

RVA 2013

A large green graphic of the state of Virginia. The interior of the state is filled with a white grid pattern. Overlaid on the map are three white rectangular boxes. The first box on the left contains a grid pattern. The second box in the middle contains a solid black rectangle. The third box on the right contains a white target symbol with a central bullseye and crosshairs.

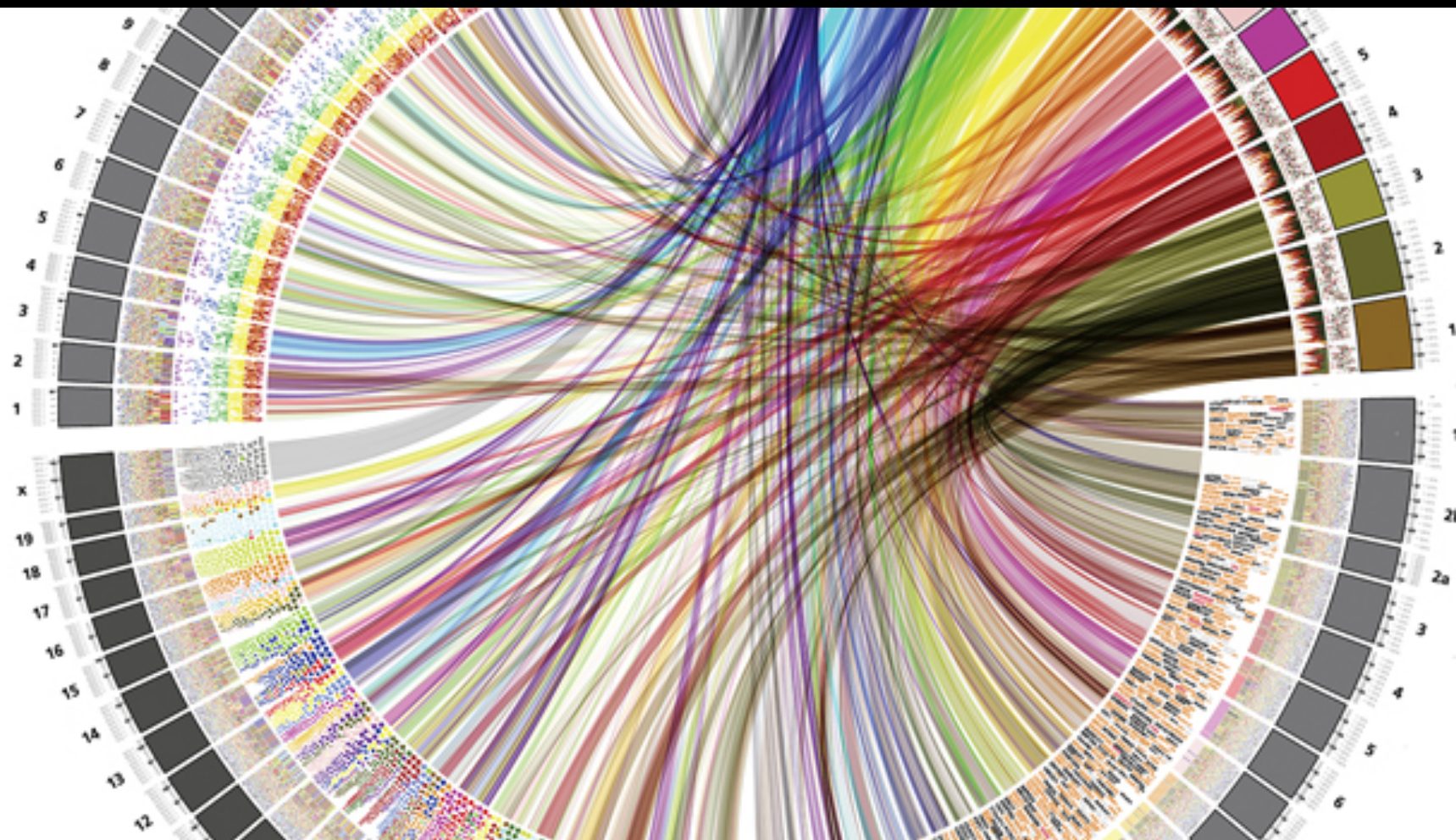
Platinum Sponsors



Gold Sponsors



TOWARDS A MODERN APPROACH TO RISK MANAGEMENT



Alex Hutton - @alexhutton

I AM HERE ON MY
OWN.

I AM **NOT** SPEAKING
ON BEHALF OF
ZIONS BANCORP

First, some inspiration:

A New Approach for Managing Operational Risk

Addressing the Issues Underlying the 2008 Global Financial Crisis

Sponsored by:
Joint Risk Management Section
Society of Actuaries
Canadian Institute of Actuaries
Casualty Actuarial Society



Prepared by:



Originally Published: December 2009
Revised: July 2010

© 2009, 2010 Society of Actuaries, All Rights Reserved
The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the sponsoring organizations or their members. The sponsoring organizations make no representation or warranty to the accuracy of the information.

A New Approach for Managing Operational Risk

Addressing the Issues Underlying the 2008
Global Financial Crisis

Sponsored by:
Joint Risk Management Section Society of
Actuaries Canadian Institute of Actuaries
Casualty Actuarial Society

www.soa.org/files/pdf/research-new-approach.pdf

Not “where is the risk?”

but...

“how much risk do we have?”

Not “where is the risk?”

but...

“how much risk do we have?”

and...

”why?”

Some level setting...

There is no “risk free” (no
“secure”)

Risk is (currently) a hypothetical
construct

There are different “risk”
approaches

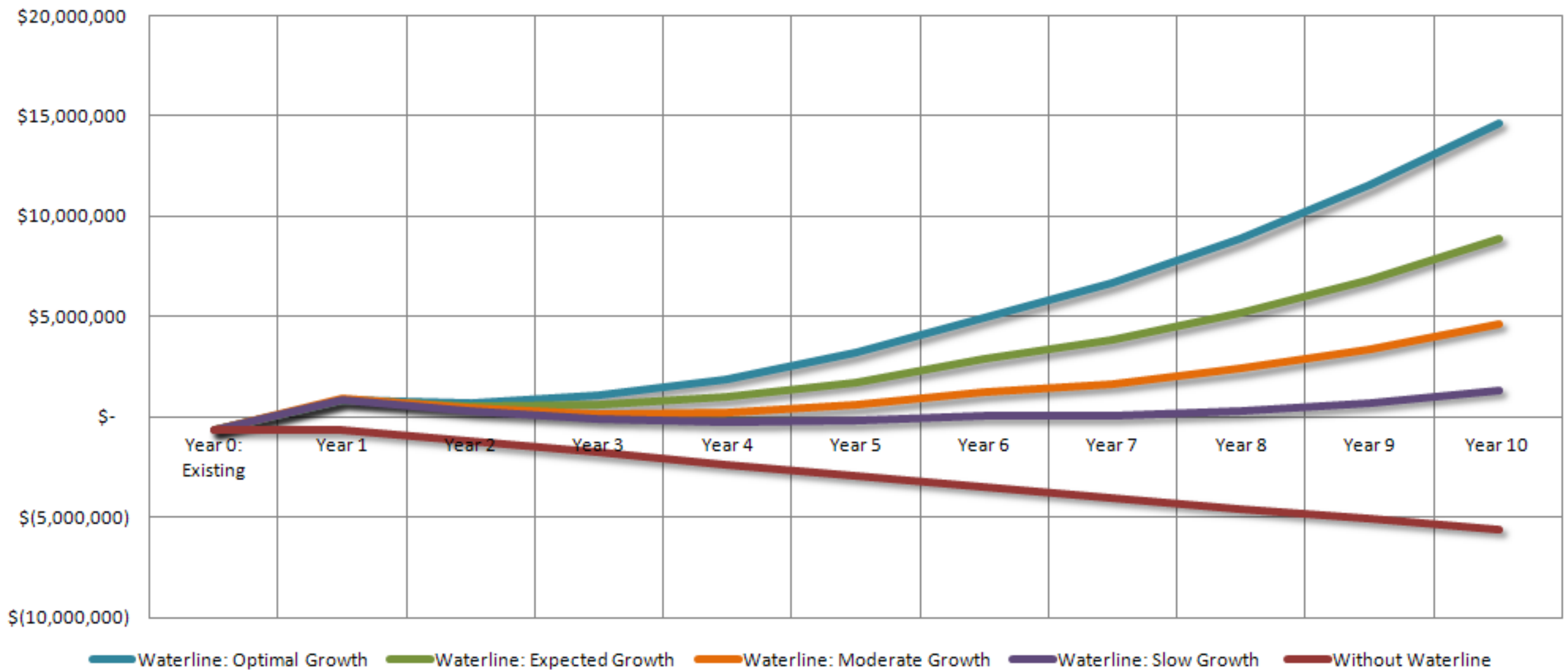
WHAT IS RISK?



How do most people view “risk”?

Financial Risk

Annual Cumulative Net Revenue: 10-Year Horizon

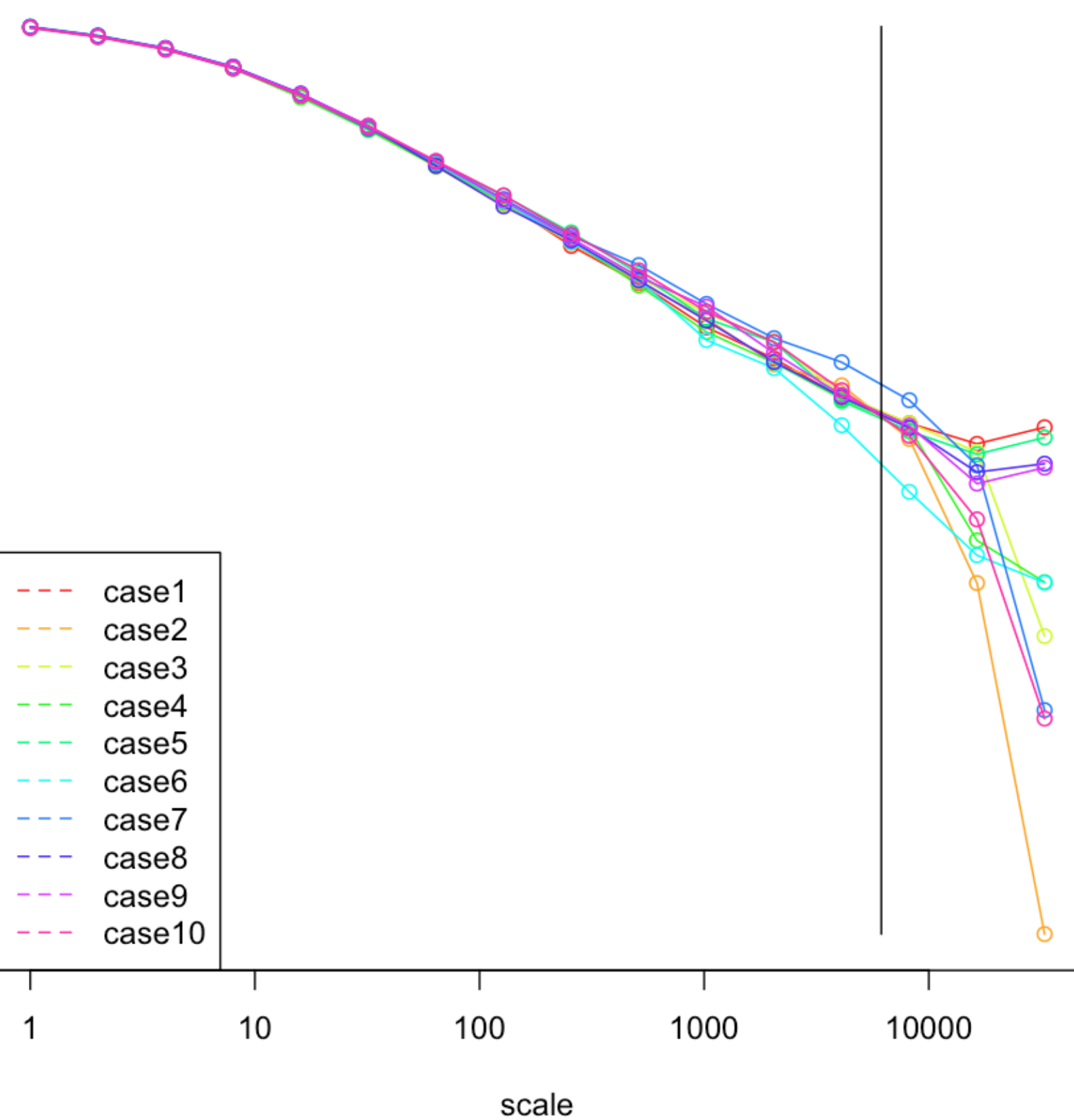


**financial risk has potential for
both positive and negative
returns**

Financial Risk

Engineering Risk





engineering risk: rate of decay

Financial Risk

Engineering Risk

A Symptom or
Audit-Driven
Approach?
("where is the risk")



**ENGINEERING RISK
MANAGEMENT:
FIND THE WEAKNESS
AND REINFORCE IT**



RCSA as commonly performed

RCSA as commonly performed

Inherent risk - Controls = Residual Risk

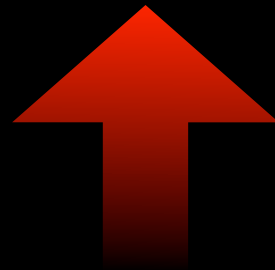
RCSA as commonly performed

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low



How awesome is your bridge?

Financial Risk

Engineering Risk

except...

Wind has no motivation

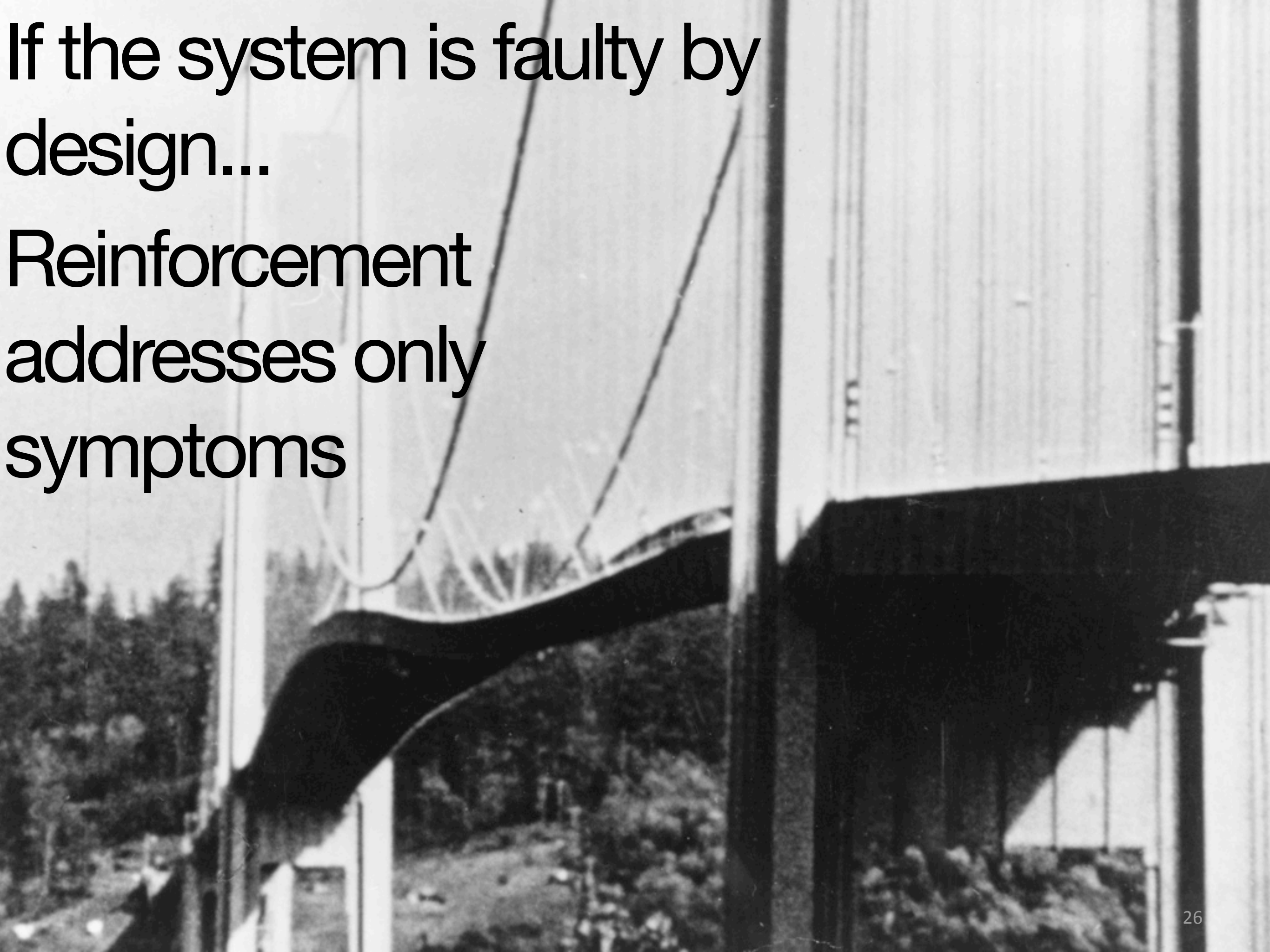


A close-up photograph of a glass surface, likely a window, covered in numerous water droplets of varying sizes. In the background, a person is visible holding a large, colorful umbrella. The person and the umbrella are out of focus, creating a bokeh effect. The umbrella has sections of teal, orange, and black. The overall scene suggests a rainy day.

Rain does not try to evade
our umbrella

If the system is faulty by
design...

