
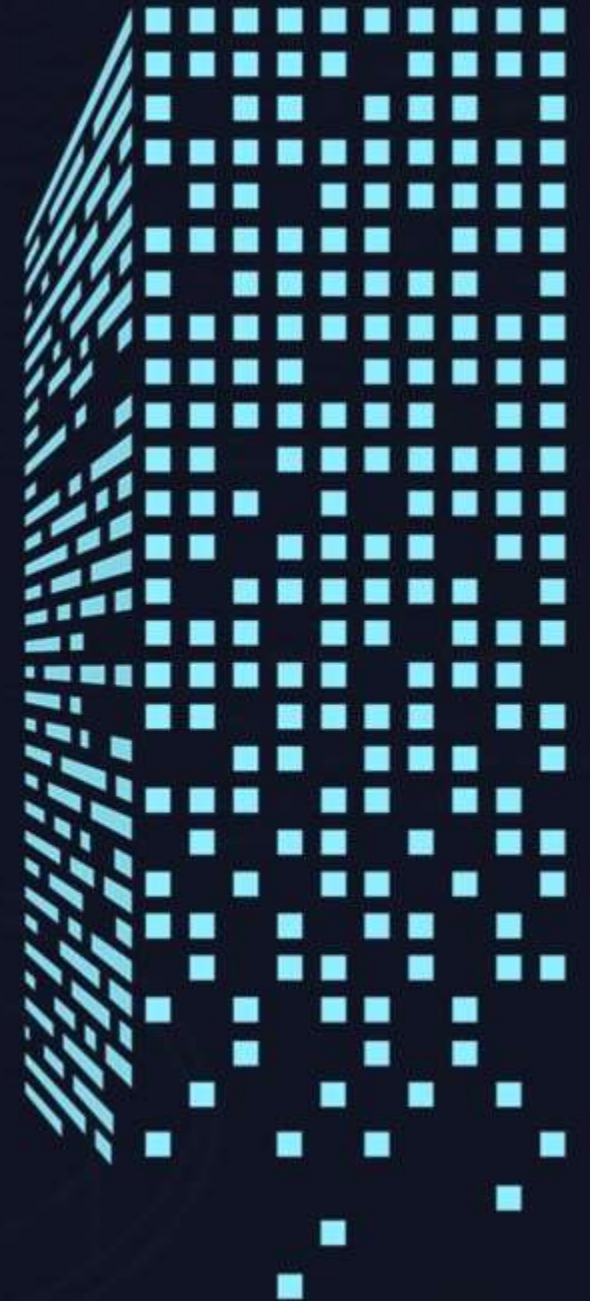


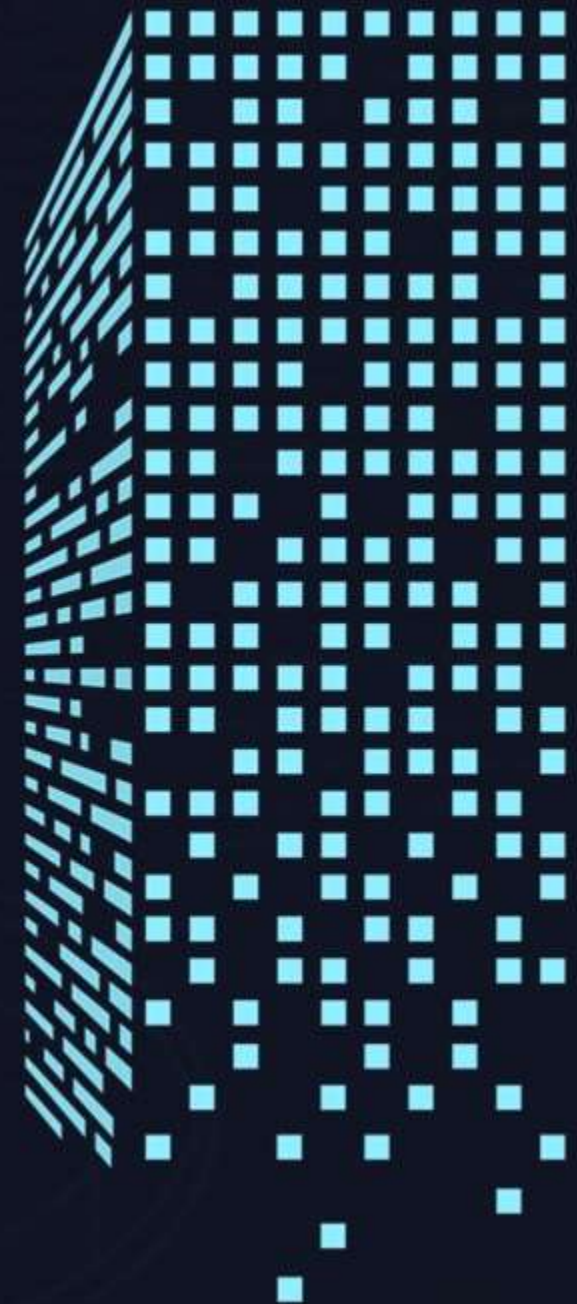
A large, stylized splash of water in shades of blue and white, centered in the background. The splash forms a circular shape with intricate, branching patterns radiating outwards.

Quantitative Privacy Risk Analysis

A solid light blue vertical bar on the left side of the slide.

R. Jason Cronk* & Stuart S. Shapiro





Talk Outline

Why measure privacy risk?

What is privacy risk?

Quantitative privacy risk modeling

Discussion

Why measure risk?

- Prioritize risk mitigation efforts
- Fit within acceptable tolerance levels
- Comply with laws and regulations

GDPR Article 25 Data Protection by Design and Default

“Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, ...”



The likelihood of a threat
exploiting a vulnerability and
resulting in adverse
consequences

What is “risk?”

What is privacy "risk?"

How Likely?

How Severe?

Threat exploiting a vulnerability and resulting in adverse consequences



Privacy?



