only the wisest and stupidest of men never change

Confucius

verizon
Cybertrust Security

Bridging Risk Modeling, Threat Modeling, and Operational Metrics With the VERIS Framework

or: Data? WTH do we do now?!

Alex Hutton
@alexhutton

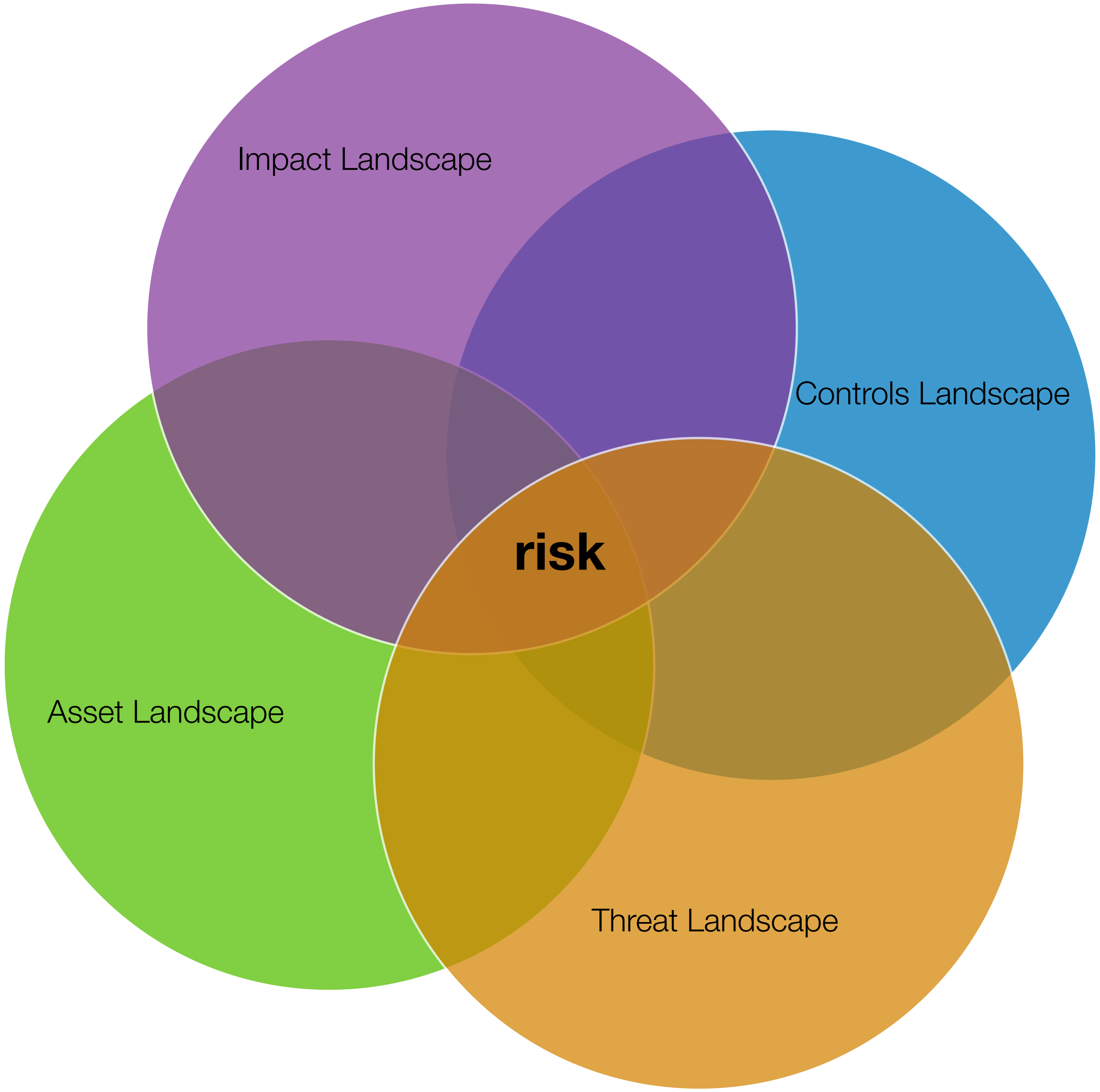