Reinforcement
addresses only
symptoms

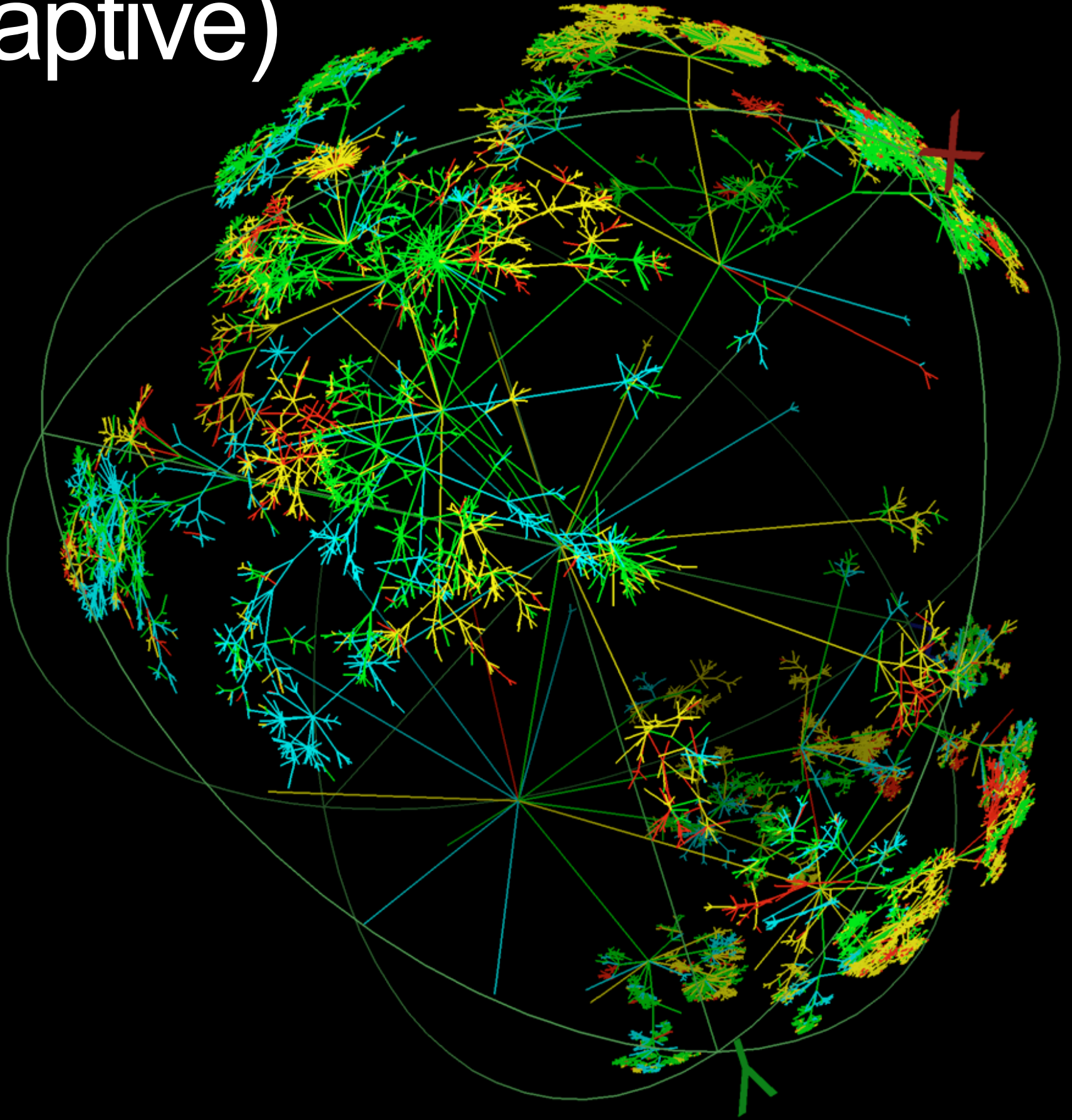


Financial Risk

Engineering Risk

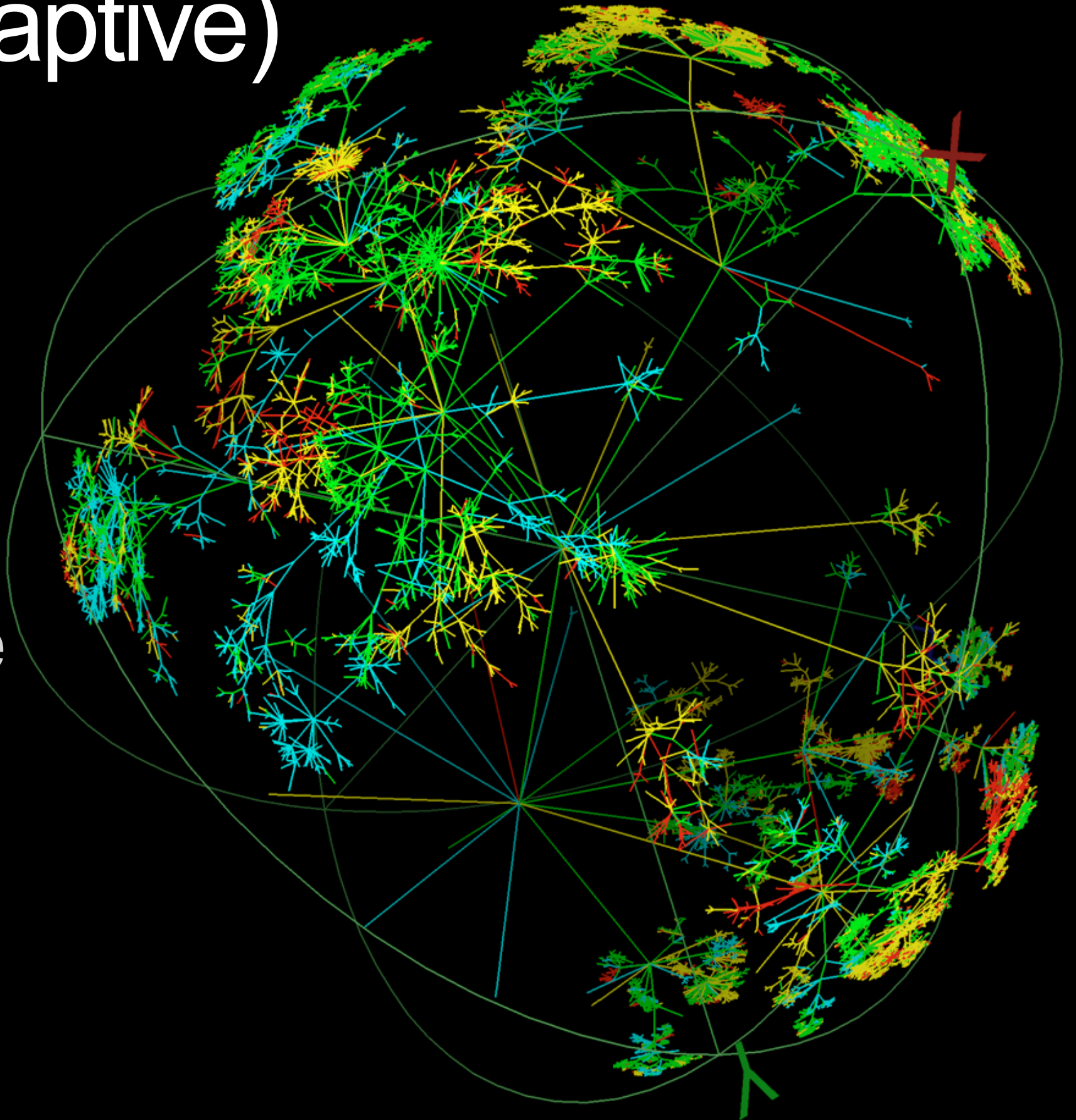
does it give a
good view of risk
in the whole
system?

Complex (adaptive) Systems



Complex (adaptive) Systems

a system
composed of
**interconnected
parts** that as a
whole exhibit one
or more
**properties not
obvious** from the
properties of the
individual parts



Complex (adaptive) Systems

a system
composed of
**interconnected
parts** that as a
whole exhibit one
or more
**properties not
obvious** from the
properties of the
individual parts



Financial Risk

Engineering Risk

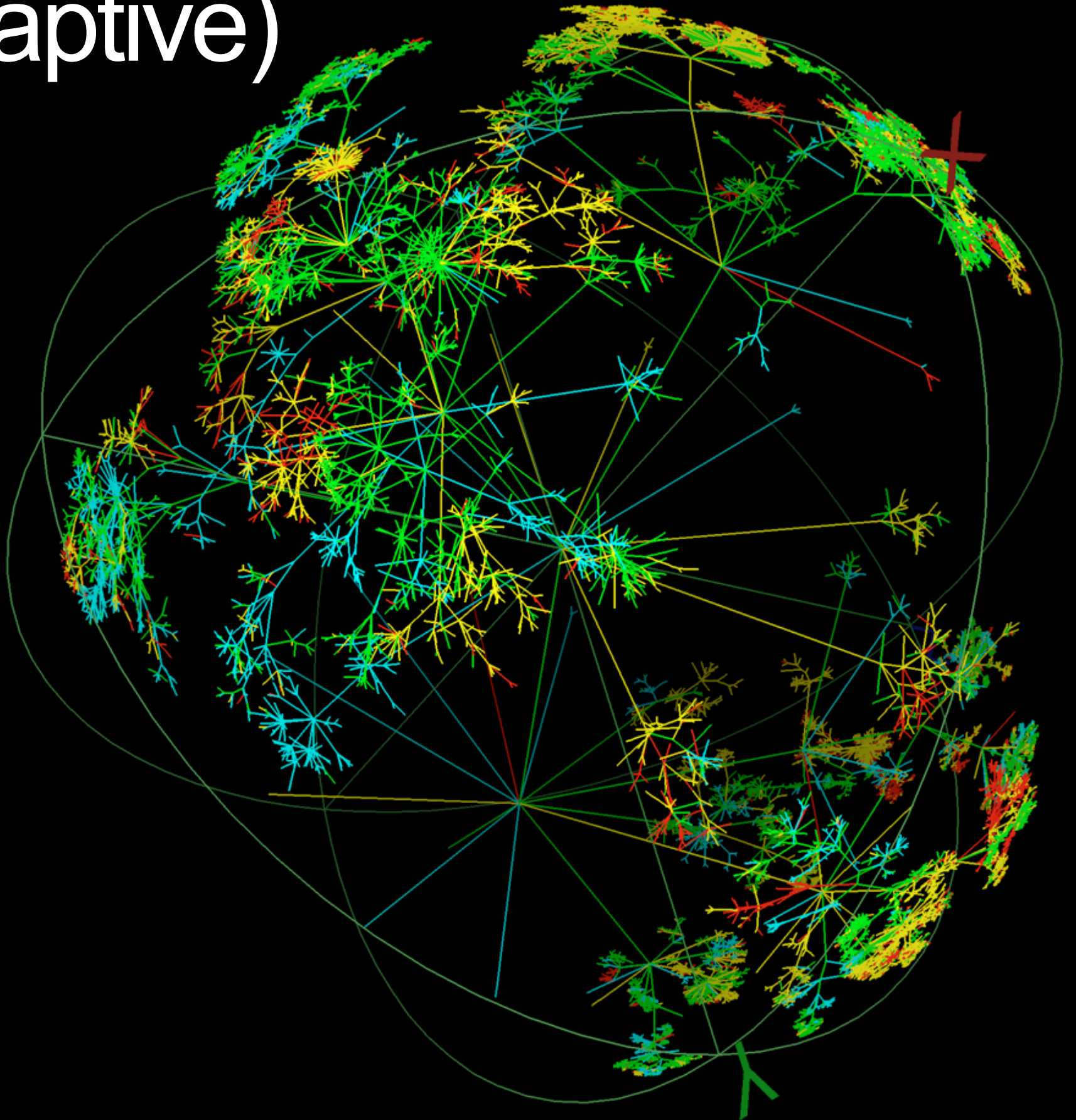
unintended
consequences
as emergent
properties





Complex (adaptive) Systems

We May be
dealing with a
complex,
adaptive system.



Financial Risk

Engineering Risk

another
problem

Science vs. Engineering?

The science of
information
security & risk
management
is hard

Pseudo-Science vs. *Proto-Science*

- somewhat random fact gathering (mainly of readily accessible data)
- a “morass” of interesting, trivial, irrelevant observations
- a variety of theories (that are spawned from what he calls philosophical speculation) that provide little guidance to data gathering

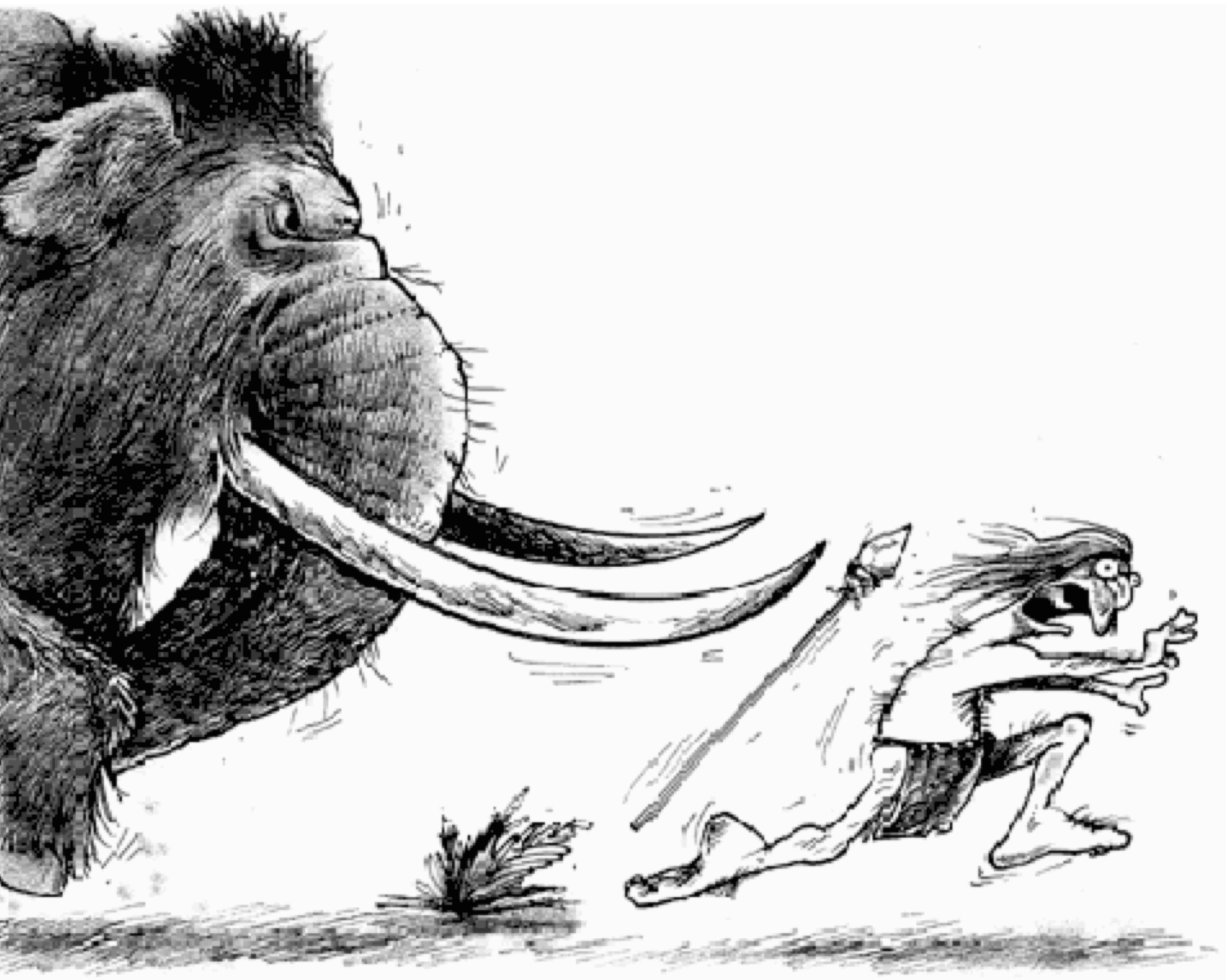




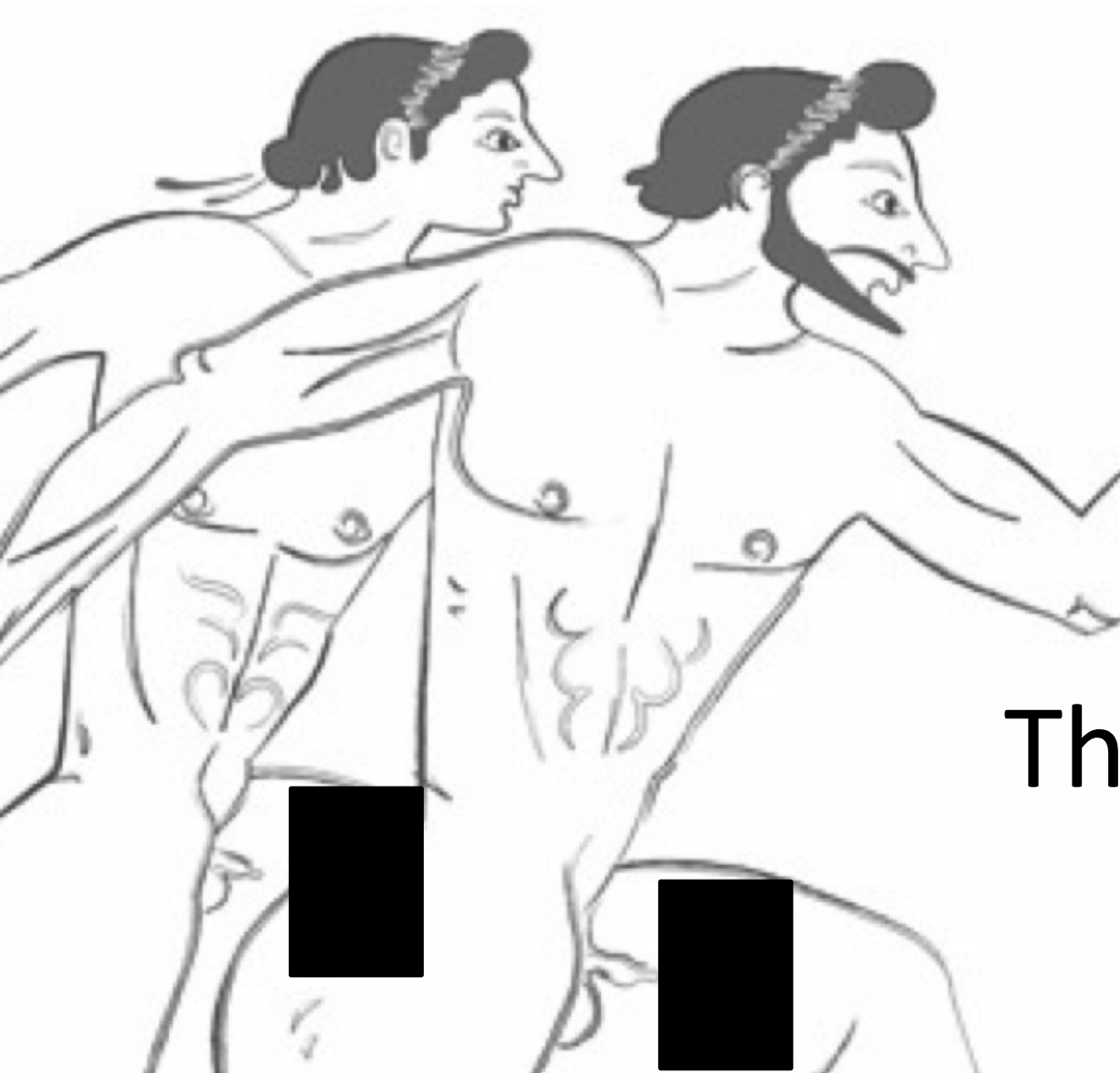
At our present skill in measurement of security, we generally **have an ordinal scale at best**, not an interval scale and certainly not a ratio scale. In plain terms, this means we can say whether X is better than Y but how much better and compared to what is not so easy.

— Dan Geer

The First (and most important) Measurement:



Survival



The Second Measurement: *comparison*

The Third Measurement: *units*

Our observable factors that correlate well with the construct of speed happen to be time and distance.



Science is based on inductive observations to derive meaning and understanding and measurement on quality (ratio) scales, so what about InfoSec?

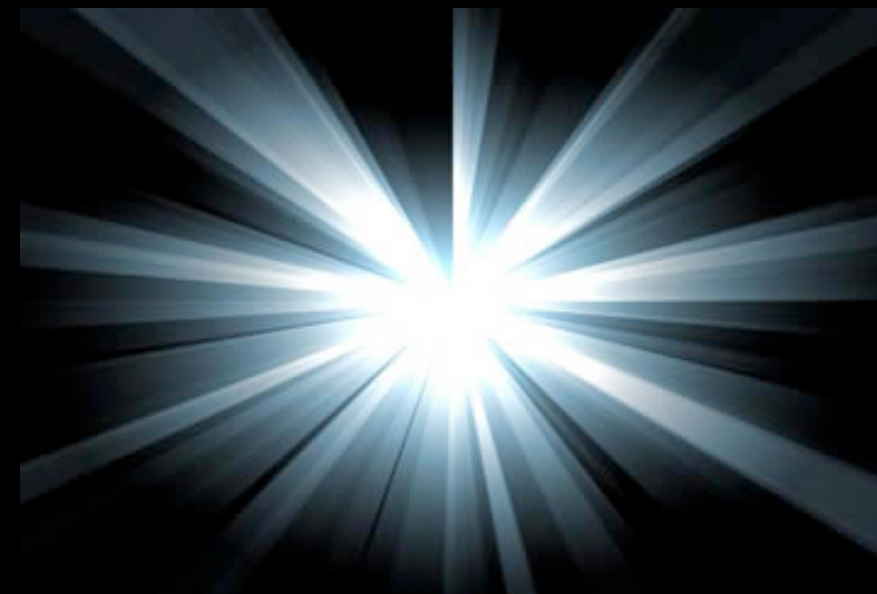
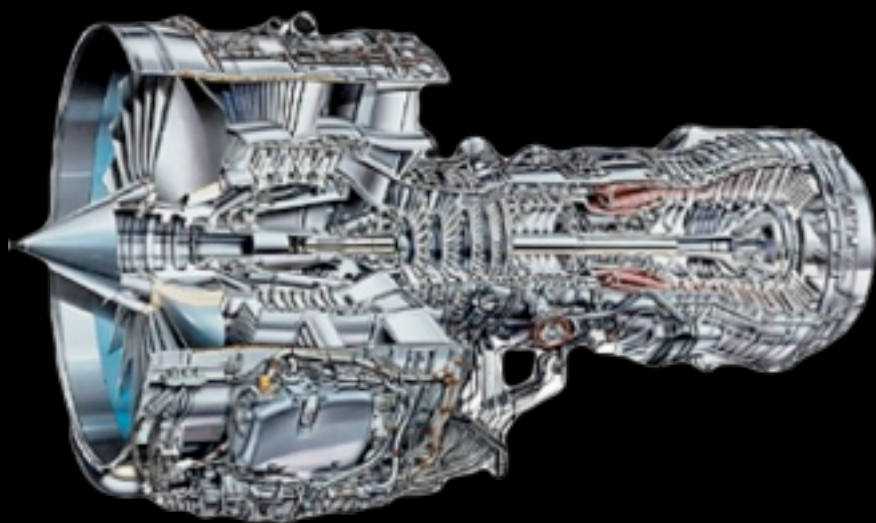
Where do we sit in the family of sciences?