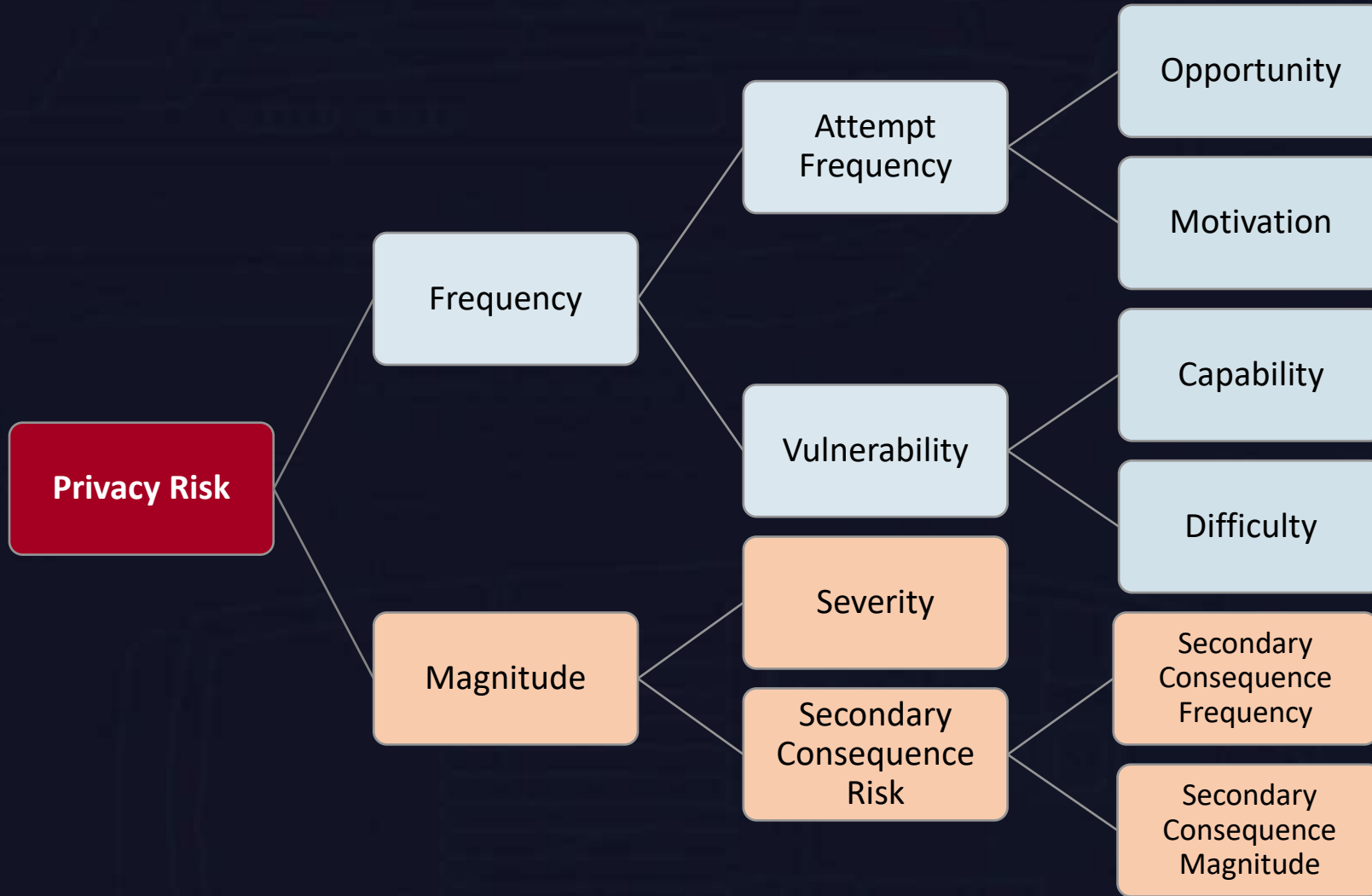
Privacy?



"Invasion of Privacy"
Or "Privacy Harm"



Factors Analysis of Information Risk (FAIR) - Privacy





Quantifying risk

What is privacy “risk?”

Threat exploiting a vulnerability and resulting in adverse consequences



Threat = Wicked Witch Watches
(threat actor and means)