State of the Industry

Ranum: *Pseudoscience*

Hutton: *Kuhn’s Protoscience*

- 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

verizon
Cybertrust Security

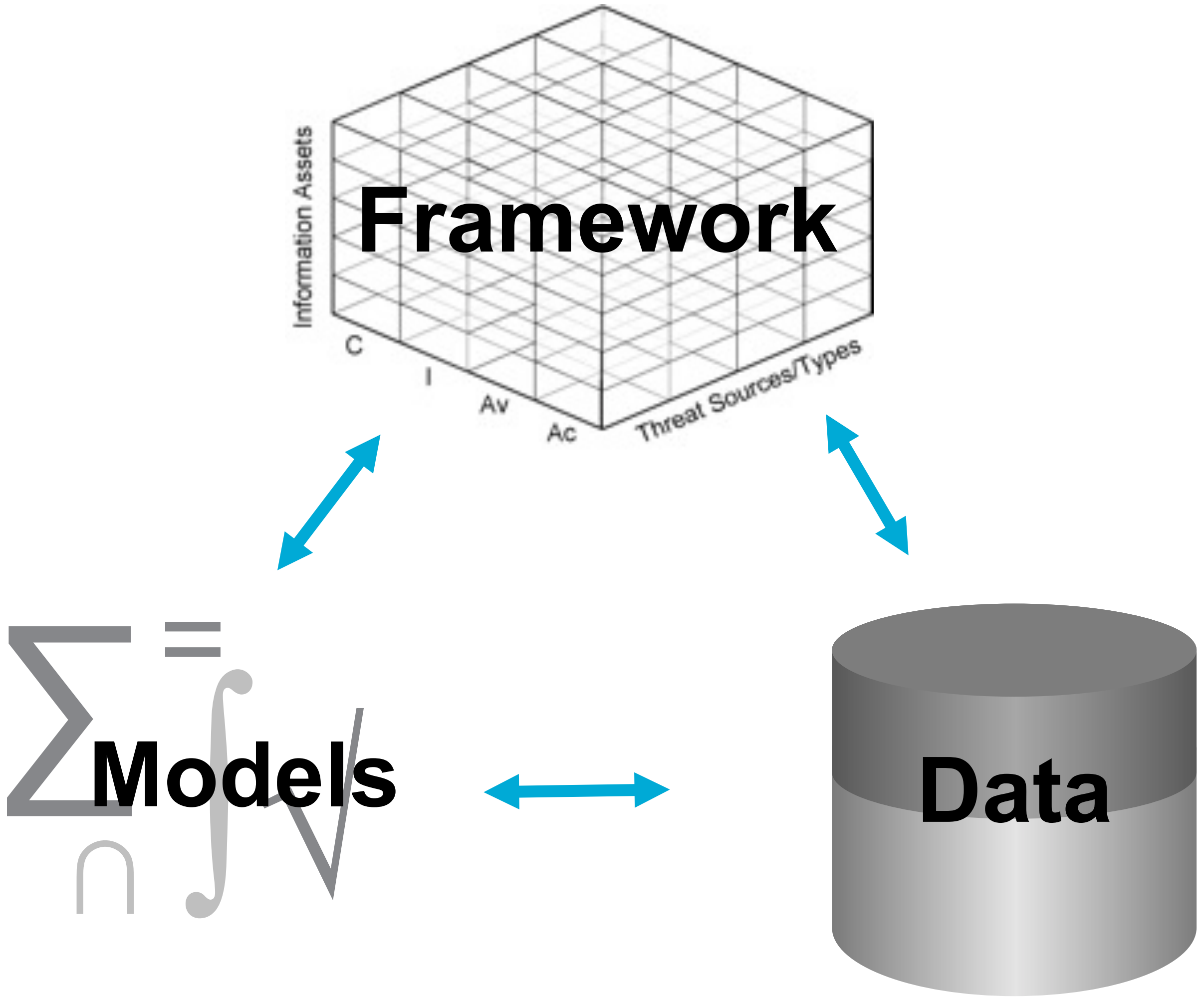


including capabilities (skills, resources, decision quality...)