**We're the Crazy Uncle
with tinfoil hat antennae
used to talk to the space
aliens of Regulus V, has
47 cats, and who too
frequently (but
benignly) forgets to
wear pants.**



Take, for example, CVSS

“the Base Equation multiplies
Impact by 0.6 and
Exploitability by 0.4”



Jet Engine X Peanut Butter = Shiny

“the Base Equation multiplies
Impact by 0.6 and
Exploitability by 0.4”

decimals aren't magic.

adding one
willy-nilly doesn't
suddenly
transform
ordinal rankings
into ratio values.



Financial Risk

Engineering Risk

another
problem

Complex (adaptive) Systems

a system
composed of
**interconnected
parts** that as a
whole exhibit one
or more
**properties not
obvious** from the
properties of the
individual parts



RCSA as commonly performed

Inherent risk - Controls = Residual Risk

RCSA as commonly performed

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low

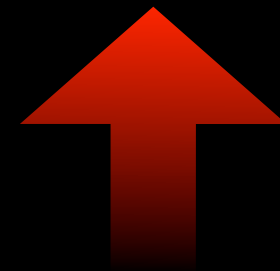
RCSA as commonly performed

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low



A Point Probability

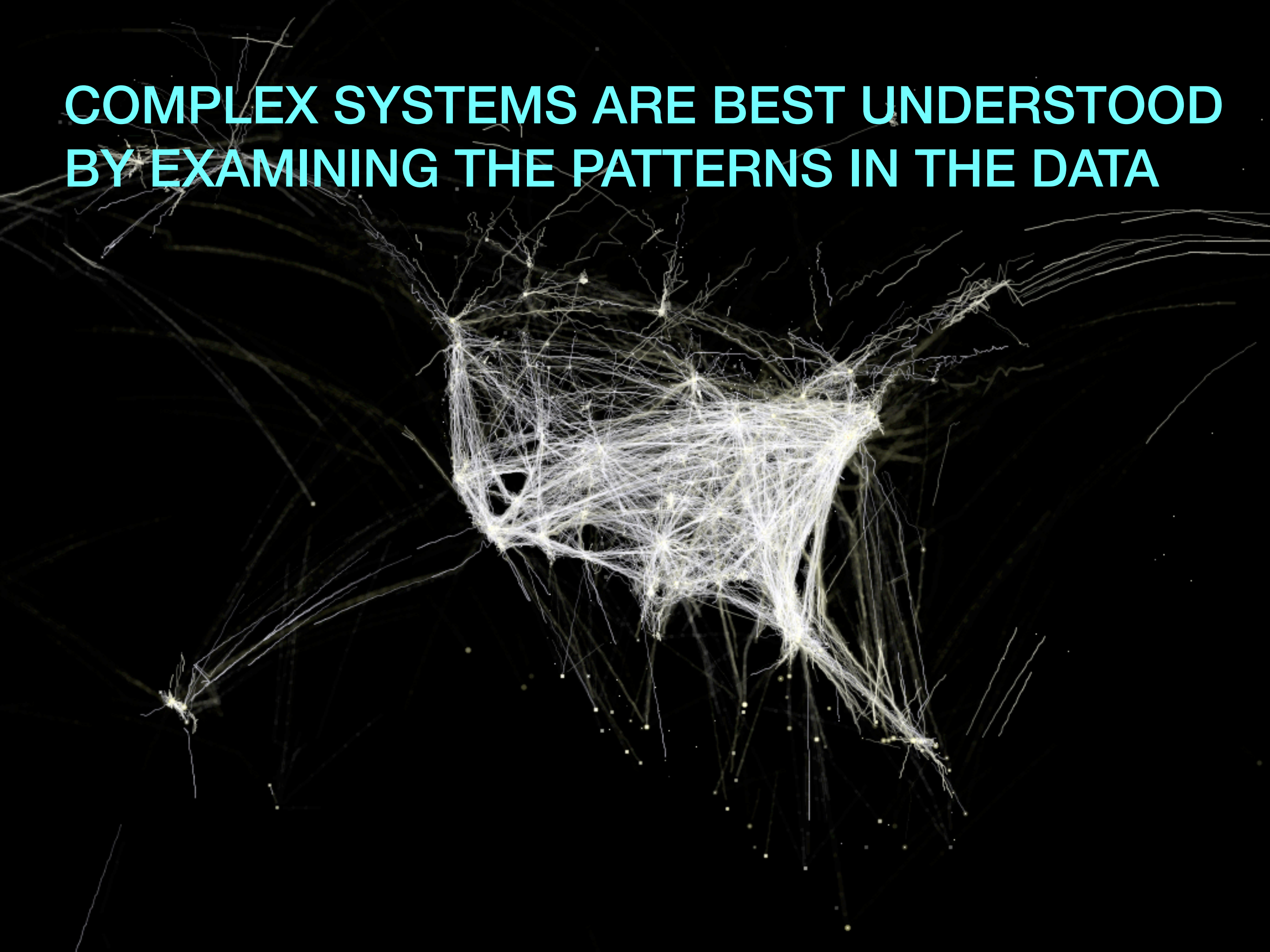
Friedrich Hayek Says:



**You're making
point
probabilities in
Complex
Systems?**

How Adorable!

**COMPLEX SYSTEMS ARE BEST UNDERSTOOD
BY EXAMINING THE PATTERNS IN THE DATA**



RCSA as commonly performed

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low

Much of (Engineering) Risk Management is a Cargo Cult

Much of (Engineering) Risk Management is a Cargo Cult



Financial Risk

Engineering Risk

must be
augmented with
something else

Financial Risk

Engineering Risk

Medical Risk

Financial Risk

Engineering Risk

Medical Risk (Criminology, too)

EPIDEMIOLOGY



EPIDEMIOLOGY

Risk Factors (Determinants)

Variables associated with increased frequency of event.

Risk Markers

Variable that is quantitatively associated with a disease or other outcome, but direct alteration of the risk marker does not necessarily alter the risk of the outcome.

Correlation vs. Causation

Risk factors or determinants are correlational and not necessarily causal, because correlation does not prove causation.



EPIDEMIOLOGY

Risk Factors (Determinants)

Variables associated with increased frequency of event.

Risk Markers

Variable that is quantitatively associated with a disease or outcome, but

direct alteration of the risk marker does not necessarily alter the risk of the outcome.

Correlation vs. Causation -

Risk factors or determinants are correlational and not necessarily causal, because correlation does not prove causation.

THE MEANS TO FIND PATTERNS



Medical Risk is designed to address
the problems we face in
understanding complex
systems

MEDICAL RISK & COMPLEX SYSTEMS FAILURE



**DR. RICHARD
COOK**

<http://www.ctlab.org/documents/How%20Complex%20Systems%20Fail.pdf>

Complex systems contain changing mixtures of failures latent within them.

The complexity of these systems makes it impossible for them to run without multiple **flaws** being present.

... individually insufficient to cause **failure**

...failures change constantly because of changing technology, work organization, and efforts to eradicate failures.

Complex systems run in degraded mode.

Risk is a characteristic of systems and not of their components

Risk is an emergent property of systems; it does not reside in a person, device or department of an organization or system.

... it is not a feature that is separate from the other components of the system.

...the state of **Risk** in any system is always dynamic

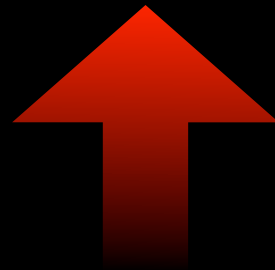
RCSA as commonly performed

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low



How awesome is your bridge?

We may want
to re-think our
approach to
risk & risk
management



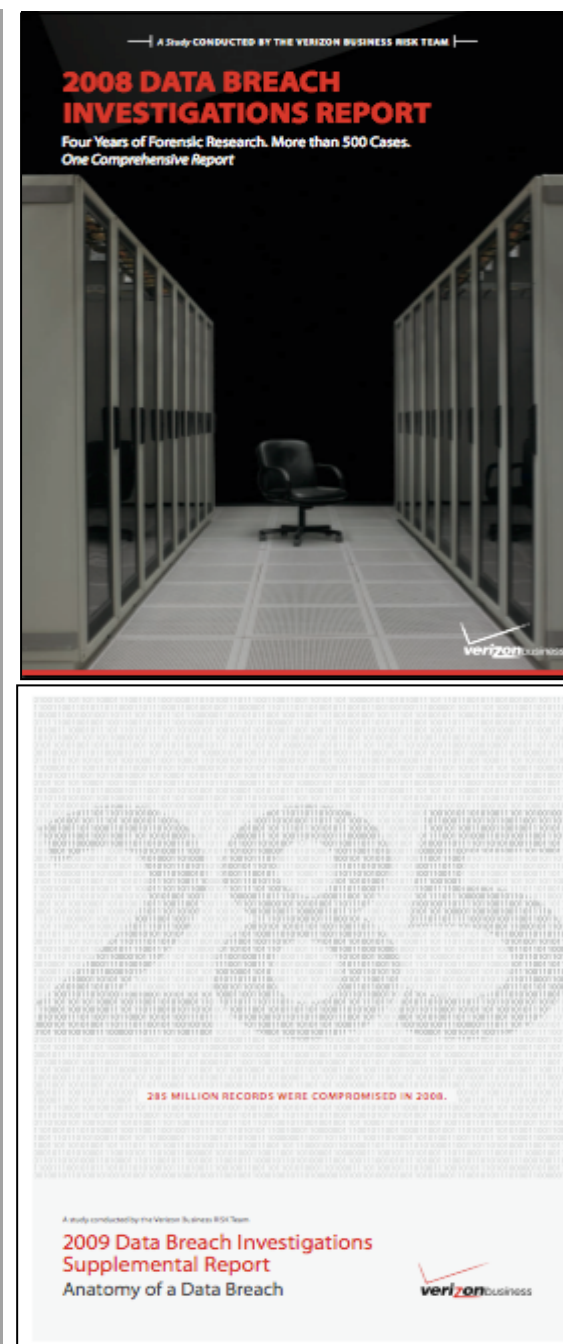
Serious Question: Can you imagine if your doctor operated in the same way we approach risk management?



Examples of “Medical Risk” in Information Technology

Data: Visible OPS for Security





Example of a medical approach:
Dr. Peter Tippet & Verizon DBIR

VERIS (Vocabulary for Event Recording & Incident Sharing)

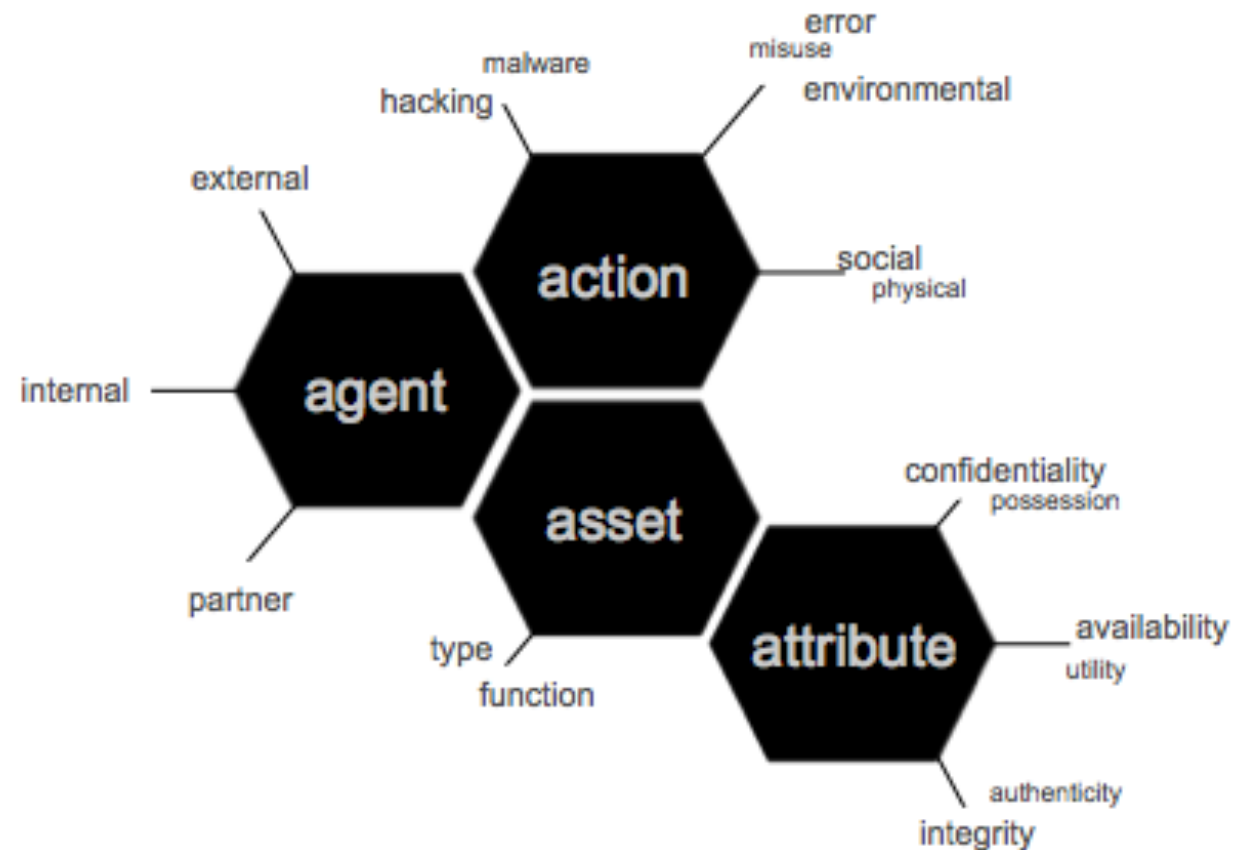
A security incident (or threat scenario) is modeled as a series of **events**. Every event is comprised of the following 4 **A's**:

Agent: Whose actions affected the asset

Action: What actions affected the asset

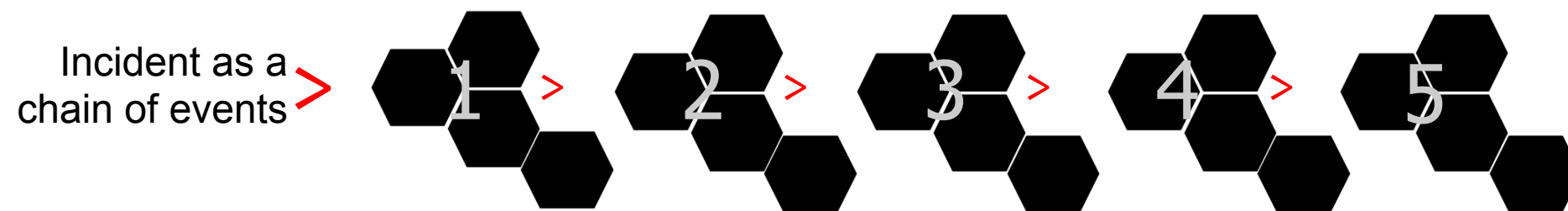
Asset: Which assets were affected

Attribute: How the asset was affected

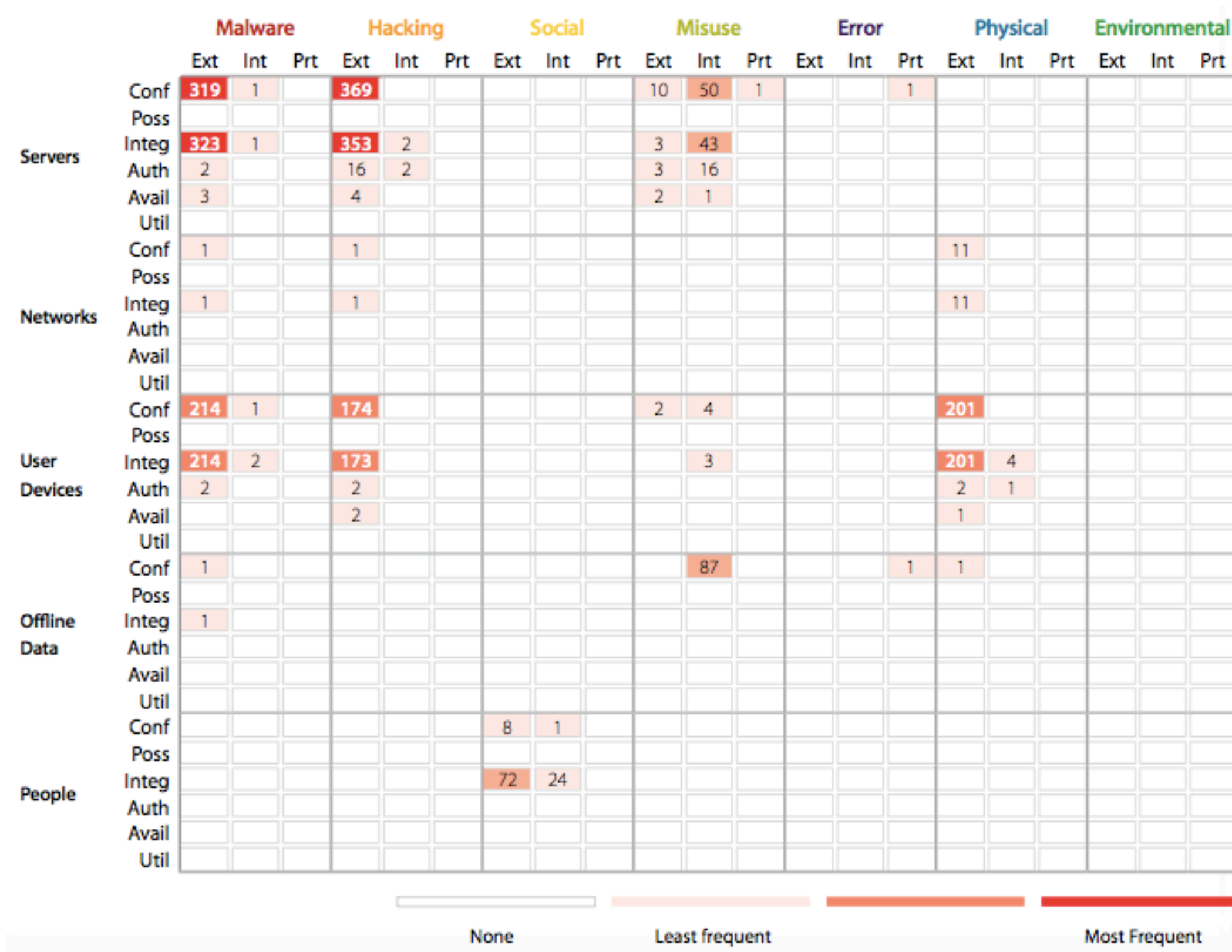


VERIS (Vocabulary for Event Recording & Incident Sharing)

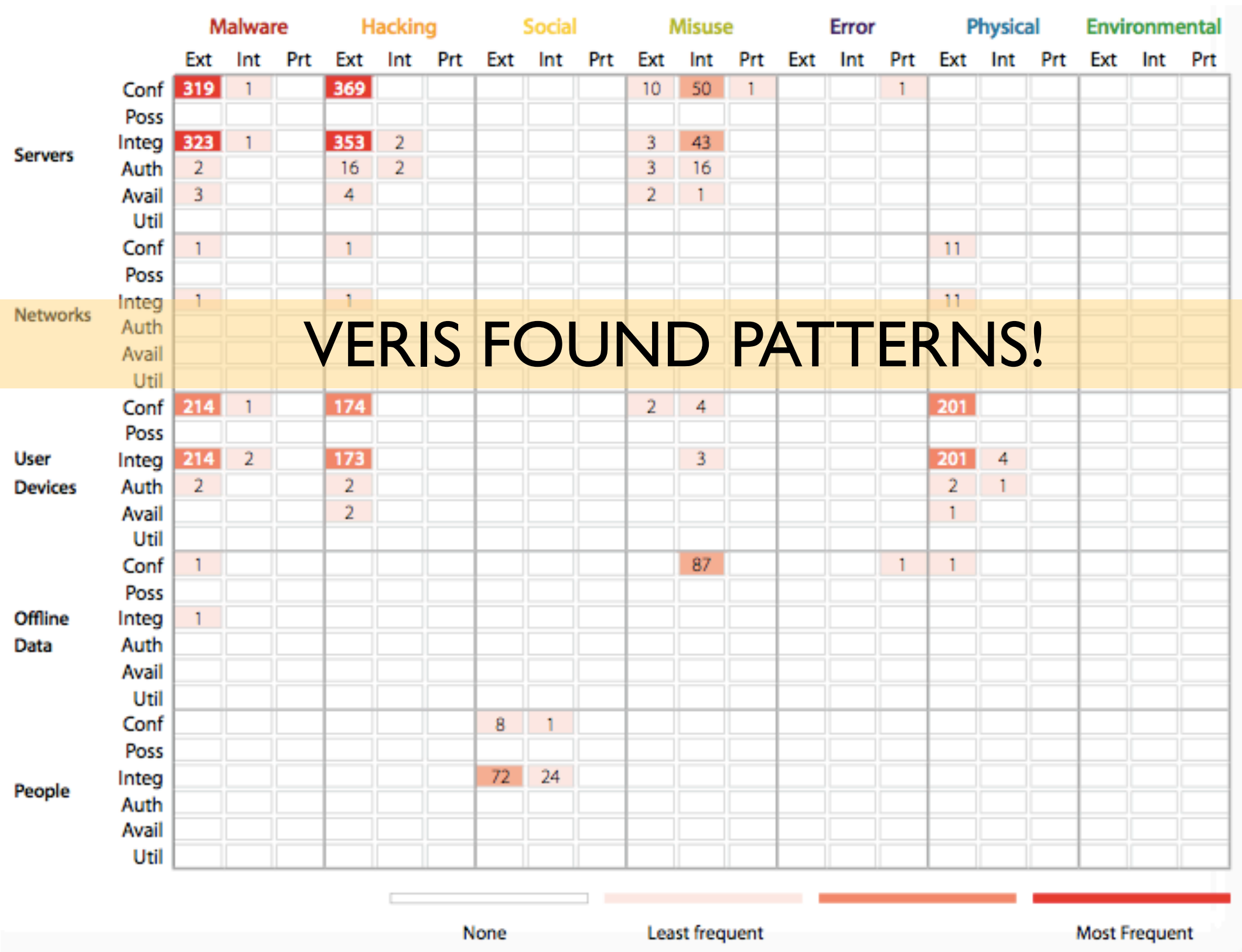
Object-Oriented Modeling



VERIS: Classification of Events by Risk Factor



Complex System?