**Vulnerability = Oz is visible through
Crystal Ball**

**Consequences = Dorothy and party
are surveilled**



FAIR - Privacy

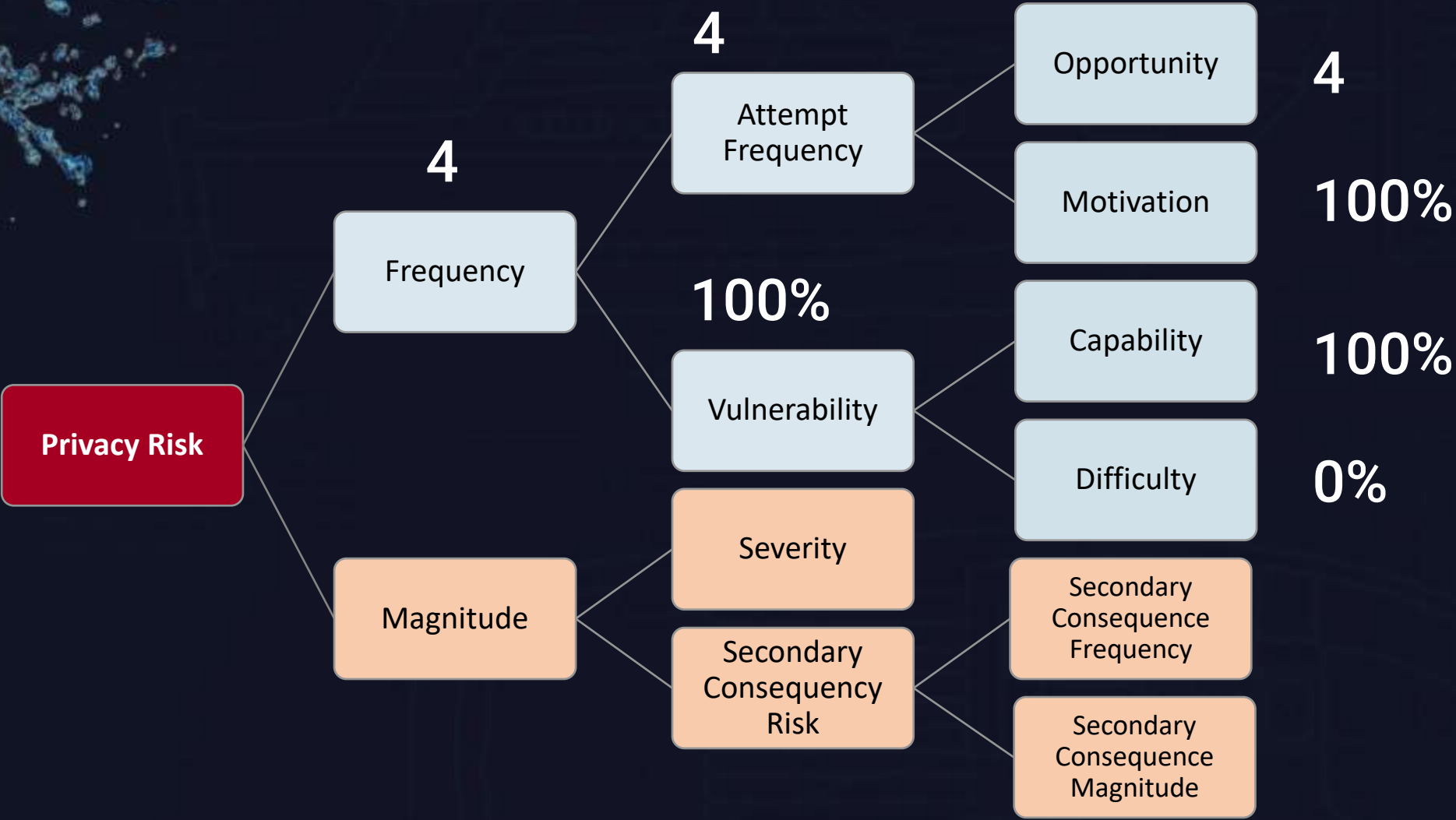
Time Period: Dorothy's trip to Oz

At-Risk: Dorothy and her compatriots

Threat Actor: Wicked Witch

Capability (skills and resources): Crystal Ball

Impediments: None



FAIR - Privacy

Awareness

None

Benefit

None

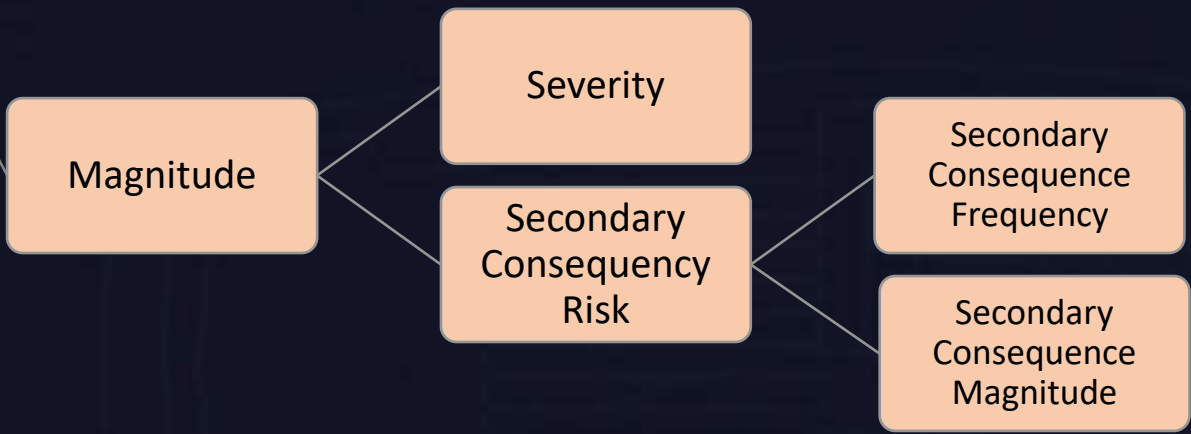
Consent

None



	Violation?
Dorothy	Yes
Scarecrow	Yes
Lion	Yes
TinMan	No
Severity	75%

Privacy Risk





Privacy Risk

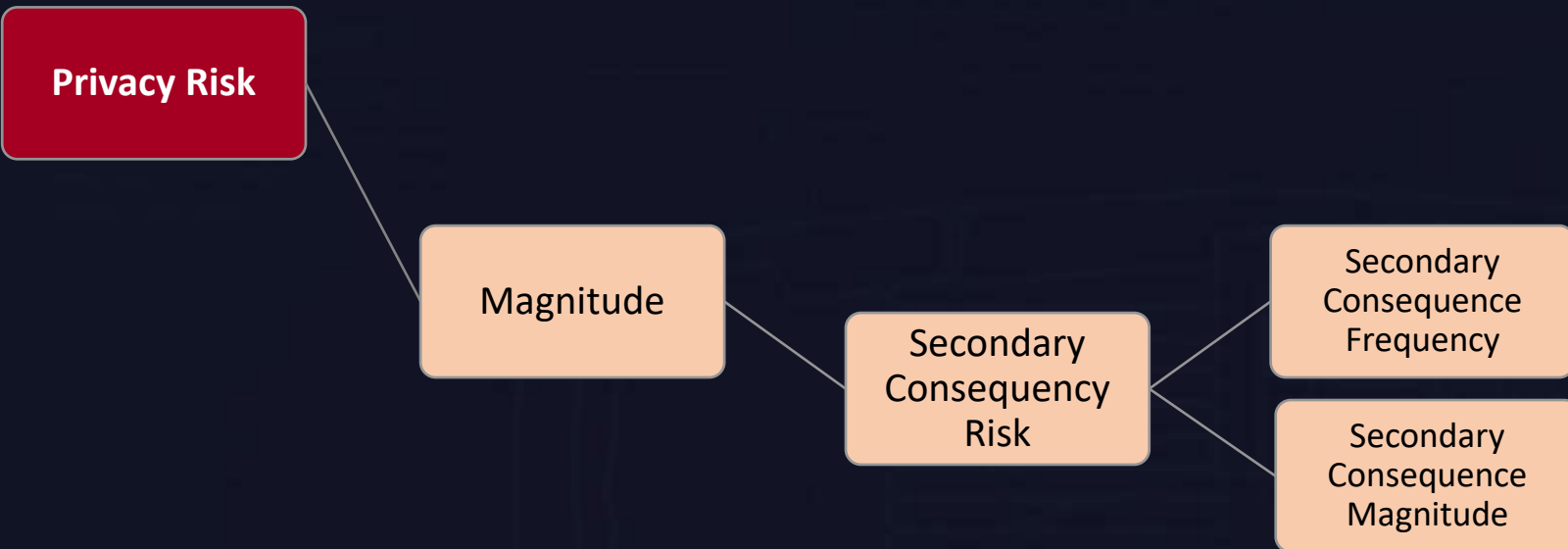


FAIR - Privacy

	Delayed	Burned	Rusted	Scared
Dorothy	1 hour	1%	0%	0
Scarecrow	1 hour	5%	0%	.75
Lion	1 Hour	0%	0%	1
Tin Man	1 Hour	1%	20%	0

	Violation?
Dorothy	Yes
Scarecrow	Yes
Lion	Yes
TinMan	No
Severity	75%

	Delayed	Burned	Rusted	Scared
Freq.	100%	75%	25%	50%
Mag.	1 hour	1% to 5%	20%	.75 to 1