Managing risk means aligning the capabilities of the organization, and the exposure of the organization with the tolerance of the data owners

- Jack Jones

Verizon RISK Team: Operating Model



Framework

Models

Data

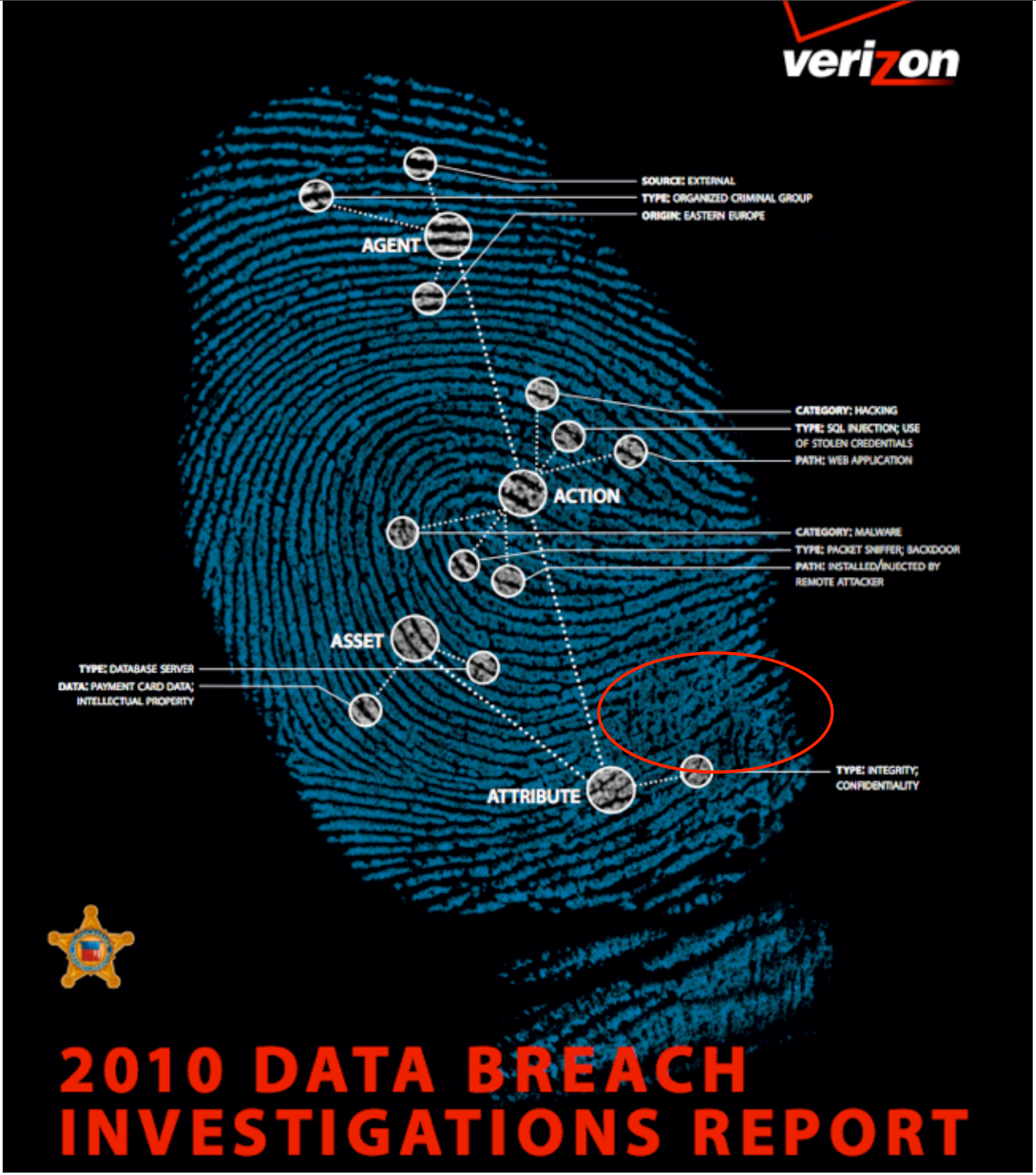
- VERIS is our framework that provides context

verizon
Cybertrust Security

A Brief Overview of VERIS

(the Verizon Enterprise Risk & Incident Sharing Framework)