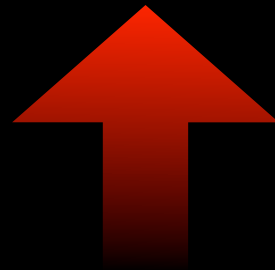
RCSA as commonly performed

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low



How awesome is your bridge?

The data says that **capability to manage** (not necessarily the breadth of controls) is the **key determinant**

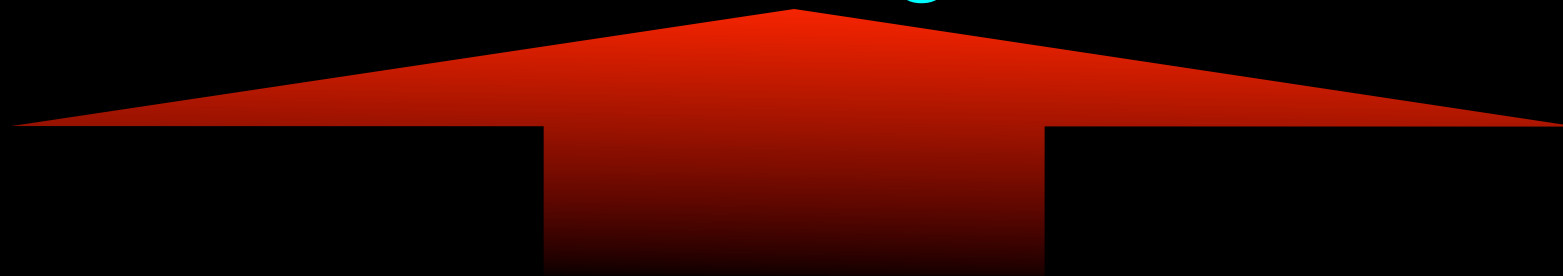
Evidence-Based Analysis

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low



How much are you associated with Failure?

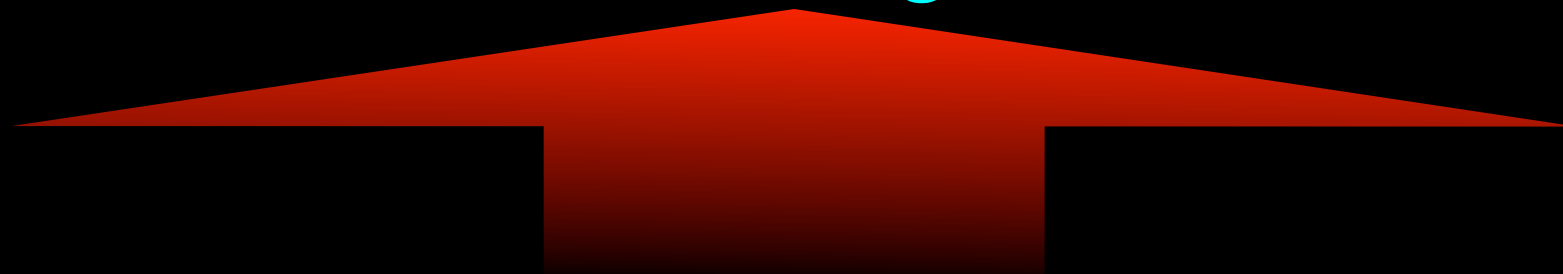
Evidence-Based Analysis

Inherent risk - Controls = Residual Risk

HIGH

Strong

Low



How GOOD is your lifestyle?



A hand holds a white rectangular sign against a background of green foliage. The sign has handwritten text in black and red ink. The text is arranged in four lines: 'WHAT DO WE WANT?' in black, 'EVIDENCE-BASED CHANGE' in red, 'WHEN DO WE WANT IT?' in black, and 'AFTER PEER REVIEW' in red. The sign is slightly wrinkled and the lighting is bright, casting shadows.

WHAT DO WE WANT?
EVIDENCE-BASED CHANGE
WHEN DO WE WANT IT?
AFTER PEER REVIEW

Shall we talk about change?

The Modern Approach to Risk Management

The Modern Approach to Risk Management: **A Manifesto**

The Modern Approach to Risk Management: **A Manifesto**

Premise: Risk Management must provide value, address the need, & be ethical.

The Modern Approach to Risk Management: **A Manifesto**

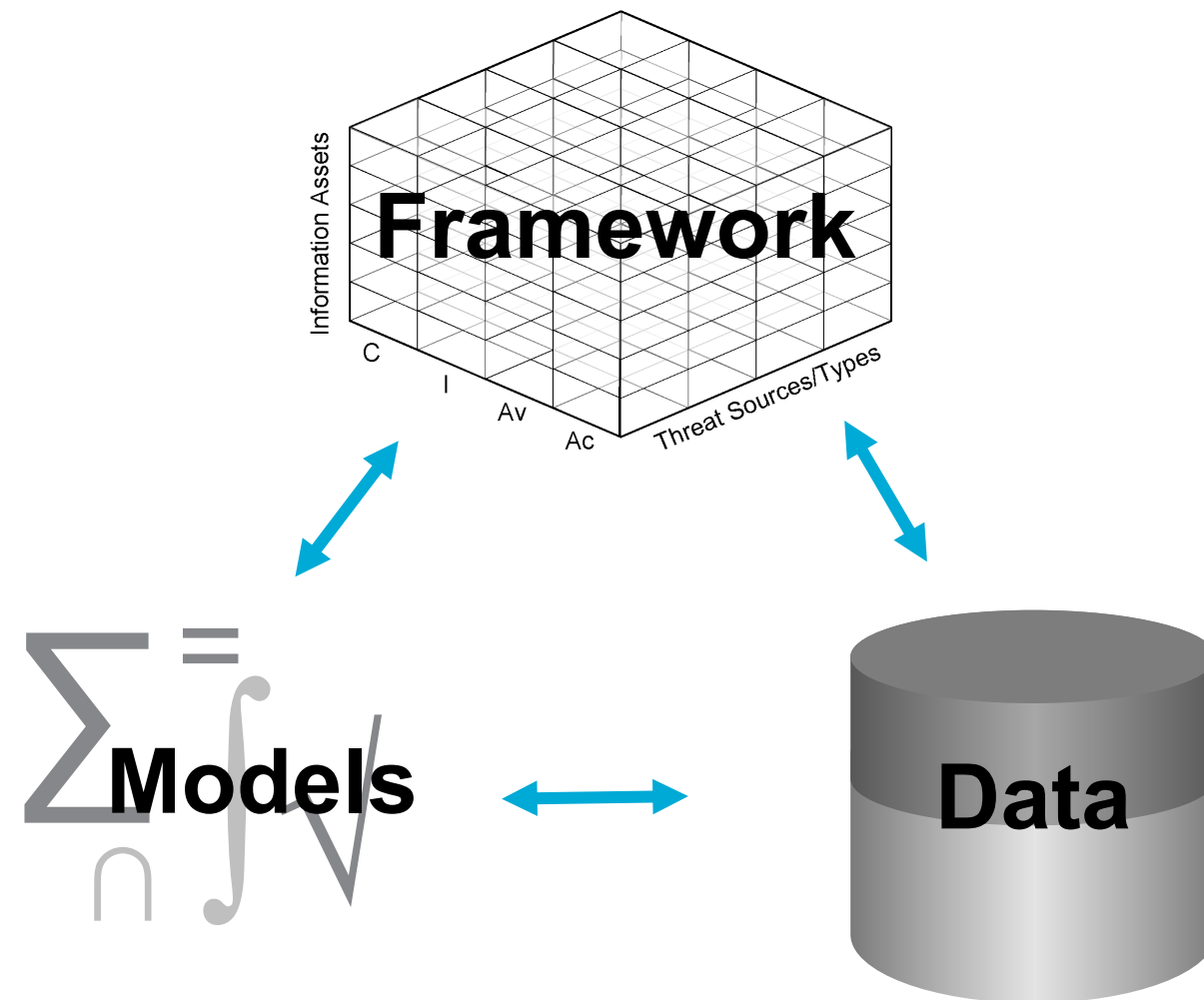
Clause One: To be ethical, the risk manager must be, first and foremost, a data scientist.

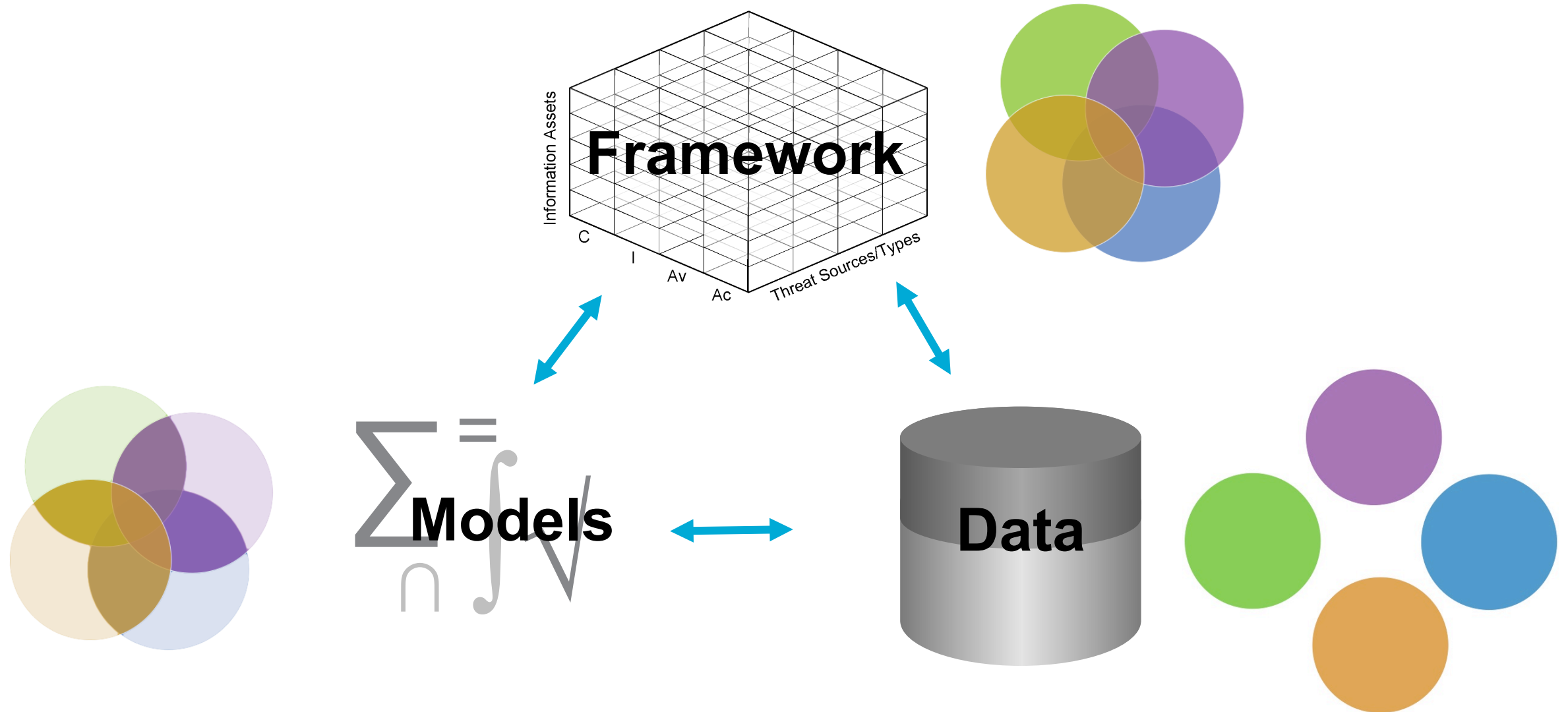
Statistics & Probability Ryan Gosling Says:



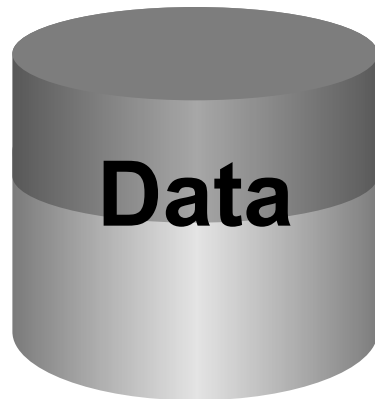
What to study: Sources of Knowledge







We quickly figured out:



We quickly figured out:

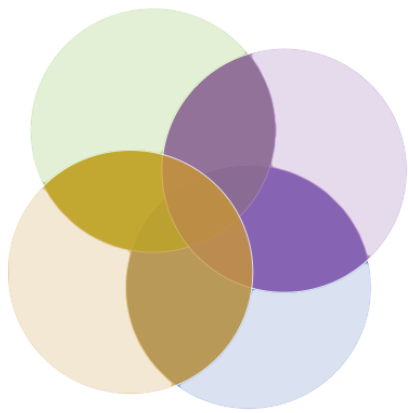
1.) The means to address the system must be data-driven, and



We quickly figured out:

1.) The means to address the system must be data-driven, and

2.) We must study the individual parts,



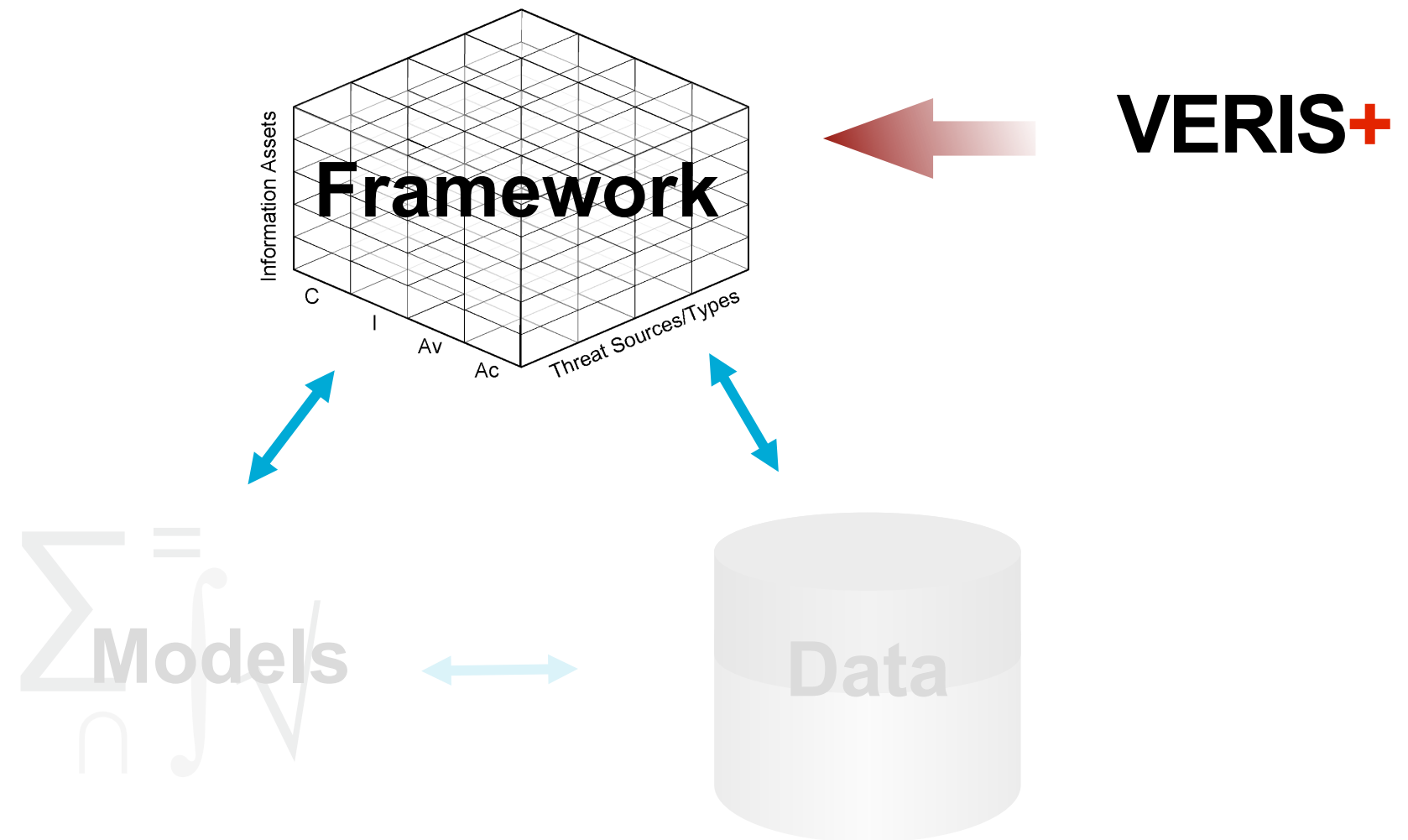
We quickly figured out:

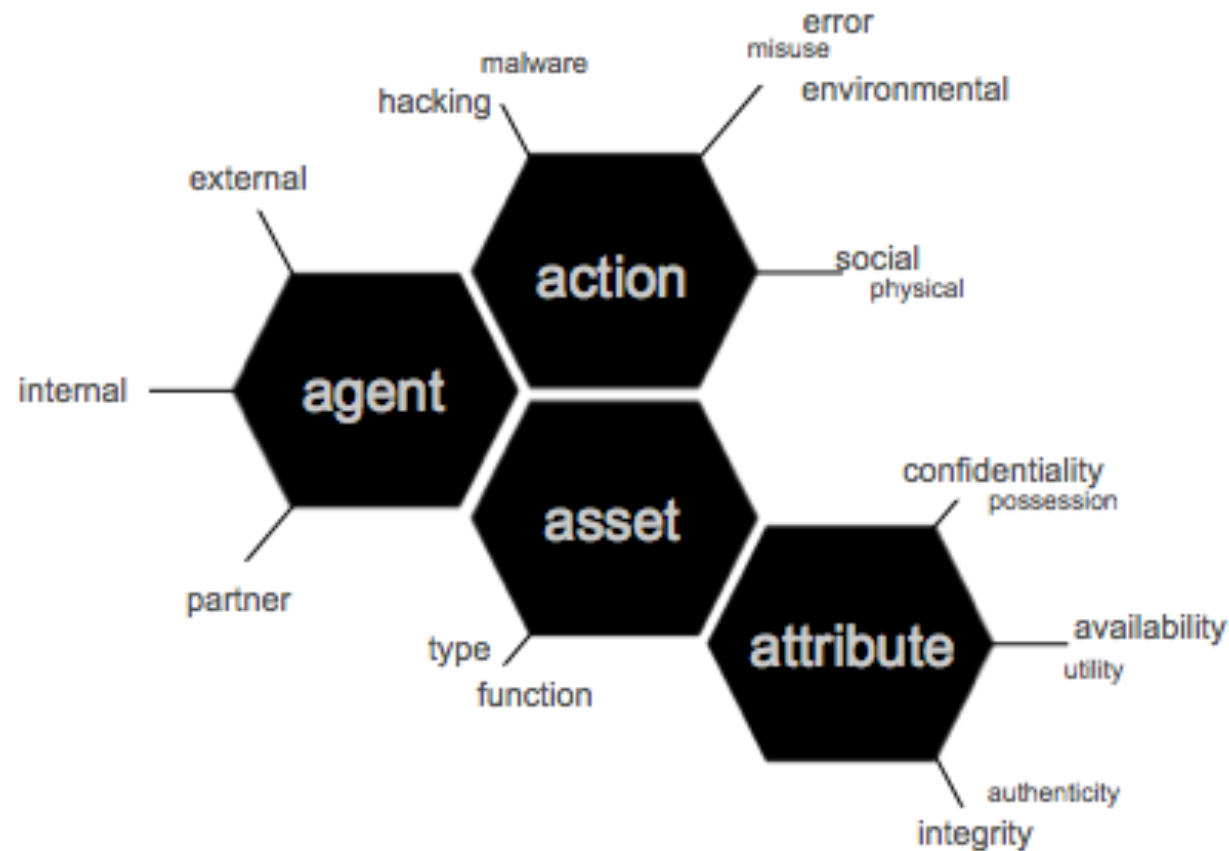
- 1.) The means to address the system must be data-driven, and
- 2.) We must study the individual parts, then the relationships between parts



We quickly figured out:

- 1.) The means to address the system must be data-driven, and
- 2.) We must study the individual parts, then the relationships between parts, then and only then we can discuss the whole





VERIS WILL ALLOW US TO:

- 1.) Describe the elements of banking operations (using Basel-esque high level categorization)
- 2.) Fully categorize whatever we're looking at
- 3.) Collect data in a same to same fashion

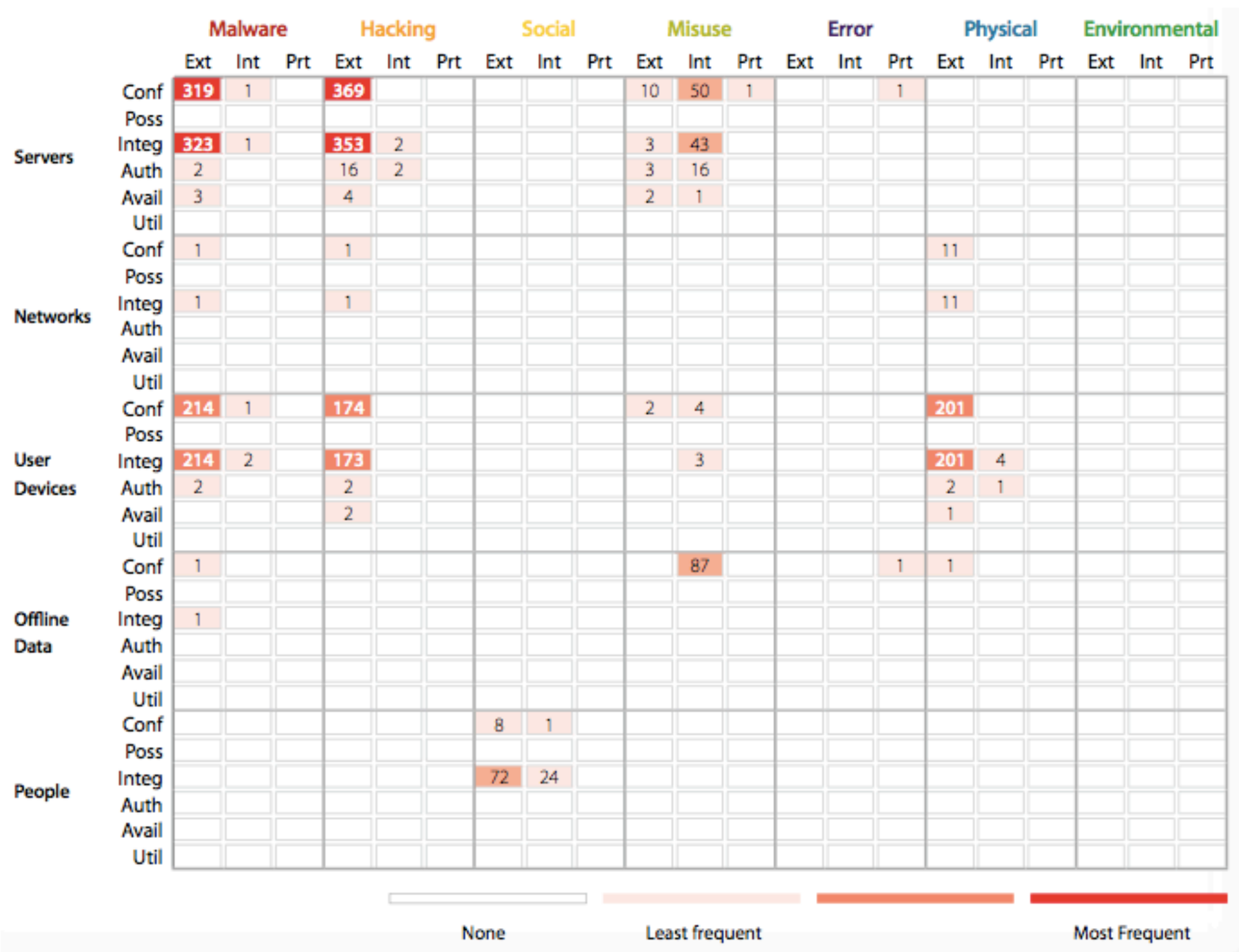


We quickly figured out:

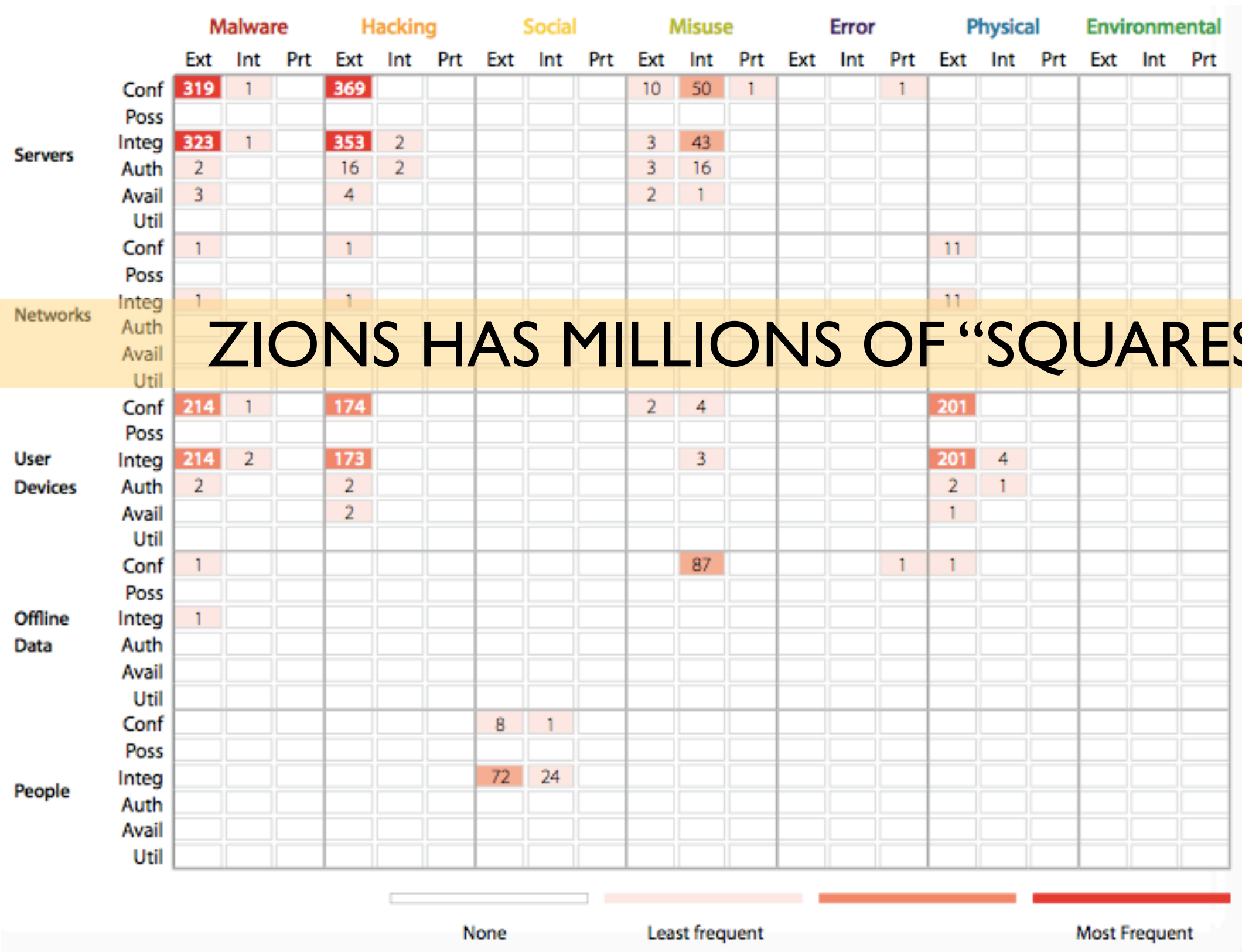
- 1.) The means to address the system must be data-driven, and
- 2.) We must study the individual parts, then the relationships between parts before we can discuss the whole, and
- 3.) We're looking at a **boat-load** of data.

How big is a boat-load?

How big is a boat-load?



How big is a boat-load?



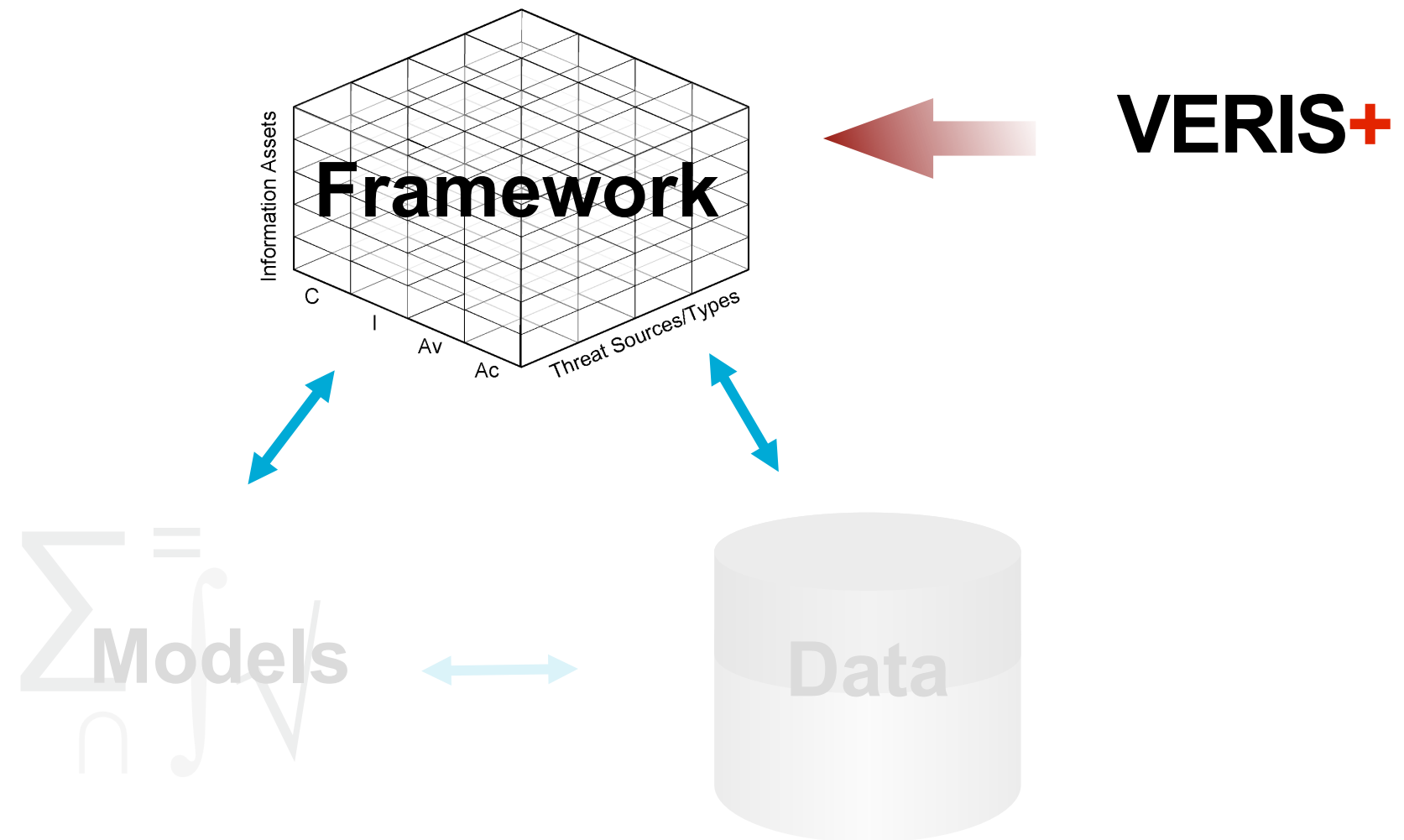
ZIONS HAS MILLIONS OF “SQUARES”



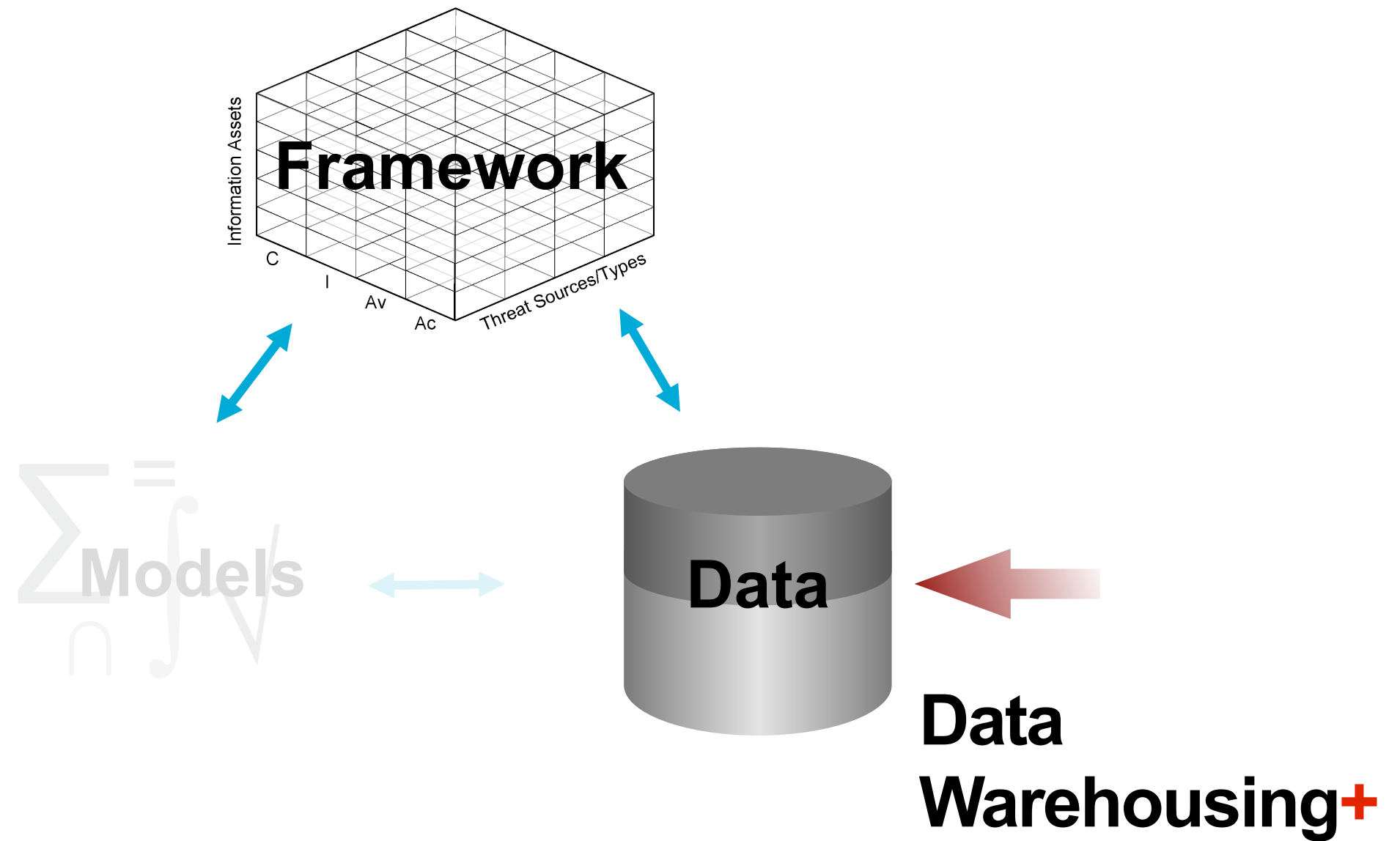
We're going to need a bigger boat

Security Data Warehousing

How will we deal with a boat-load?



How will we deal with a boat-load?



How will we deal with a boat-load?



How will we deal with a boat-load?



Data

Threat Intel Feeds
Control Data
Control Logs
System Logs

Event History & Loss
Loss Distribution Dev.
B.I.A.