FAIR - Privacy

Privacy Risk

**3 Violations
of Privacy
(e.g. people
surveilled)**

**4 hours
of delay**

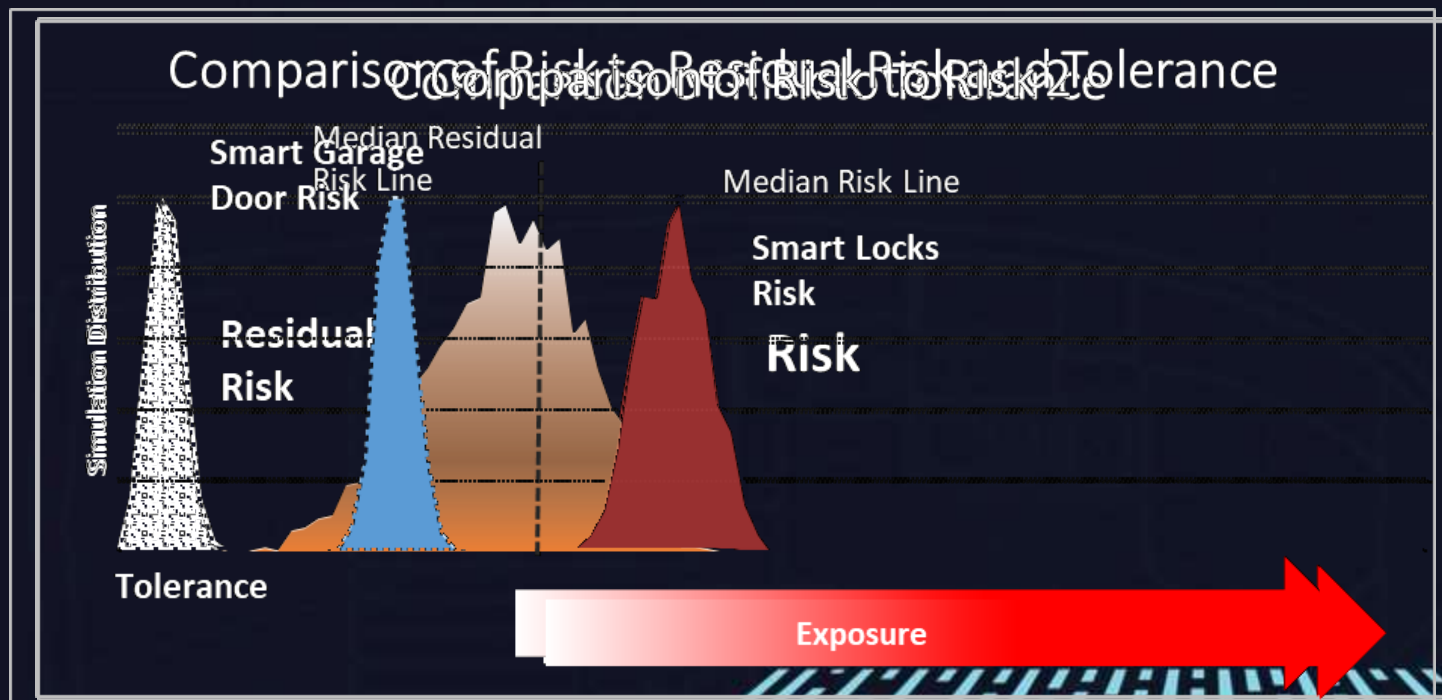
**3 burns
over 1-5%
of their
body**

**1 Rusting
over 20
percent of
their body**

**2 People
scared
from .75 to
1 on a 0-1
scale**


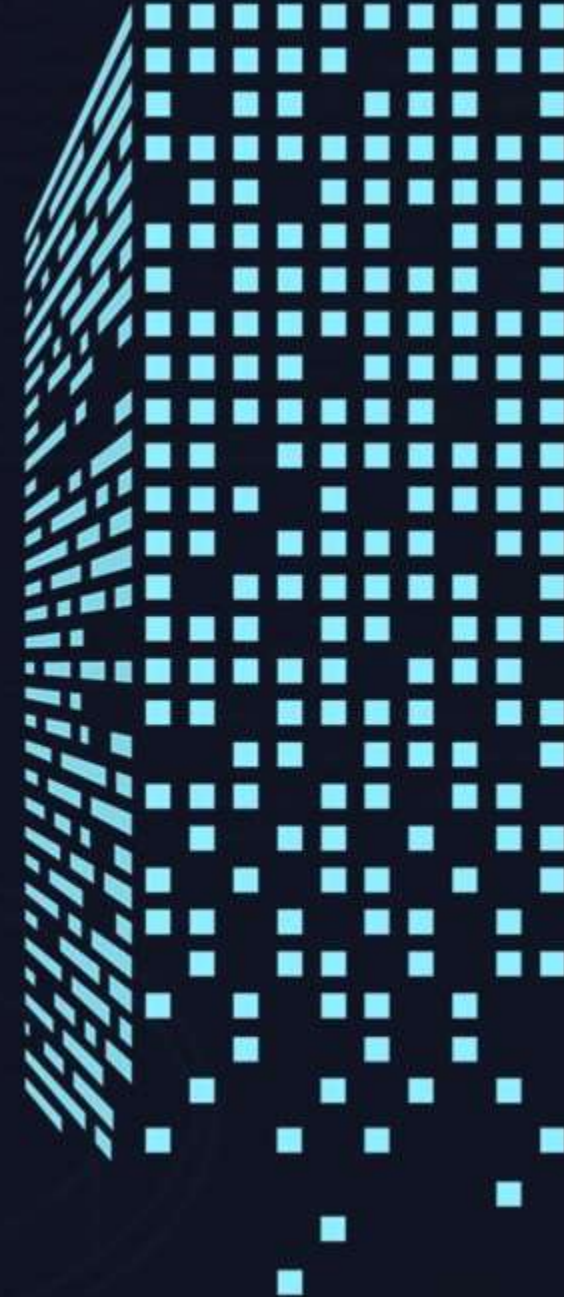
Reality

- Each factor uses a probability distribution to represent uncertainty and variance in values
- Monte Carlo method used to simulate thousands of trial periods



A dynamic splash of water in shades of blue and white, centered behind the main text.A 3D perspective view of a grid of glowing blue squares, receding into the distance on the right side of the slide.

Use Case – Data Transfer Risk Assessments (Article 46 GDPR)

A dynamic splash of water in shades of blue and white, centered behind the text.A 3D grid of glowing blue squares on a dark background, receding into the distance on the right side of the slide.

Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, *if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice*, to your transferred data and/or importer.

- European Data Protection Board



FAIR - Privacy

Threat:
access by authorities
in 3rd country

Frequency

Attempt
Frequency

Opportunity

Motivation

Vulnerability

Capability

Difficulty

Severity:
How "bad" is it?

Magnitude

Severity

Secondary
Consequence
Risk

Secondary
Consequence
Frequency

Secondary
Consequence
Magnitude

Privacy Risk

At-Risk:

Data subjects of transferred data

Threat Actor:

Government authorities

Capability:

Do they have legal (warrant, subpoena, etc.) or technical skills and resources

Impediments:

Supplemental Measures

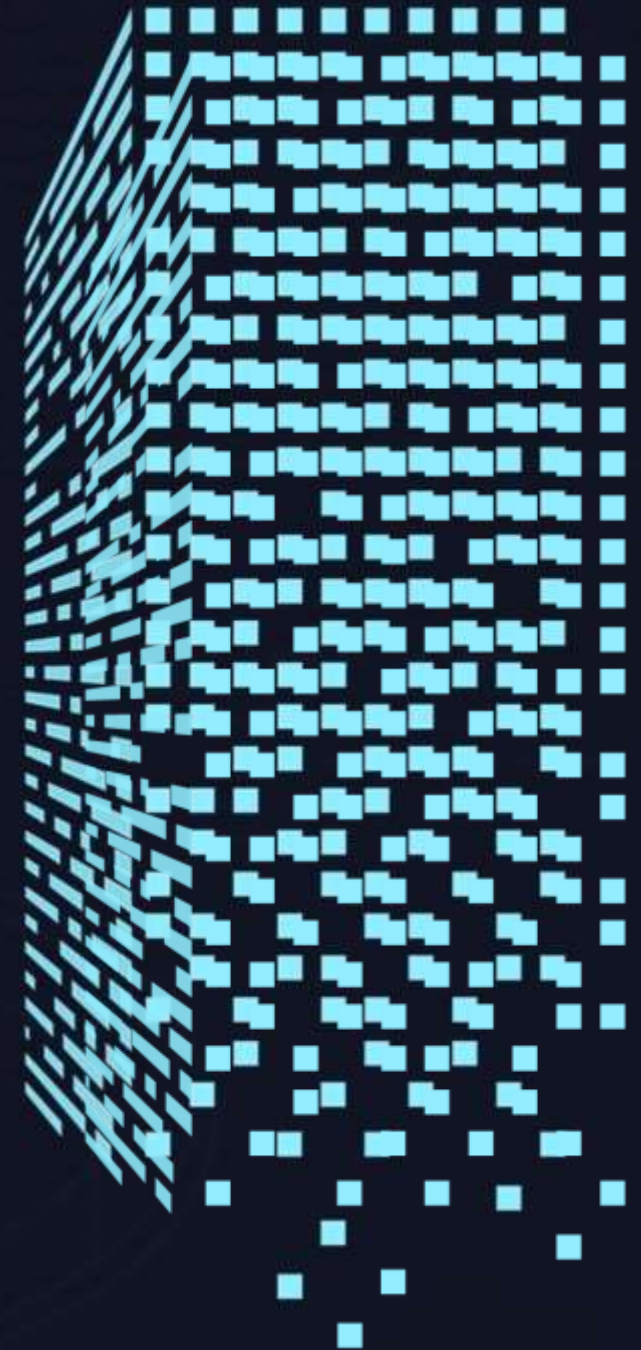
Secondary Consequences:

Unable to exercise rights of redress, erasure, access
No-fly list, arrest, seizure