Verizon has shared data


verizon
AGENT
SOURCE: EXTERNAL
TYPE: ORGANIZED CRIMINAL GROUP
ORIGIN: EASTERN EUROPE
ACTION
CATEGORY: HACKING
TYPE: SQL INJECTION; USE OF STOLEN CREDENTIALS
PATH: WEB APPLICATION
CATEGORY: MALWARE
TYPE: PACKET SNIFFER; BACKDOOR
PATH: INSTALLED/INJECTED BY REMOTE ATTACKER
ASSET
TYPE: DATABASE SERVER
DATA: PAYMENT CARD DATA; INTELLECTUAL PROPERTY
ATTRIBUTE
TYPE: INTEGRITY; CONFIDENTIALITY

2010 DATA BREACH INVESTIGATIONS REPORT

- 2010 ~ 900 cases
  - (900 million records)

Verizon is sharing our framework

Verizon Enterprise Risk & Incident Sharing (VERIS) Framework

it’s open*!

* kinda

What is the Verizon Incident Sharing (VERIS) Framework?

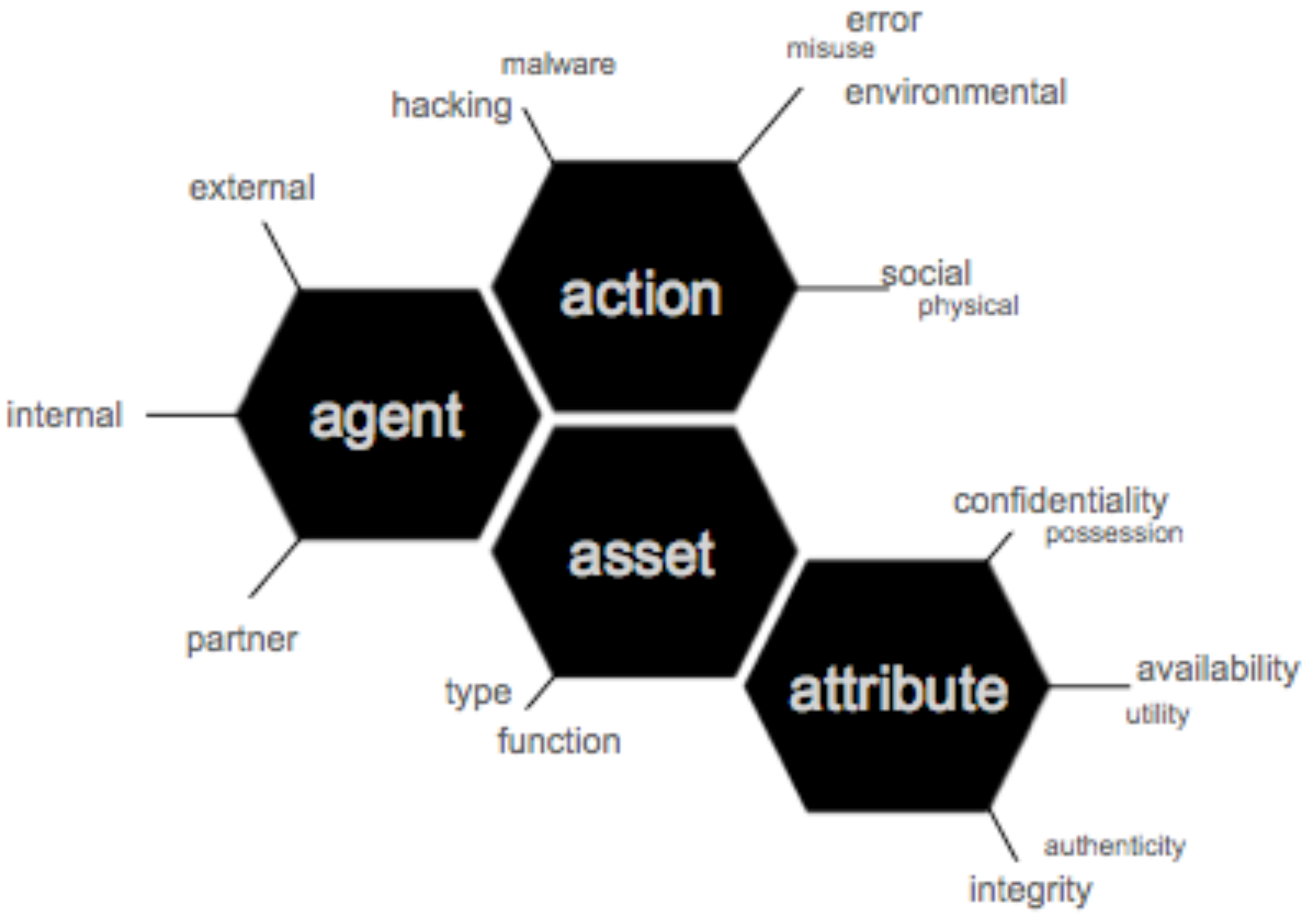
- A means to create metrics from the incident narrative
  - how Verizon creates measurements for the DBIR
  - how *anyone* can create measurements from an incident
  - http://securityblog.verizonbusiness.com/wp-content/uploads/2010/03/VerIS_Framework_Beta_1.pdf