Control Data
Control Logs
System Logs

Configuration Data
Vulnerability Data
HR Information
Process Behaviors

MapReduce Process



XML
CSV
EDI
LOG
SQL
JSON
Text
Binary
Objects

create map

reduce

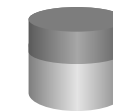


Analytics & Reporting

Rapid Access
Database
Systems



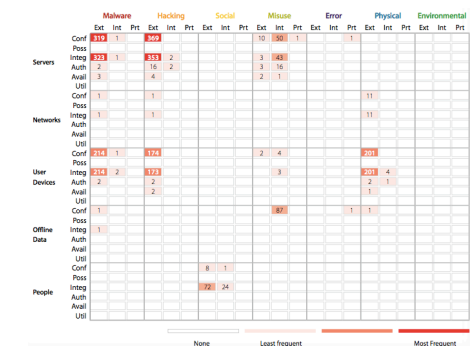
Workflow



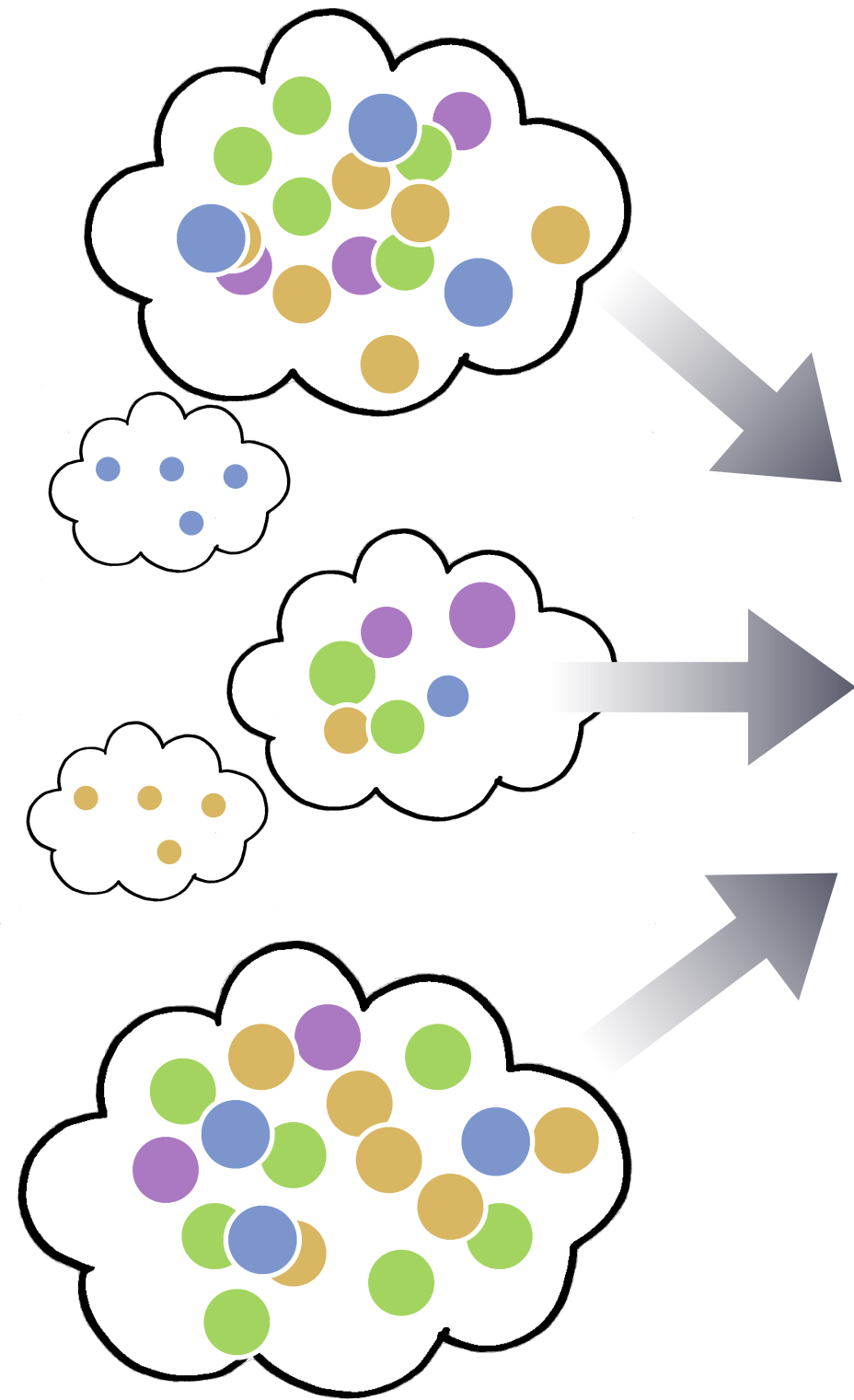
Analytics



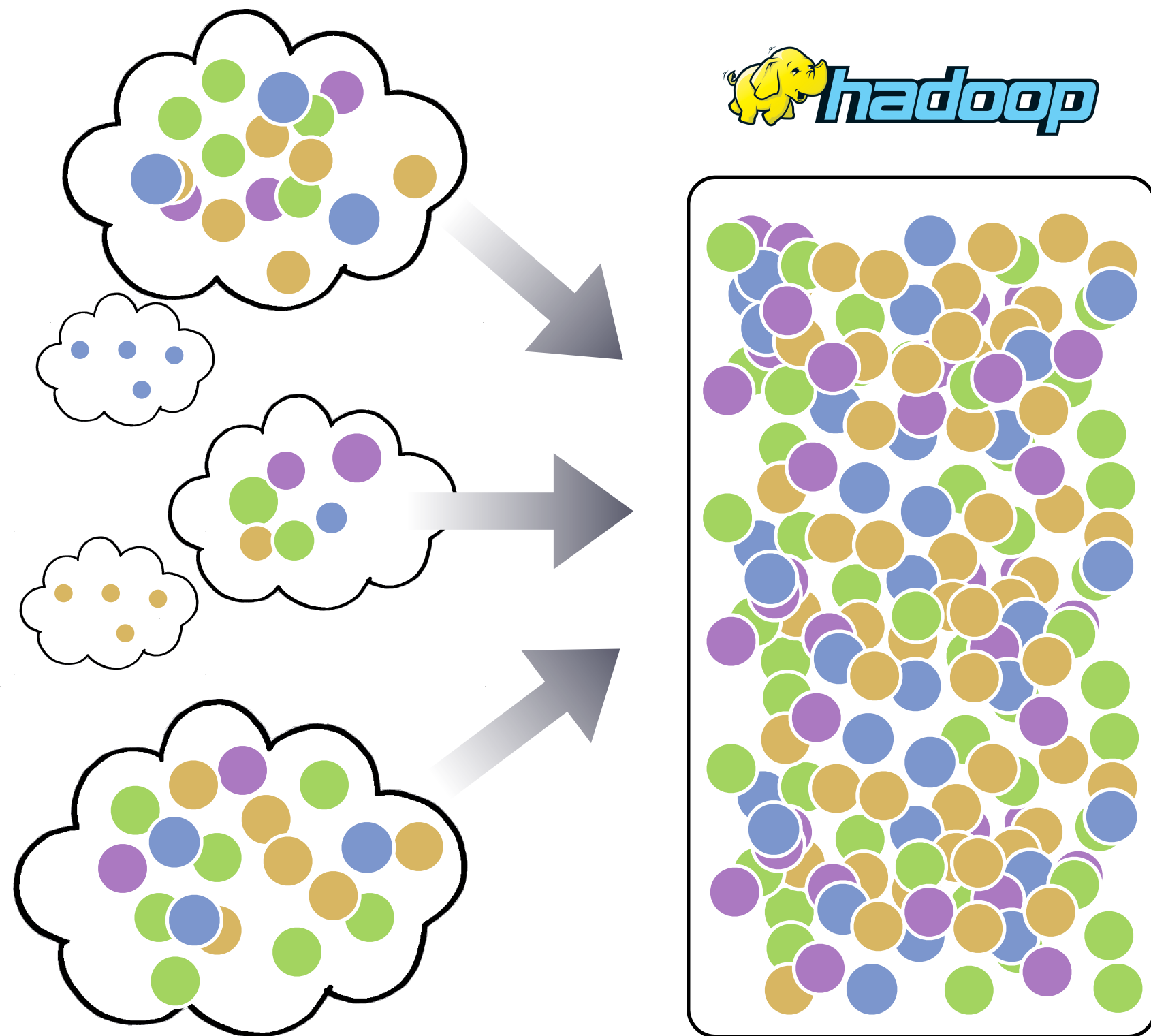
Reporting



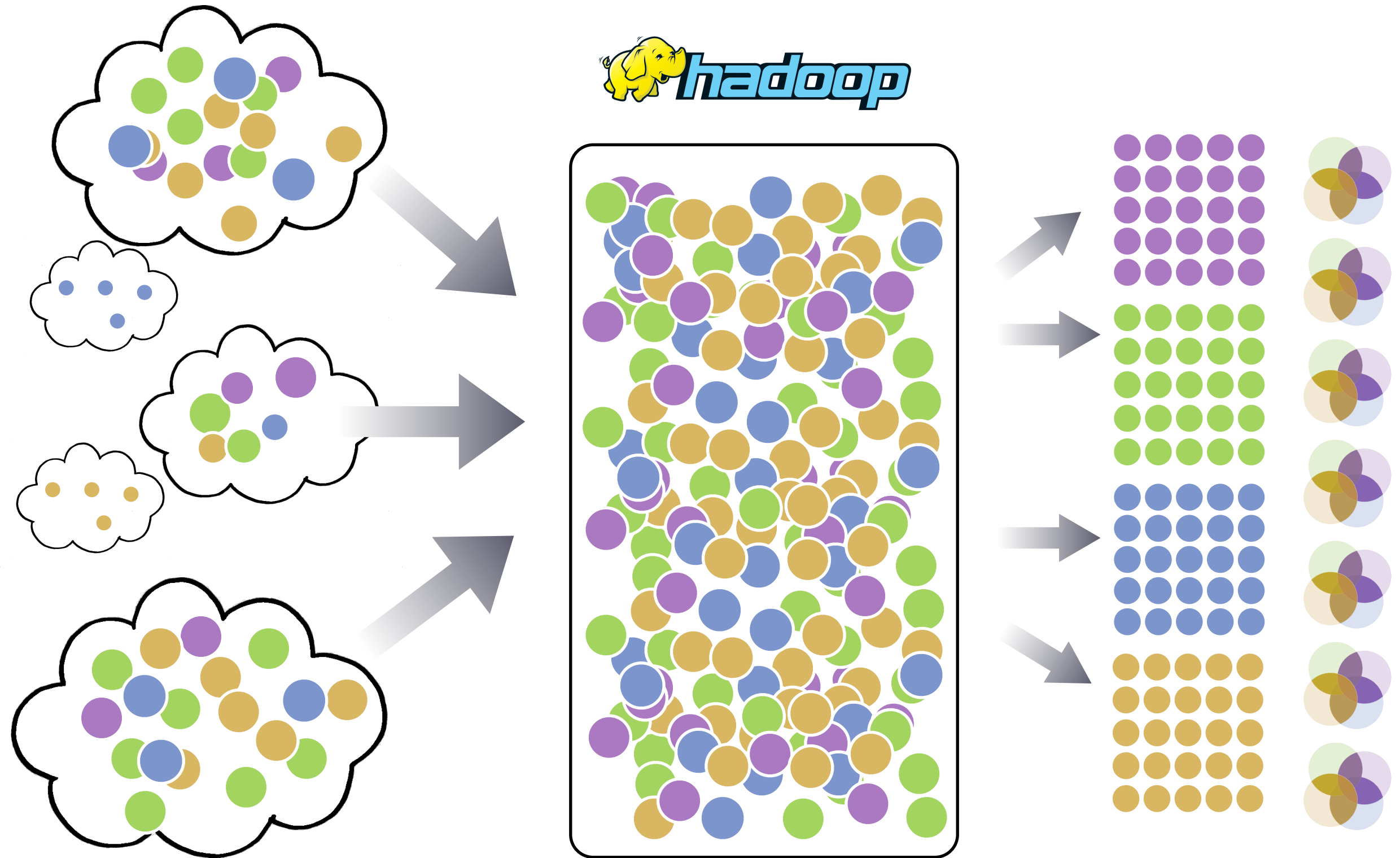
How will we deal with a boat-load?



How will we deal with a boat-load?

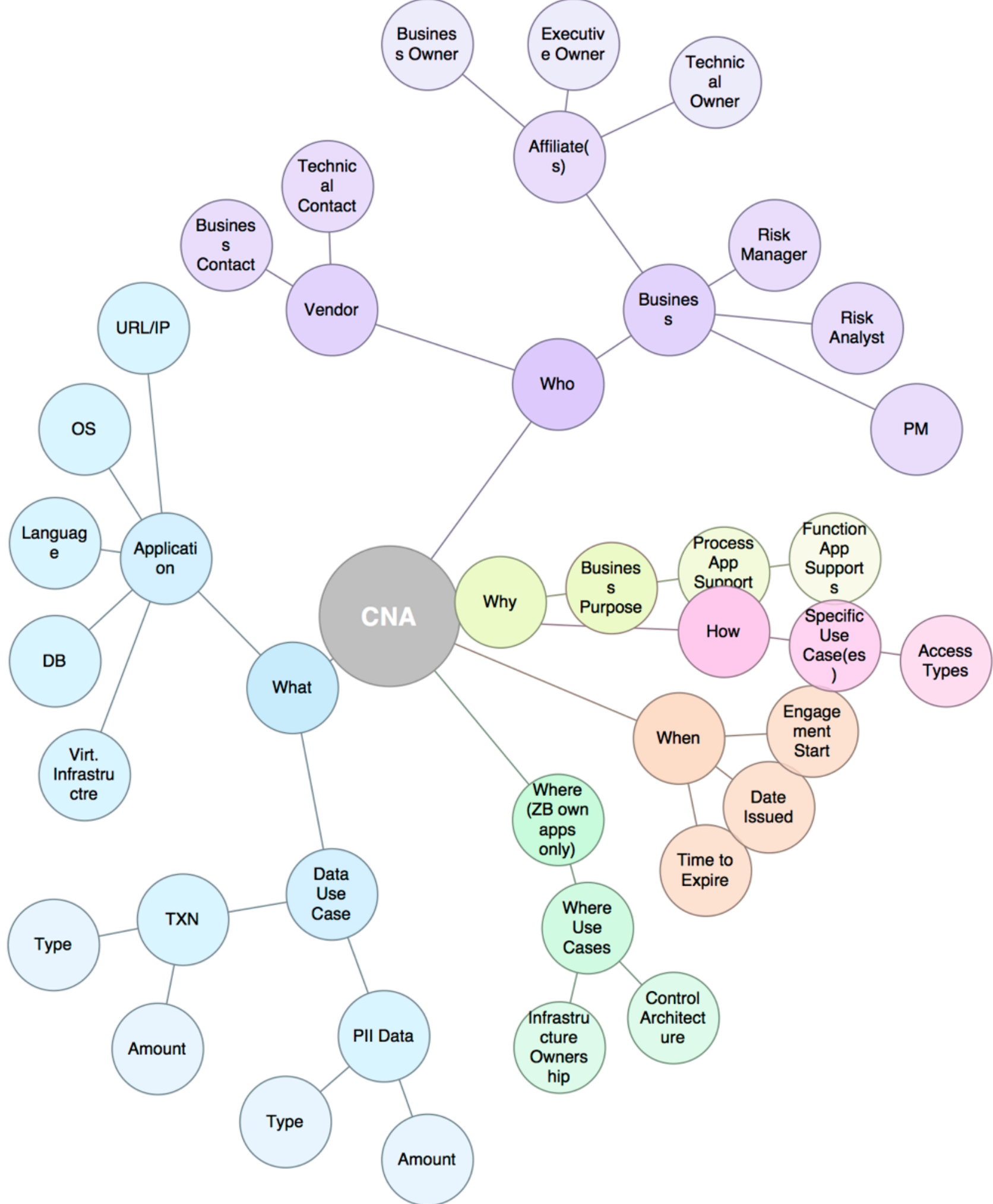


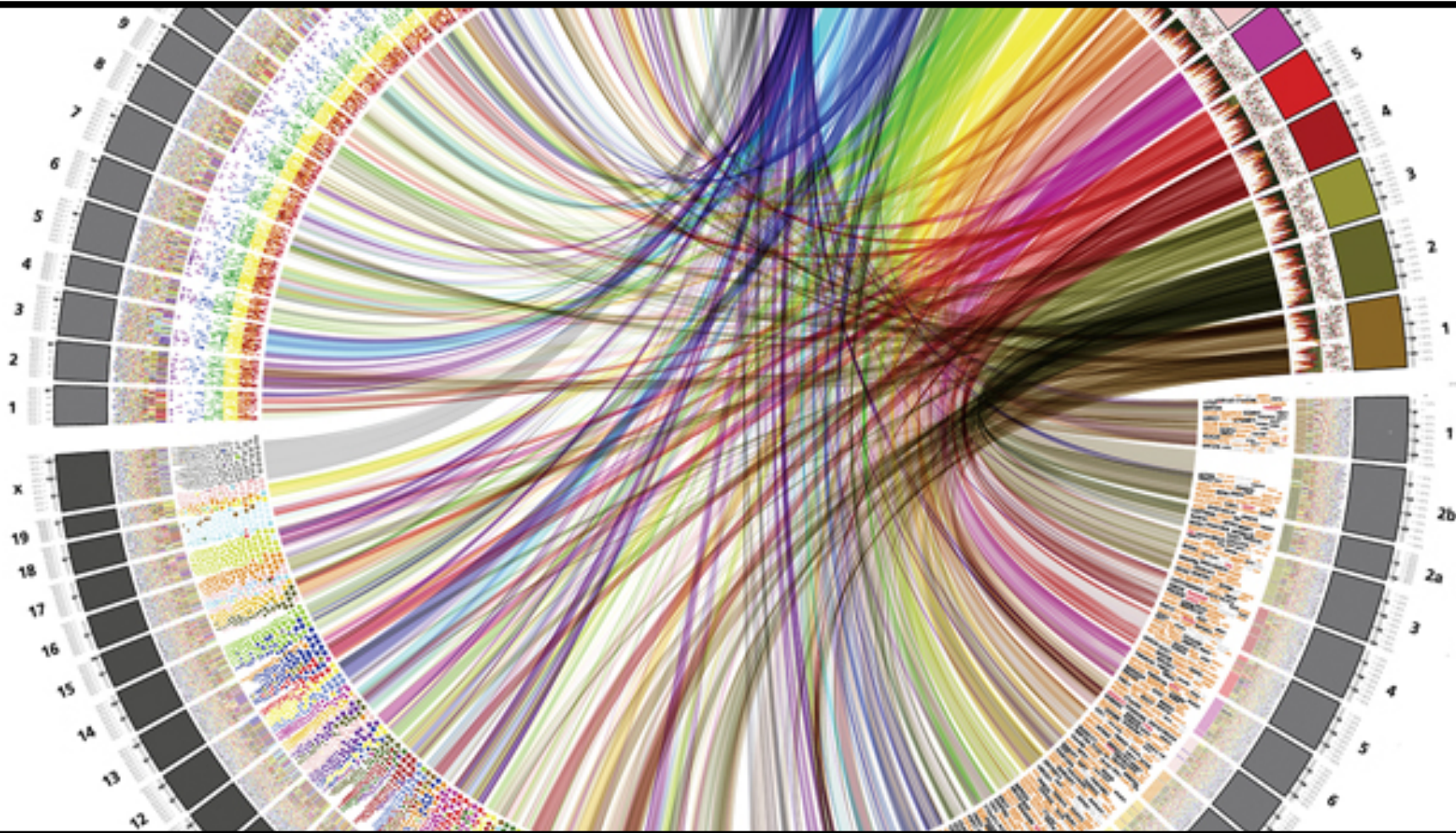
How will we deal with a boat-load?



Example:

Vendor-owned
SaaS
application





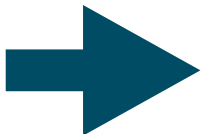
Genomic sequencing
for operational risk

The Modern Approach to Risk Management: **A Manifesto**

Clause 2: To provide value the modern approach has to support counter-threat operations.

data in

new input from any source

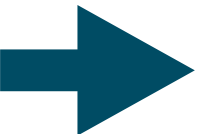


being proactive here will mean identifying regular, recurring sources and setting up processes.

categorized

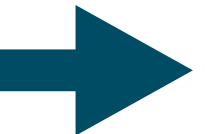
And is then categorized in TOPS Op Risk Categories

- financial reporting
- technology
- financial crime /
- regulatory / legal
- business continuity
- people
- vendor management
- operations
- customer treatment



classified

belongs to one of the following basic classifications of data: intelligence, scenario development request, incident information, issue management



TRM will have to come up with the taxonomies on the left for each of the categories on the right. VERIS is probably 60-75% of what we need.

broken into elements

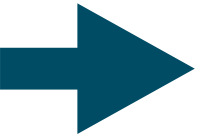
the analyst then identifies the following elements relevant to each data object per the selected categories taxonomy of:

- agent
- action
- asset
- attribute/Loss
- controls



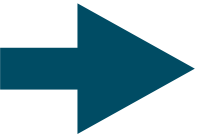
Processed

As a historical incident, scenario, or KRI



Modeled

Given meaning through model of scenario, added or modifying KRIs, or added to historical register.



Reported

Output is either back to the input when they've requested development, or reported in a regular report/ dashboard/ scorecard

the right tool here will make it easy to slice and dice reports and "auto-update."

Risk Management is
an intelligence function

duh.