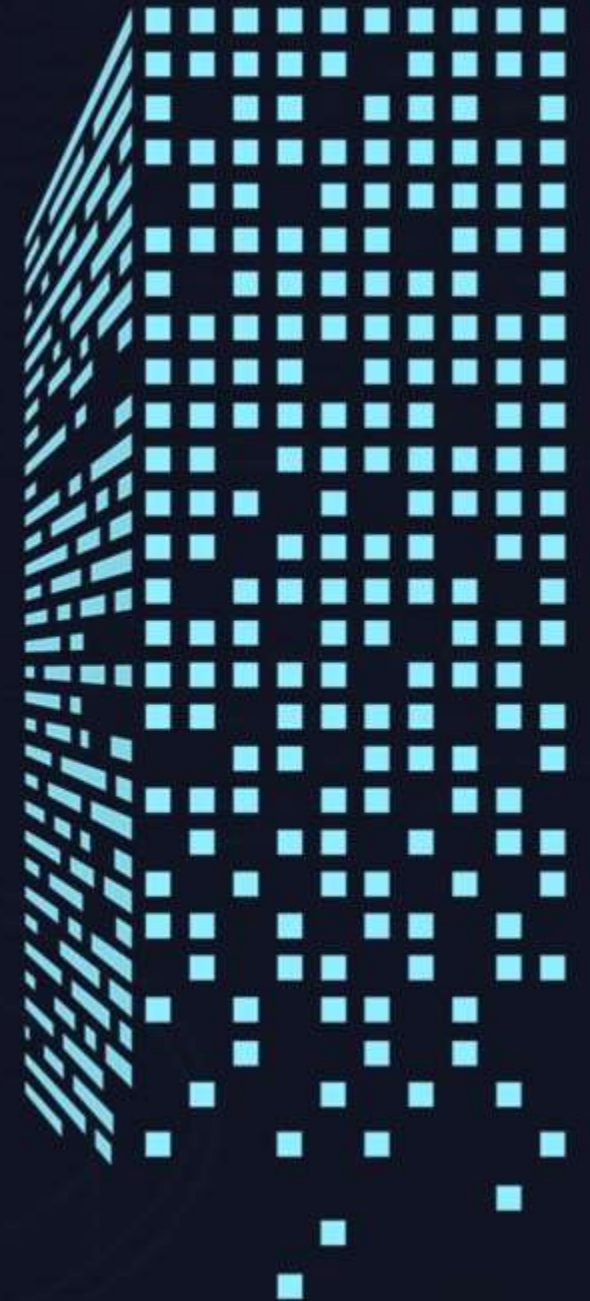


Questions

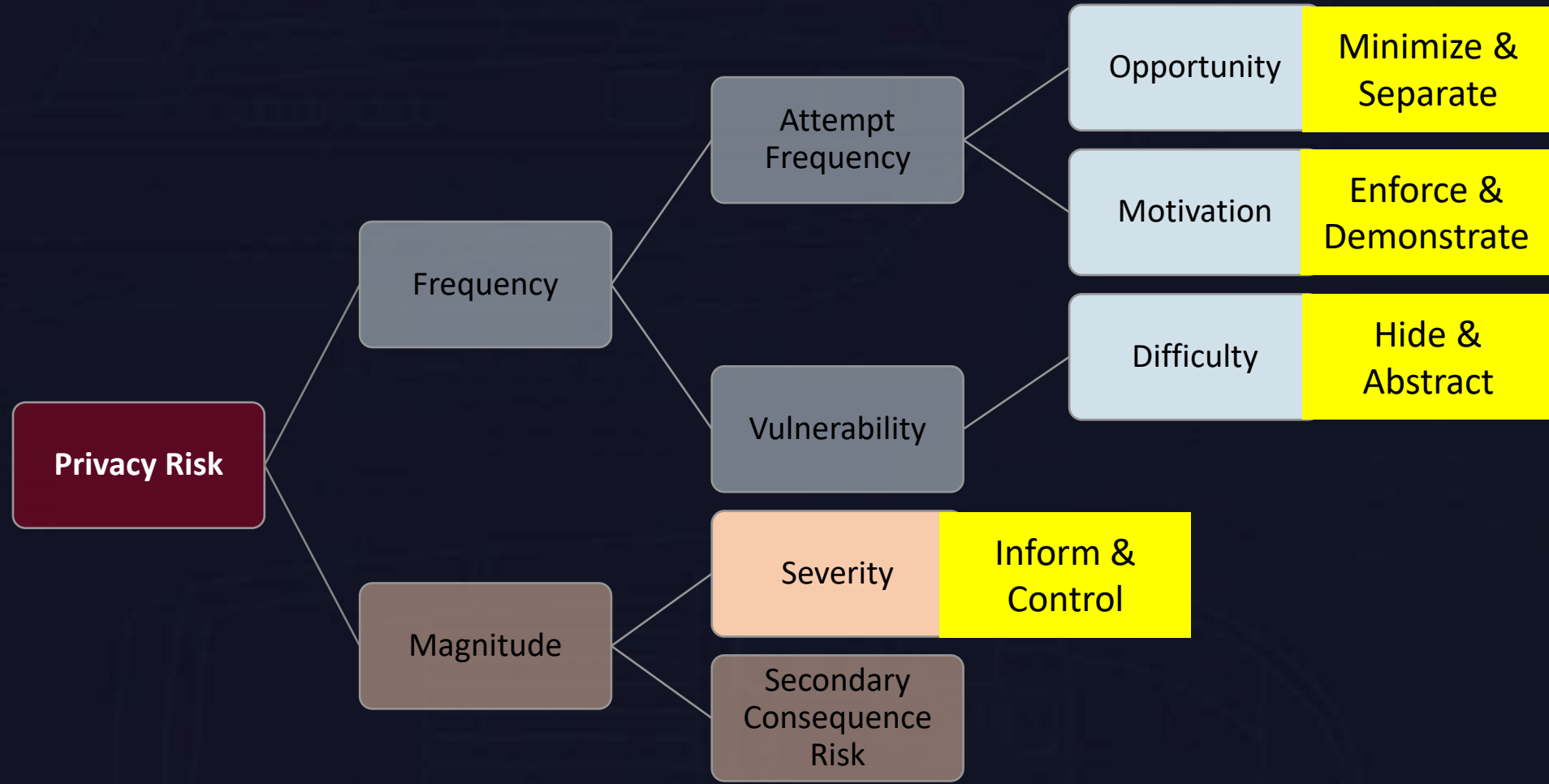


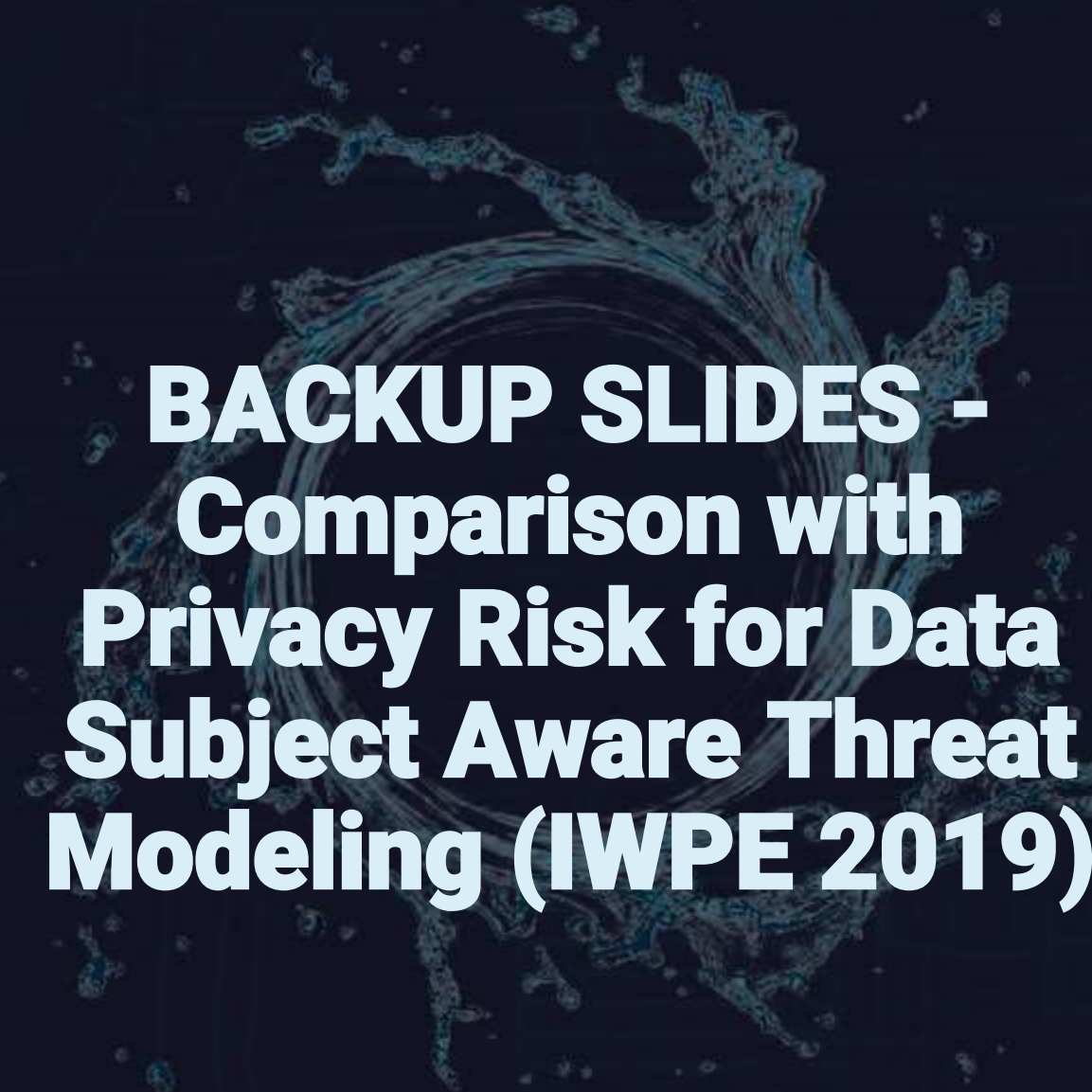