What makes up the VERIS framework?

- Demographics
- Incident Classification
  - Event Modeling (a^4)
- Discovery & Mitigation
- Impact Classification
  - Impact Modeling

What VERIS Contains

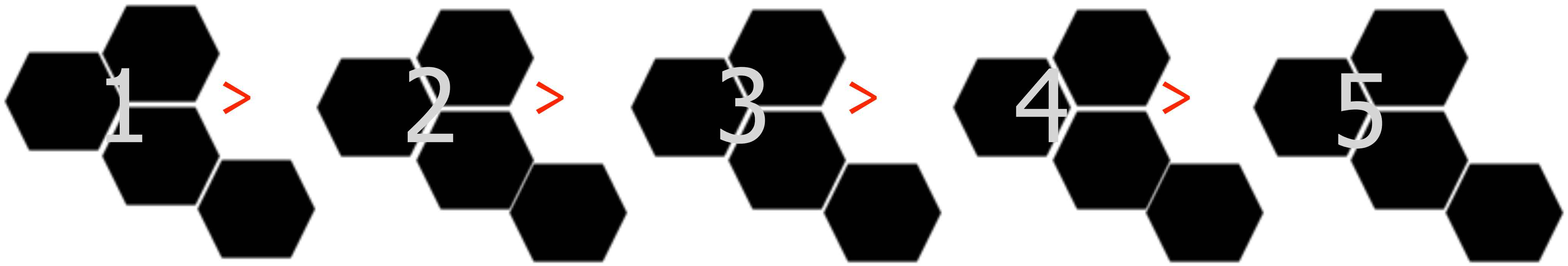
The Incident Classification section employs Verizon’s A^4 event model



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

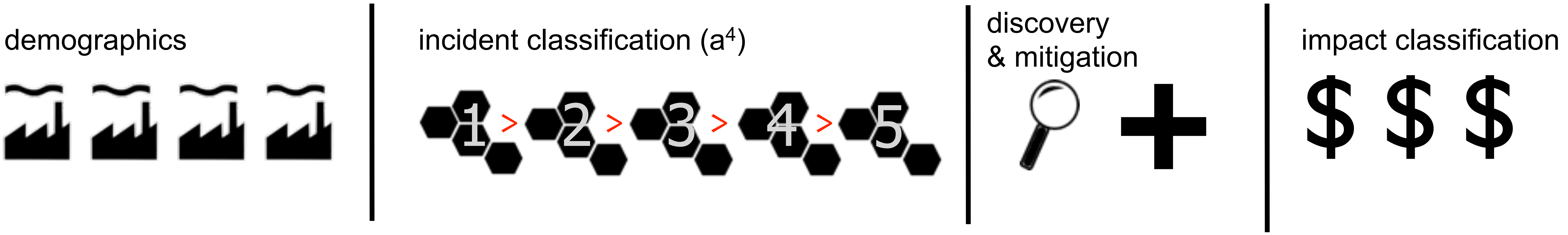
Agent: Whose actions affected the asset
Action: What actions affected the asset Asset:
Which assets were affected Attribute: How the
asset was affected