3 types of intel functions for Operational Risk

Type of Intel	Real Time	Tactical	Strategic
Audience	(counter threat operations)	(Security Operations)	(Security & Executive Management)
Risk's Role	low	medium	high
Main Information Types	asset (TO focuses on threat)	asset, threat, control	time, money
Tools	controls, hadoop, storm, kafka, hive, dremel, drill	controls, hadoop, hive, R	Hadoop, R

3 types of intel functions for Operational Risk

Type of Intel	Real Time	Tactical	Strategic
Audience	(counter threat operations)	(Security Operations)	(Security & Executive Management)
Risk's Role	low	medium	high
Main Information Types	asset (TO focuses on threat)	asset, threat, control	time, money
Tools	controls, hadoop, storm, kafka, hive, dremel, drill	controls, hadoop, hive, R	Hadoop, R

3 types of intel functions for Operational Risk

Type of Intel	Real Time	Tactical	Strategic
Audience	(counter threat operations)	(Security Operations)	(Security & Executive Management)
Risk's Role	low	medium	high
Main Information Types	asset (TO focuses on threat)	asset, threat, control	time, money
Tools	controls, hadoop, storm, kafka, hive, dremel, drill	controls, hadoop, hive, R	Hadoop, R

3 types of intel functions for Operational Risk

Type of Intel	Real Time	Tactical	Strategic
Audience	(counter threat operations)	(Security Operations)	(Security & Executive Management)
Risk's Role	low	medium	high
Main Information Types	asset (TO focuses on threat)	asset, threat, control	time, money
Tools	controls, hadoop, storm, kafka, hive, dremel, drill	controls, hadoop, hive, R	Hadoop, R

How will we deal with a boat-load?



Data

MapReduce Process



Analytics & Reporting

Threat Intel Feeds
Control Data
Control Logs
System Logs

Event History & Loss
Loss Distribution Dev.
B.I.A.

Control Data
Control Logs
System Logs

Configuration Data
Vulnerability Data
HR Information
Process Behaviors

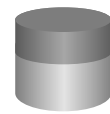
XML
CSV
EDI
LOG
SQL
JSON
Text
Binary
Objects

create map

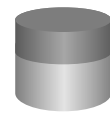
reduce



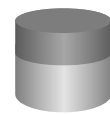
Traditional
RDBMS
Systems



Workflow



Analytics



Reporting

		Malware		Hacking		Social		Misuse		Error		Physical		Environmental	
		Ext	Int	Ext	Int	Ext	Int	Ext	Int	Ext	Int	Ext	Int	Ext	Int
Servers	Conf	114	1	144				10	10	1					
	Post	114	1	113	2			3	143						
	Auth	1	1	16	2			3	16						
	Util	3		4				2	1						
	Conf	1		1								11			
Networks	Post	1		1								11			
	Auth														
	Util														
	Conf	214	1	124				2	4			214			
	Post	214	2	123				3				214	4		
User Devices	Auth	2		2								2	1		
	Util			2								1			
	Conf	1						14				1	1		
	Post														
	Auth														
Office Data	Post														
	Auth														
	Util														
	Conf														
	Post														
People	Integ														
	Auth														
	Util														
	Conf														
	Post														

FEEDBACK LOOPS

The primary control of
the future might just be
the combination of
behavioral analytics and
machine learning

**BIG DATA IS NOT THE
SOLUTION!**

Data Science is.

Example of current
success

Internal employee behaviors

systems connecting	(tactical, real time)
time of connection	(real time)
riskiest cost center	(strategic)

The Modern Approach to Risk Management: **A Manifesto**

Clause 3: To address the need the modern approach has support rational decision making.

**Rational Decision Making
requires multiple models,
multiple perspectives.**

Scenario Analysis: FAIR

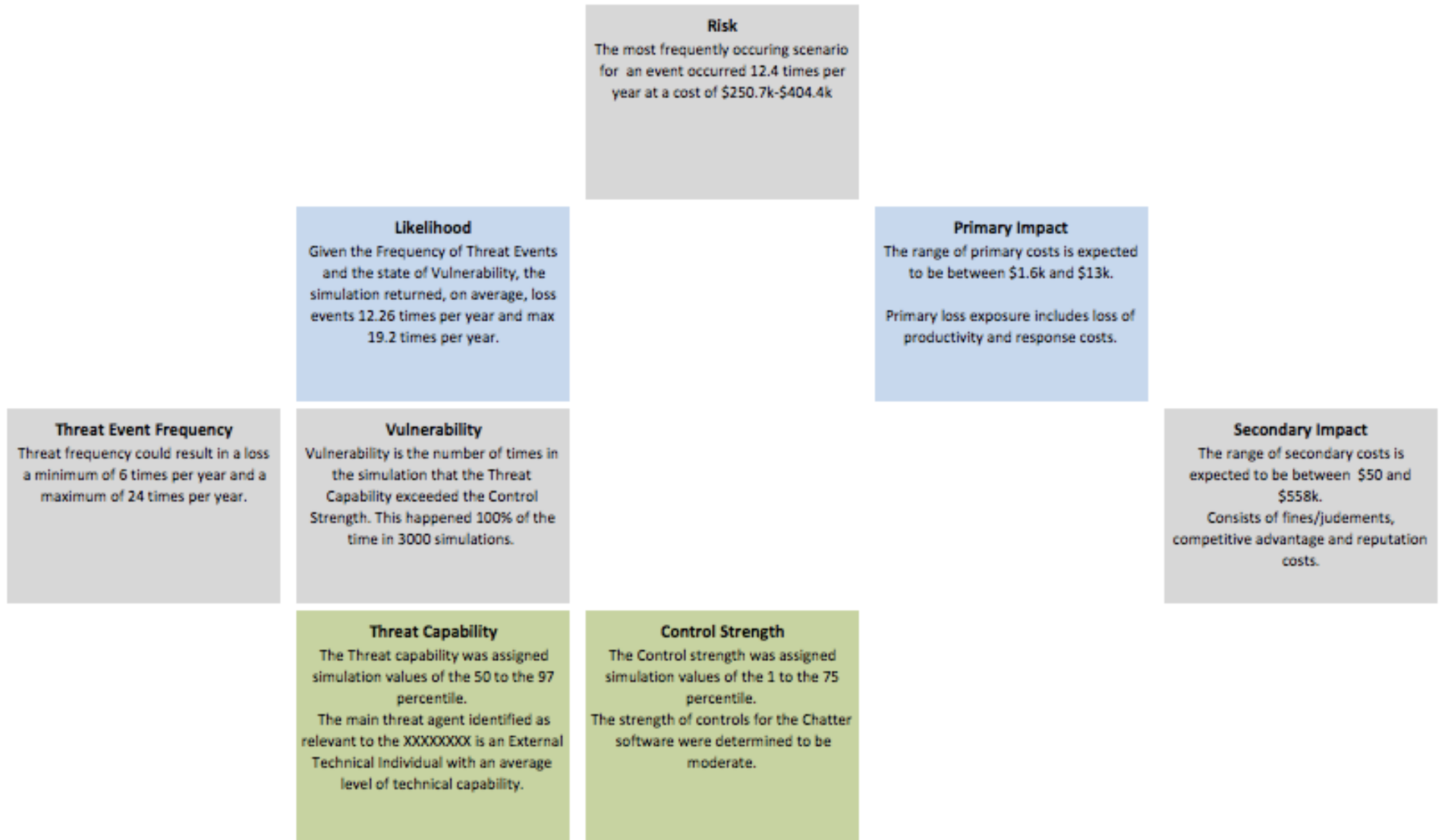
State Analysis: Homebrew

**Rational Decision Making
requires multiple models,
multiple perspectives.**

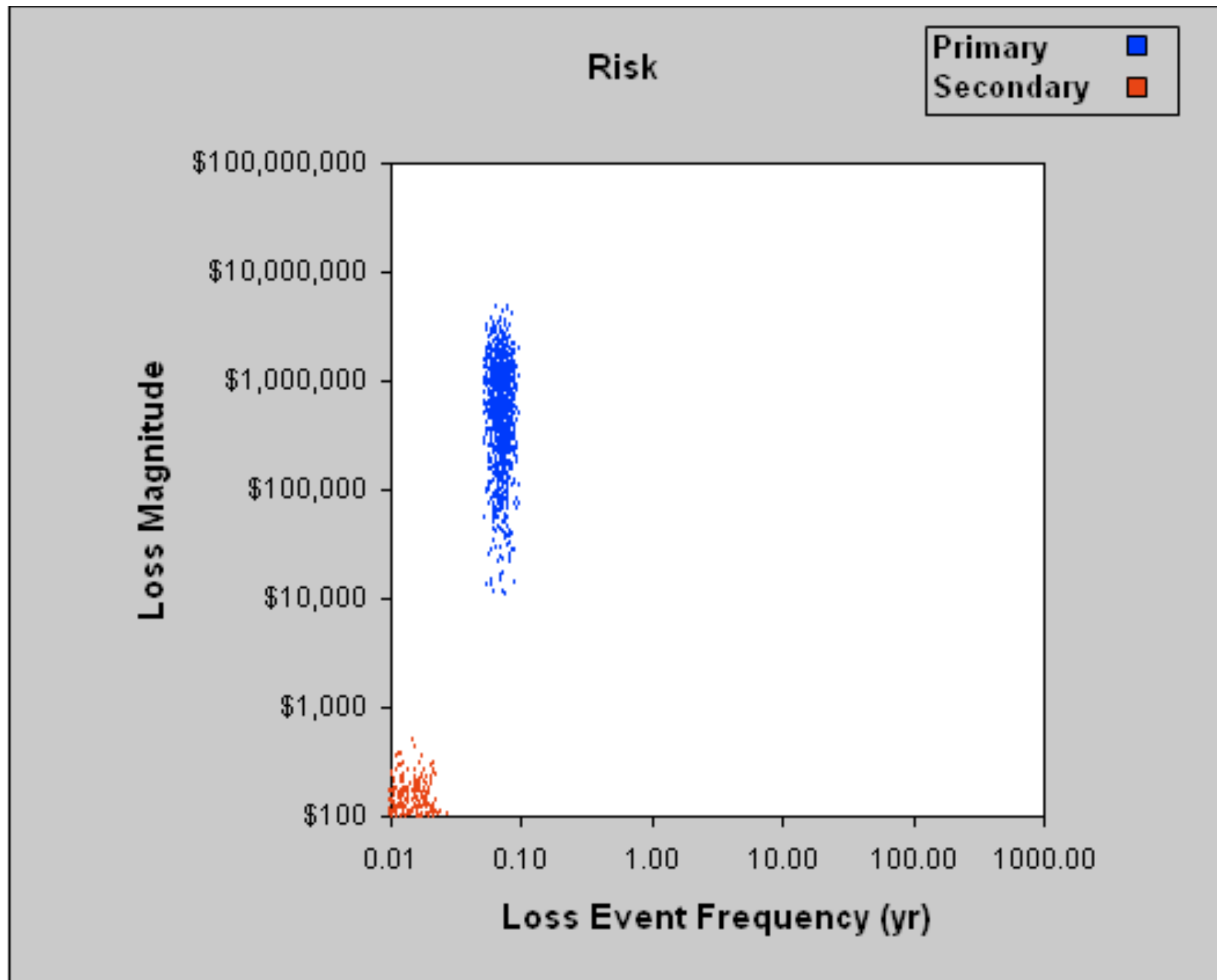
Scenario Analysis: FAIR
(how much risk do I have)

State Analysis:
(how well am I living)

FAIR Analysis



FAIR Analysis



FAIR Analysis

Impact

The maximum loss magnitude is \$404.4k. The most likely loss magnitude is \$226.7k.

These costs estimates include the time required to perform incident response and lost productivity, losses covering fines and judgements, as well as costs associated with customer notification and credit monitoring.

Likelihood

The likelihood of an event may occur, on average, 12.26 times per year, with a maximum occurrence of 19.2 times per year.

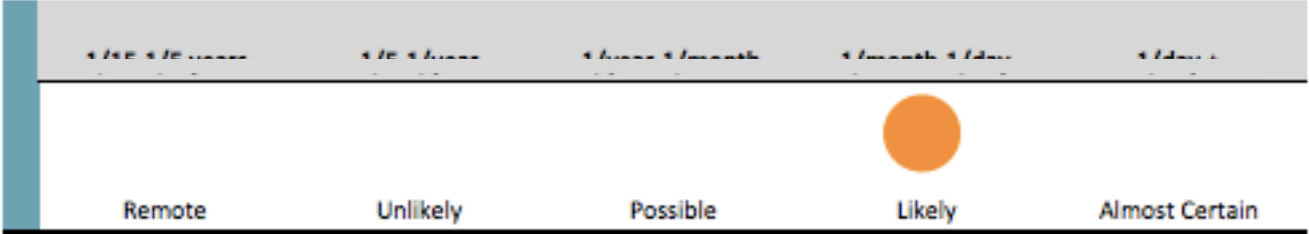
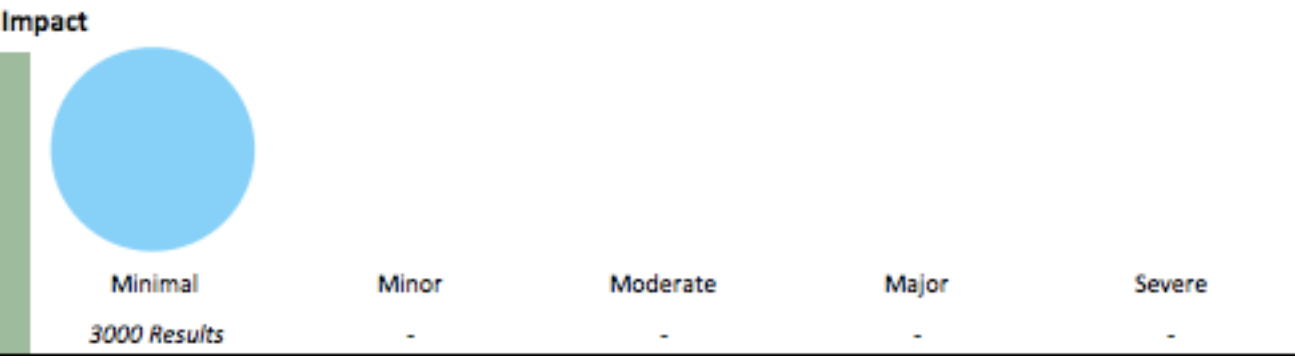
The simulation shows the event is likely to occur monthly. This is a fairly high frequency event due to the lack of controls preventing external attacks and the relatively low level of expertise required to initiate an attack.

Risk

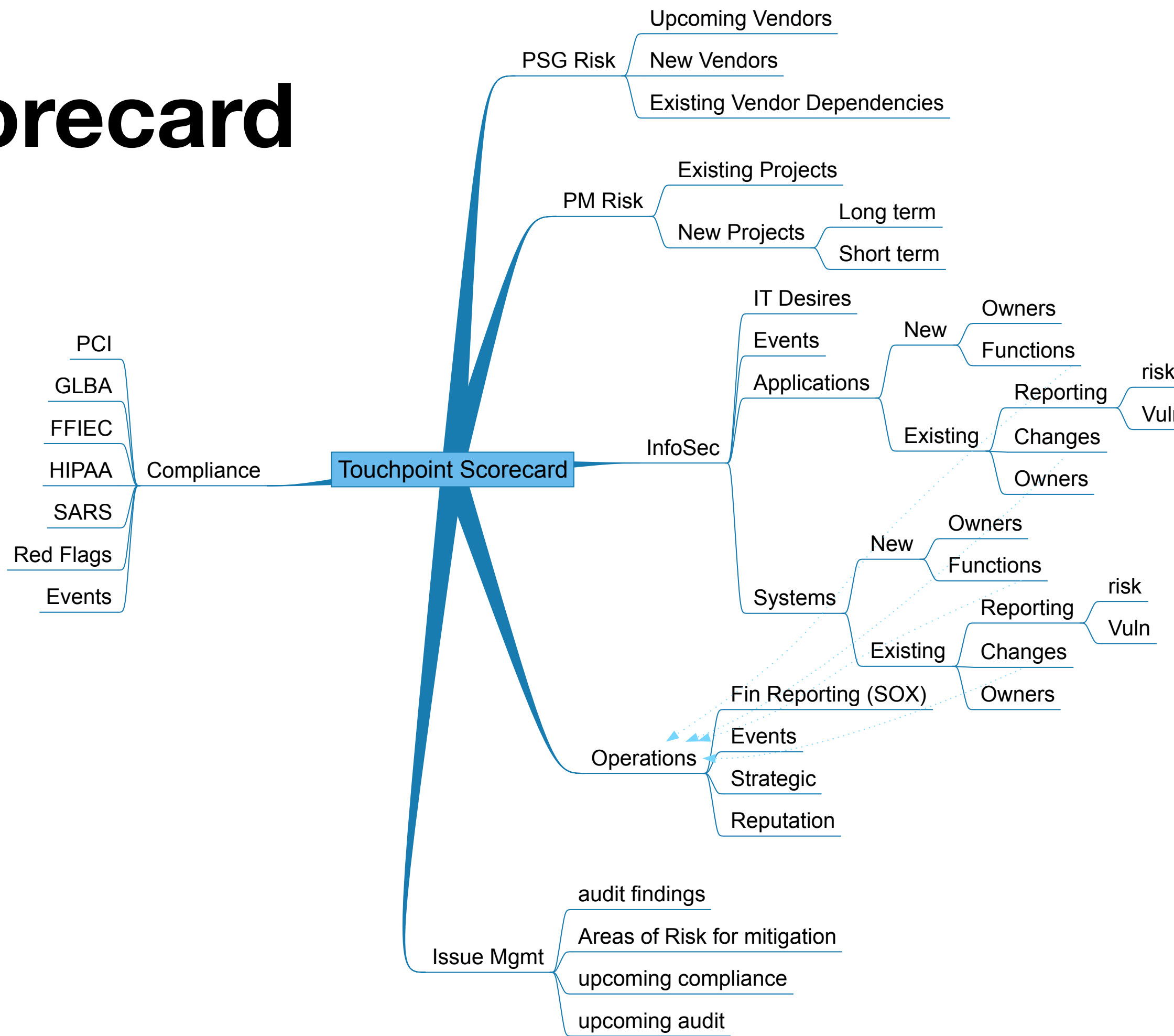
Likelihood x Impact = **Moderate**

Residual Risk Determination

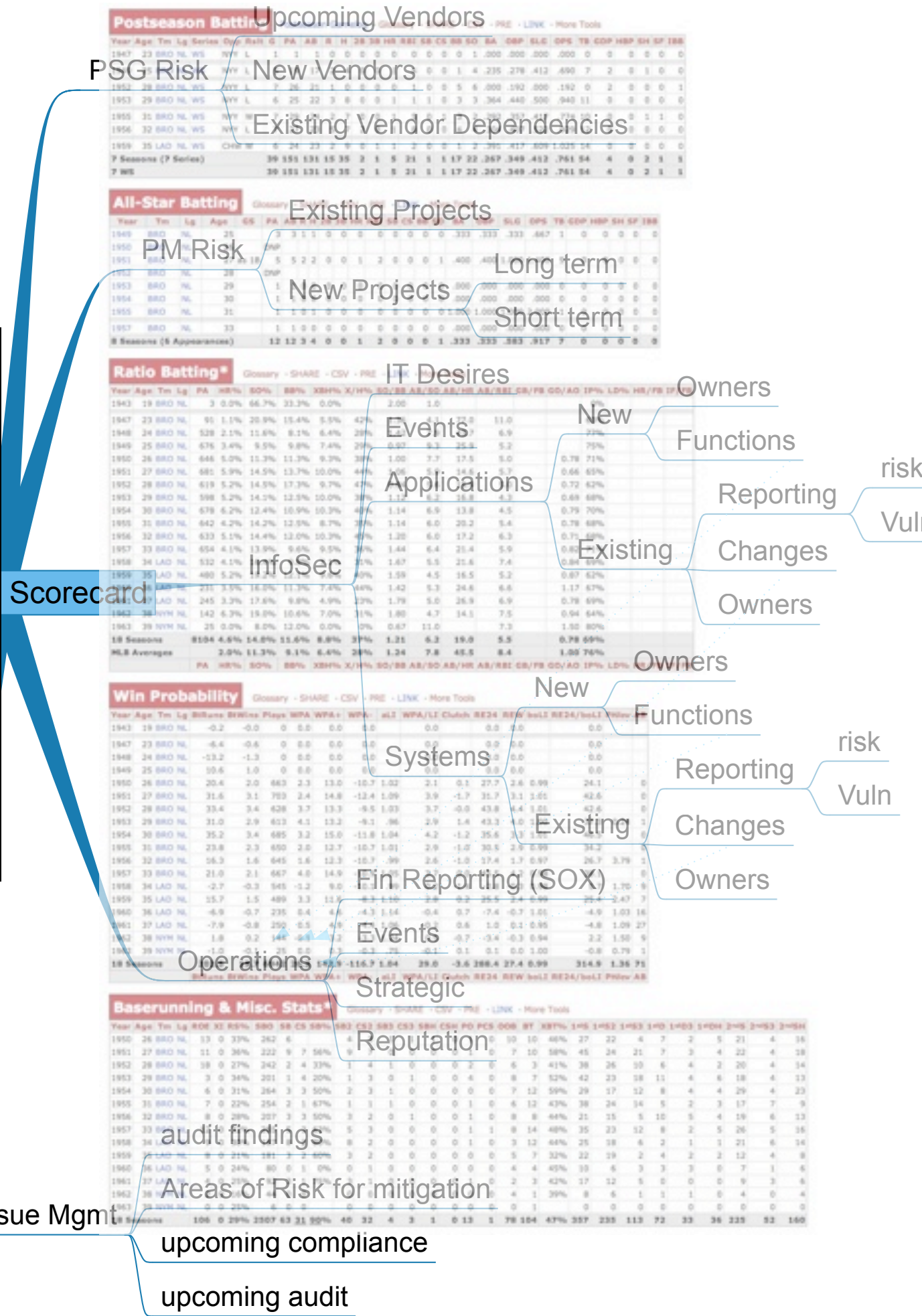
Simulations of the magnitude and frequency of an external data breach returned the following:



