contact (ways virus enters body)
Vulnerability	A weakness exploitable by the threat	**Vulnerability 1**: Attack surface (mouth, nose, hands) **Vulnerability 2**: Respiratory system
Threat Impact	Consequences of successful exploitation	High impact = Death, Medium = Hospitalization Low = Home quarantine
Vulnerability Severity	Ease of exploitation of the weakness	Implied in resistance strength vs. virus capability
Likelihood	Probability that the threat will succeed in exploiting a weakness, depending on exposure and resistance	Shown as **“Threat Capability ÷ Resistance Strength”** — e.g., **no mask + high virus strength = high likelihood** of getting infected
Inherent Risk	Risk before any controls are applied	Person with no mask or immunity has full exposure **(likelihood × impact = high risk)**
Risk Score	Numerical or categorical level of risk	Not quantified directly, but inferred through severity levels (High, Medium, Low)

Risk Concepts Made Simple: A Day at the Barber

This analogy shows how everyday situations at a barber shop risks reflect formal risk concepts.

Formal Risk Term	Definition	Barber Shop Analogy
Asset	Something of value worth protecting	Client’s head
Threat	Potential cause of unwanted harm	Poor haircut, skin infection, cut
Threat Actor	Entity responsible for the threat	Untrained barber
Threat Vector	Means by which a threat is realized	Scissors, razor, towel
Vulnerability	Weakness in the system or process that may be exploited	Dirty tools, lack of sanitization
Threat Impact	Consequences of successful exploitation	Minor: uneven trim Medium: skin rash High: cut requiring stitches Critical: severe infection
Likelihood	Probability of the threat exploiting the weakness	More likely during peak hours with inexperienced staff

Real Nature of Risk ,Security, Controls and Residual Risk

Risk Can Never Be Eliminated 100% : ***We Can’t Remove All Risk***

- Every action or system has some level of risk
- Our job is to spot risks early and manage them smartly
- Even with the best controls, some risk always remains.

Security Doesn’t Mean “Perfect Safety” : ***Security ≠ 100% Protection***

- No system is 100% safe from hackers or failures
- Security is about reducing the chances and the damage
- Think layers: backups, passwords, firewalls — they work together
- "Wearing a seatbelt doesn’t stop all injuries, but it makes accidents less harmful. Security works the same way.“

What Are Controls?

- Controls are like the precautions you take every day.
- In cybersecurity, controls include: firewalls, password rules, backups, training.
- But in real life:
  - Locking your shop at night
  - Teaching kids not to open the door to strangers
- These don't remove risk, but they reduce the chance of something going wrong.

Residual Risk – The Risk That Remains

- Even after you apply all your controls, some risk remains.
- That leftover risk is called Residual Risk.
- Analogy: "Wearing a helmet while cycling lowers your risk of injury, but doesn’t eliminate the chance of falling”. **That remaining risk is Residual Risk.**

Controls (Tools & Actions to Reduce Risk)

Controls don’t erase risks — they help manage it and **keep it under control**.

Domain	**Everyday Controls (Barber Shop & Virus Analogy)**	**Why it Makes Sense**
Barber Shop	- Sterilizing scissors & razors - Barber wears gloves or mask - Using a clean towel for each customer - Displaying a hygiene certificate	Keeps germs away and prevents cuts — just like using antivirus or locking your phone
Virus Spread	- Wearing a face mask - Washing hands - Social distancing - Vaccination - Using sanitizer before touching face	Stops germs from spreading — like using passwords and backups to stop cyberattacks

Key takeaways:

- **Controls aren’t about perfection** — they’re about protection. That’s what keeps the business (and the barber) running.
- **Controls are like caring parents** — they can’t prevent every fall, but they do everything to keep you safe.
- **Good controls are like good barbers** — when they work, no one notices. When they fail, everyone screams.

Residual Risk (What Still Remains After Controls)

That **small leftover risk** is what we call **Residual Risk** — and we must stay alert to manage it **continuously.**

Domain	**Examples of Residual Risk**	**Why it Matters**
Barber Shop	- Despite clean tools, a minor rash may occur - Slight discomfort from a rushed cut during peak hours	You can sanitize everything — but even the best barbers slip sometimes.
Virus Spread	- Even with a mask or vaccine, you might still catch a mild cold. - Some people can spread the virus without knowing they have it.	You can do all the right things — and still get unlucky. Just like cyber risk — ***it only takes one click.*** 🖱️

Residual risk is like garlic breath — no matter how much you prepare, some always lingers.
In risk, perfection is a myth. Precision is a must.
You manage risk not to ***eliminate surprises*** — but to survive them.

The Power of Understanding — Knowledge, Wisdom & Common Sense

Concept	What We Use	Why It Helps
Knowledge	Formal definitions and formulas: • Risk = AV × TI × VS • CIA model • Threat Capability ÷ Resistance Strength	Builds a shared language for everyone to work from
Wisdom	Use of relatable analogies (e.g., health and virus metaphors) Clarifying misunderstood terms (like "Asset Impact" vs. "Asset Value")	Draws from real-world context to make complex ideas clearer. Brings risk to life — like knowing not to trust a barber with shaky hands
Common Sense	Simple scenarios: • No mask = exposure • Hands/nose as attack surfaces • Dirty razor = risk	Keeps risk relatable and applicable to everyday decisions

Everyone Thinks Differently — and That's Okay.
Whether **it's a formula, a metaphor, or a lived experience** — the aim is to speak to all , because risk is best managed when everyone understands it.
In risk, like in haircuts, **you only realize the mistake once it's too late.**

Making Common Sense out of Security

Being Aware is the First Step towards an Informed Decision

ROSHAN NEVILLE SEQUEIRA , MSc (Information Systems Management)

Award Winner, Golden Visa - Special Talent Category

Certifications:

- Cybersecurity & Privacy: CISSP, ISSMP, CISA, CDPSE, ISO27001:LA
- Enterprise & Architecture: TOGAF
- GRC & Governance: GRCP, GRCA, CCIS, IAIP, IAAP, IPMP, ICEP, IDPP
- Other: 5S Practitioner, LEAN Foundation Certified

☎ +971-54-442-7566

LinkedIn | Personal Website | YouTube Channel | Project Cerebellum

Disclaimer:

The views and opinions expressed in this presentation are solely my own and do not necessarily reflect those of my current or past employers.