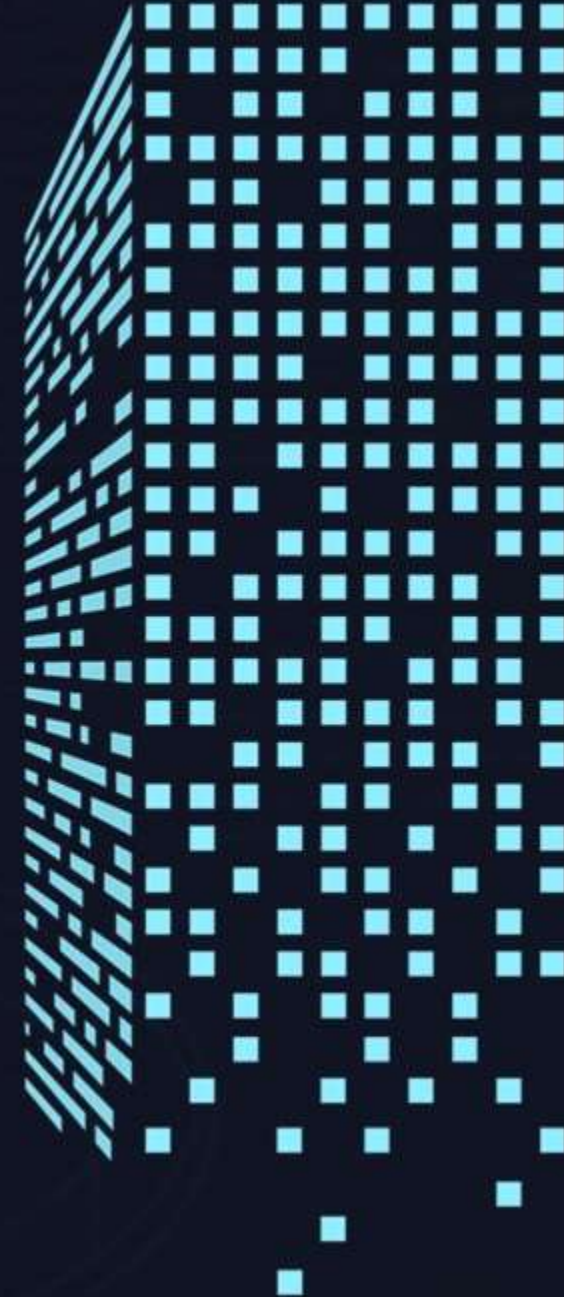
A large, stylized graphic of a water splash or circular motion in shades of blue and white, centered behind the main text.