Scorecard

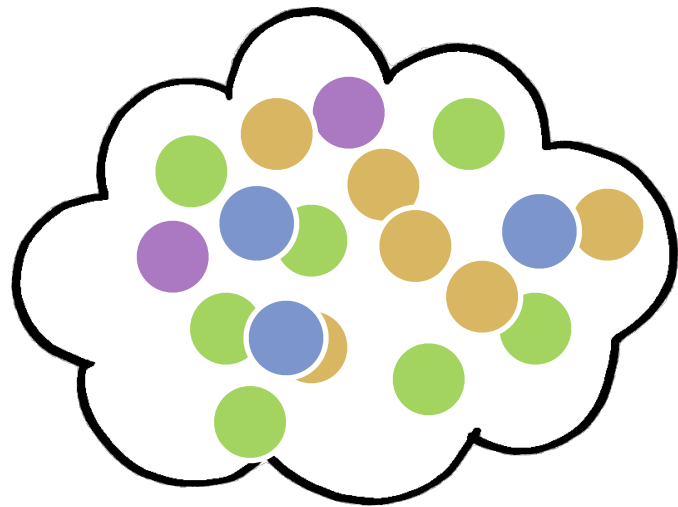


Scorecard

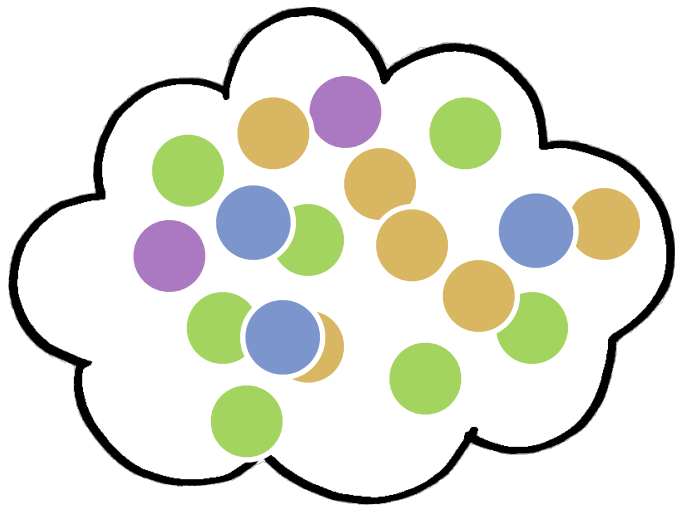


AN EASY TO USE
TOOL TO HELP YOU
FRAME THE
PROBLEM-SPACE

The RiskFish



**The problem space can
be confusing to talk
about.**

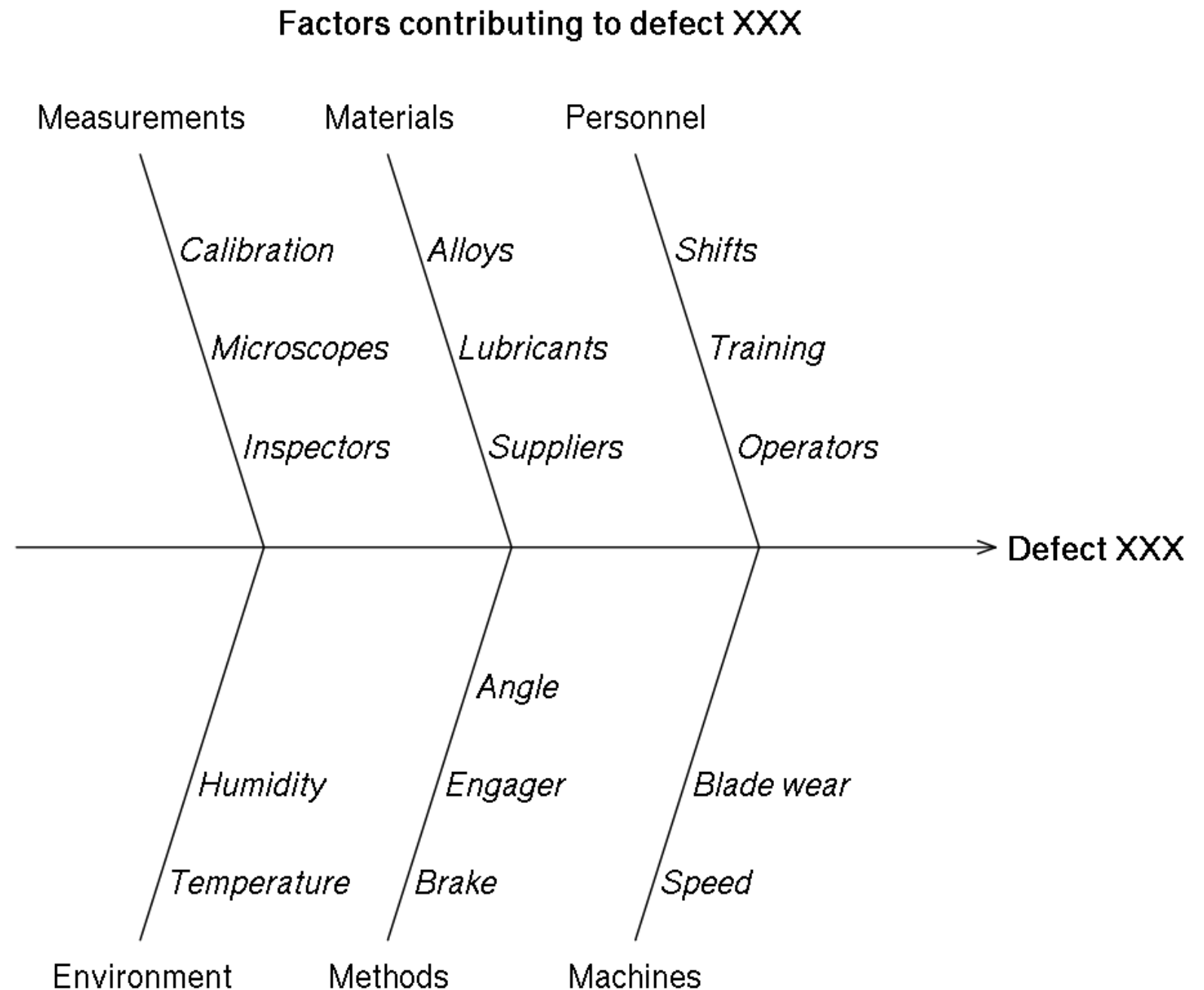


**People naturally
gravitate towards fixing
the easy symptom
rather than the hard
problem**

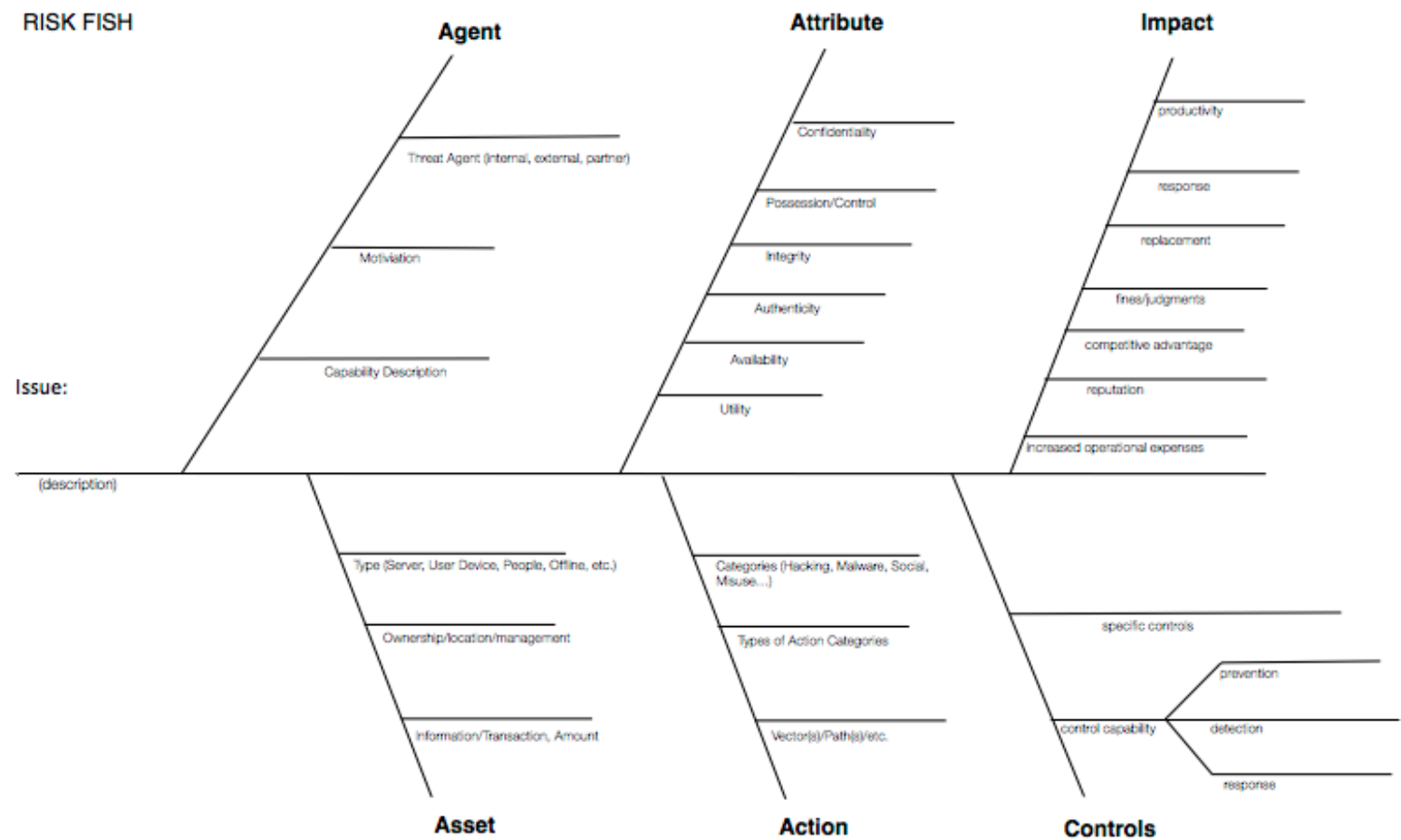


Kaoru Ishikawa
father of quality circles and
the fish diagram

Fish (Ishikawa) diagram for root cause analysis in manufacturing



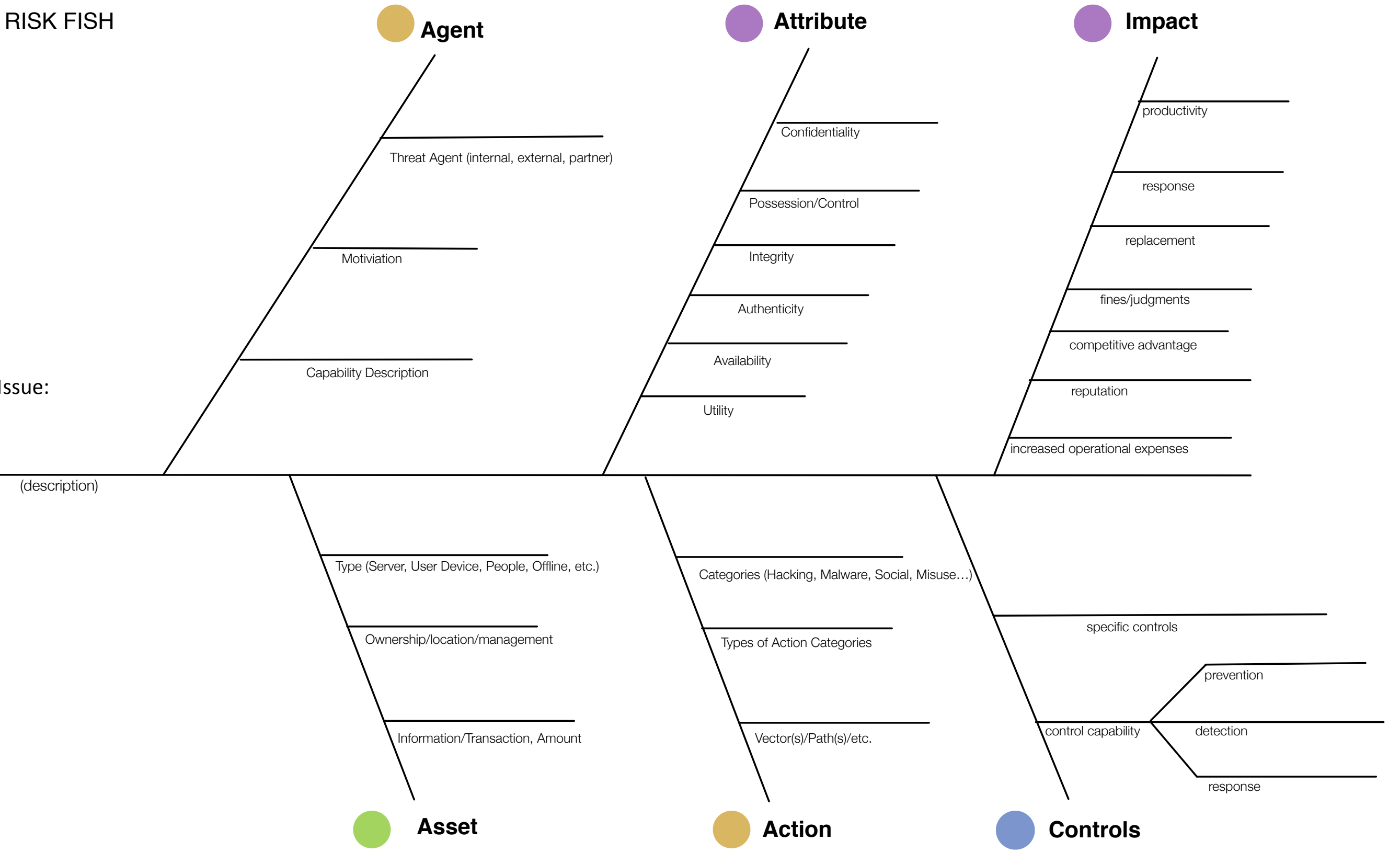
Fish (Ishikawa) diagram for root cause analysis for risk using VERIS



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>.
For more information about VERIS: <http://veriscommunity.net/> For risk community interaction and the home of the RiskFish: <https://www.societyinforisk.org/>

RISK FISH

Issue:



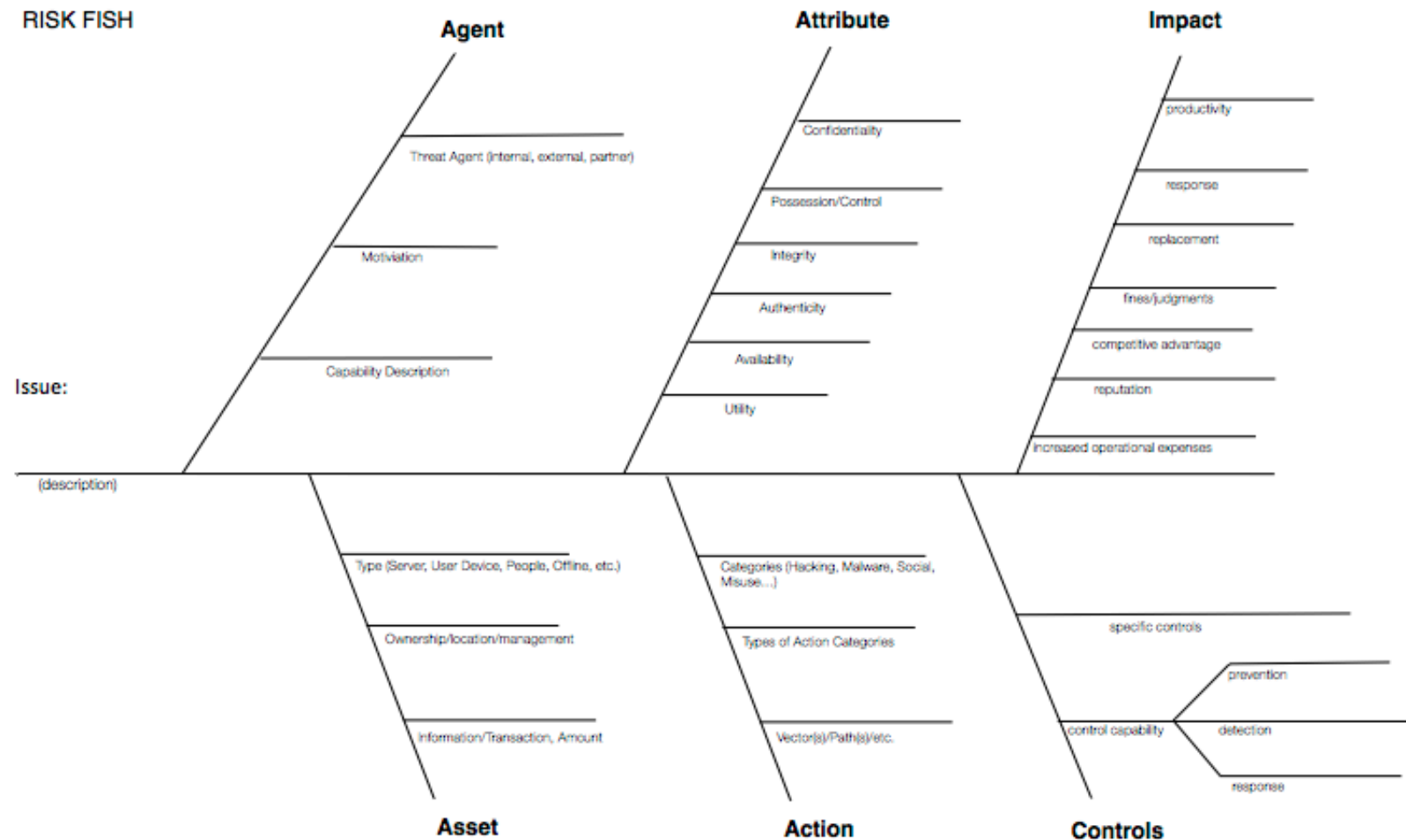
VERIS RiskFish Resources

Society of Information Risk Analysts

<http://www.societyinforisk.org>

VERIS Community

<http://www.veriscommunity.net/>



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>. For more information about VERIS: <http://veriscommunity.net/> For risk community interaction and the home of the RiskFish: <http://www.societyinforisk.org/>



Moment of Zen



The point at which you can remove the word risk from your vocabulary is the point at which you become a risk master.