BACKUP SLIDES – Privacy Design Strategies



Mapping FAIR to Privacy Design Strategies



A dynamic splash of water in shades of blue and white, centered behind the main text.A 3D grid of glowing blue squares, receding into the distance on the right side of the slide.

**BACKUP SLIDES -
Comparison with
Privacy Risk for Data
Subject Aware Threat
Modeling (IWPE 2019)**

Privacy Harms

FAIR- P

Solove Taxonomy of Privacy

- **Collection**
 - Surveillance
 - Interrogation
- **Information Processing**
 - Aggregation
 - Identification
 - Insecurity
 - Exclusion
- **Information Dissemination**
 - Disclosure
 - Exposure
 - Increased Accessibility
 - Breach of Confidentiality
 - Appropriation
 - Distortion
- **Invasion**
 - Intrusion
 - Decisional Interference

Privacy Risk for Data Subject Aware Threat Modeling



LINKABILITY



IDENTIFIABILITY



NON-REPUDATION

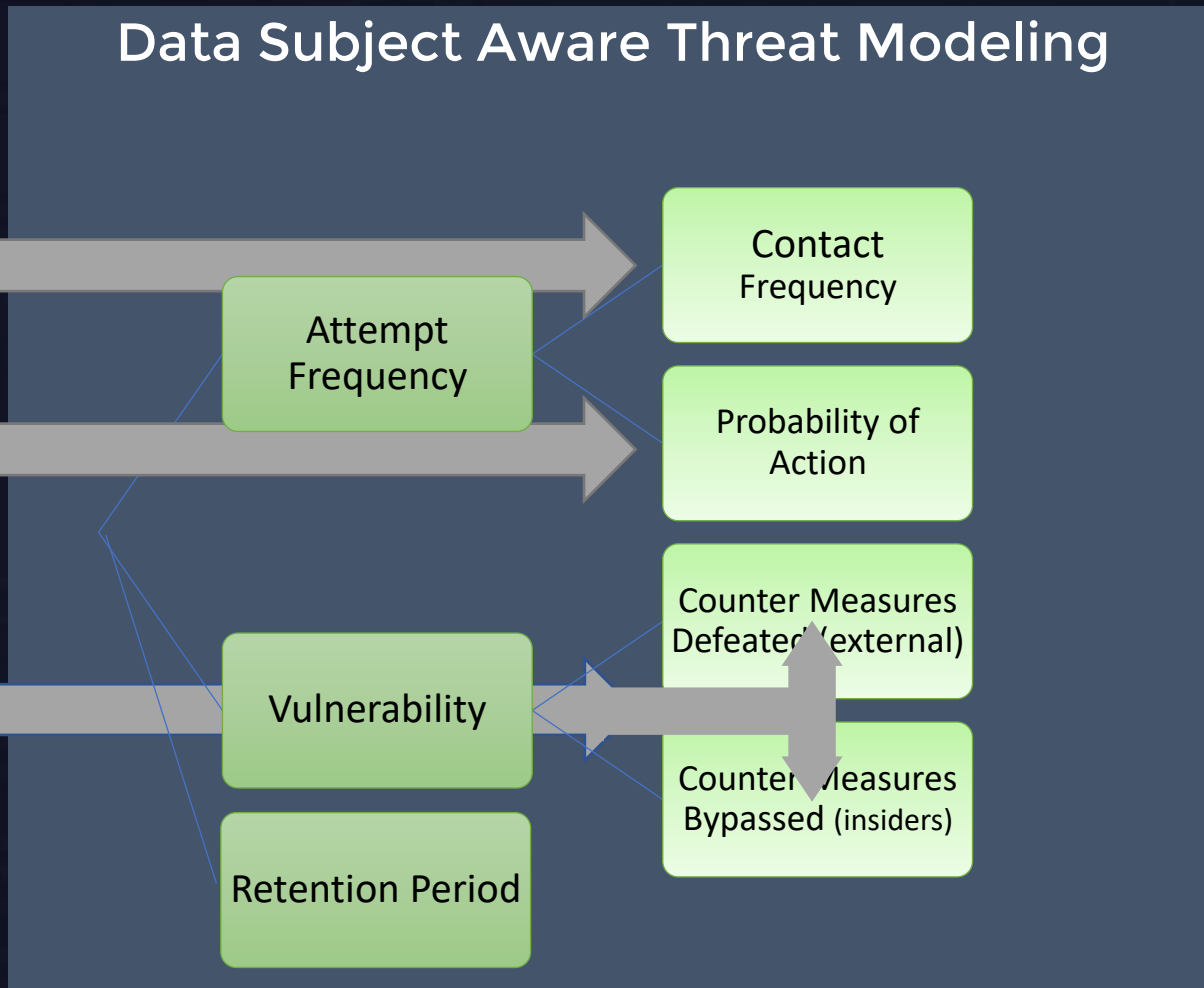


DETECTABILITY



DISCLOSURE OF INFORMATION

Frequency Factors



Magnitude Factors