Incident as a
chain of events >



Cybertrust Security

incident narrative → incident metrics

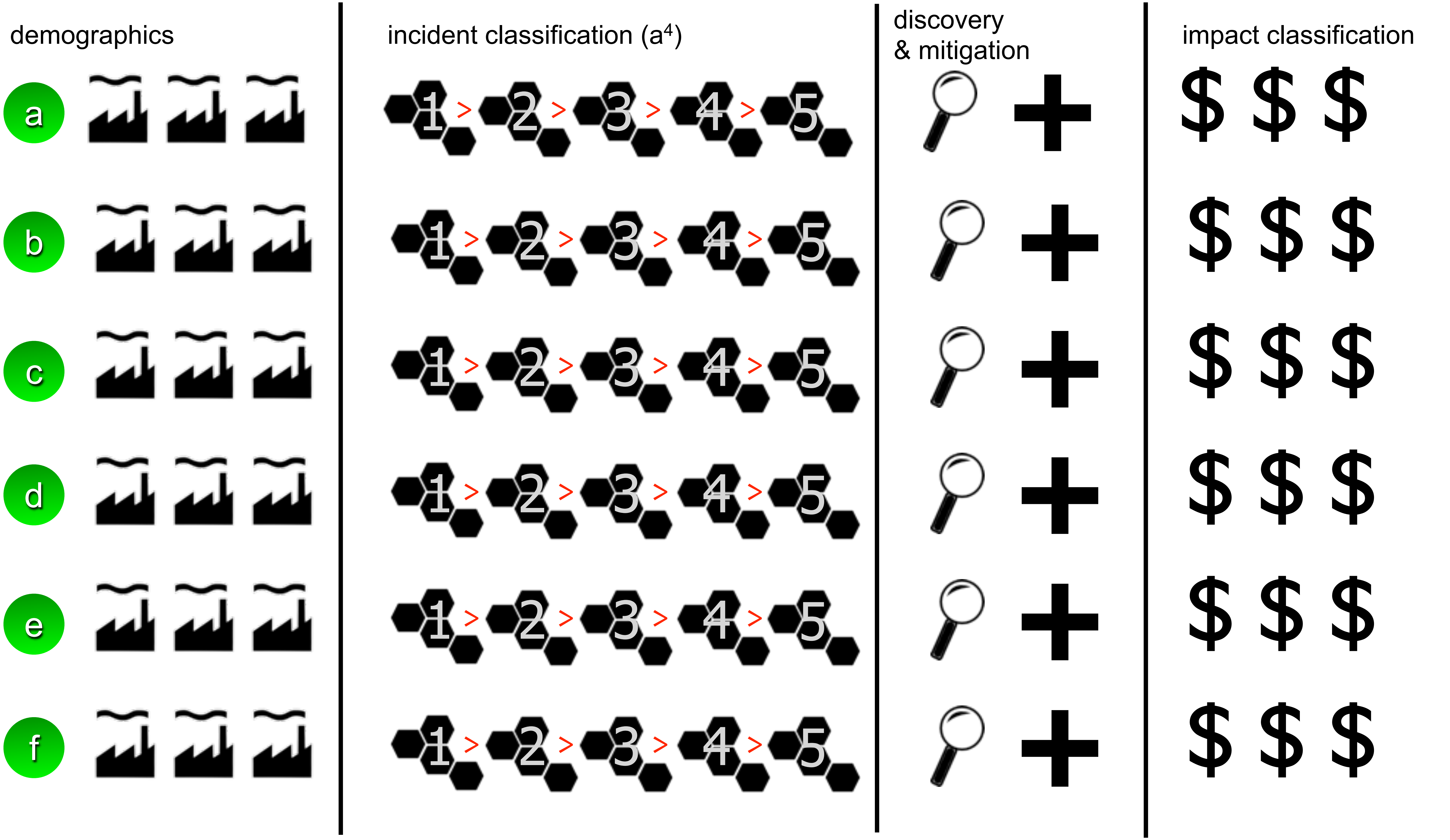

demographics

incident classification (a^4)

discovery
& mitigation

impact classification

case studies → data set



verizon
Cybertrust Security

VERIS Data Comes From...

- External Sources
- Internal Sources

  - DBIR + Secret Service is the start of the VERIS data set.

Good Lord Of The Dance,

Models and data sharing!

verizon
Cybertrust Security

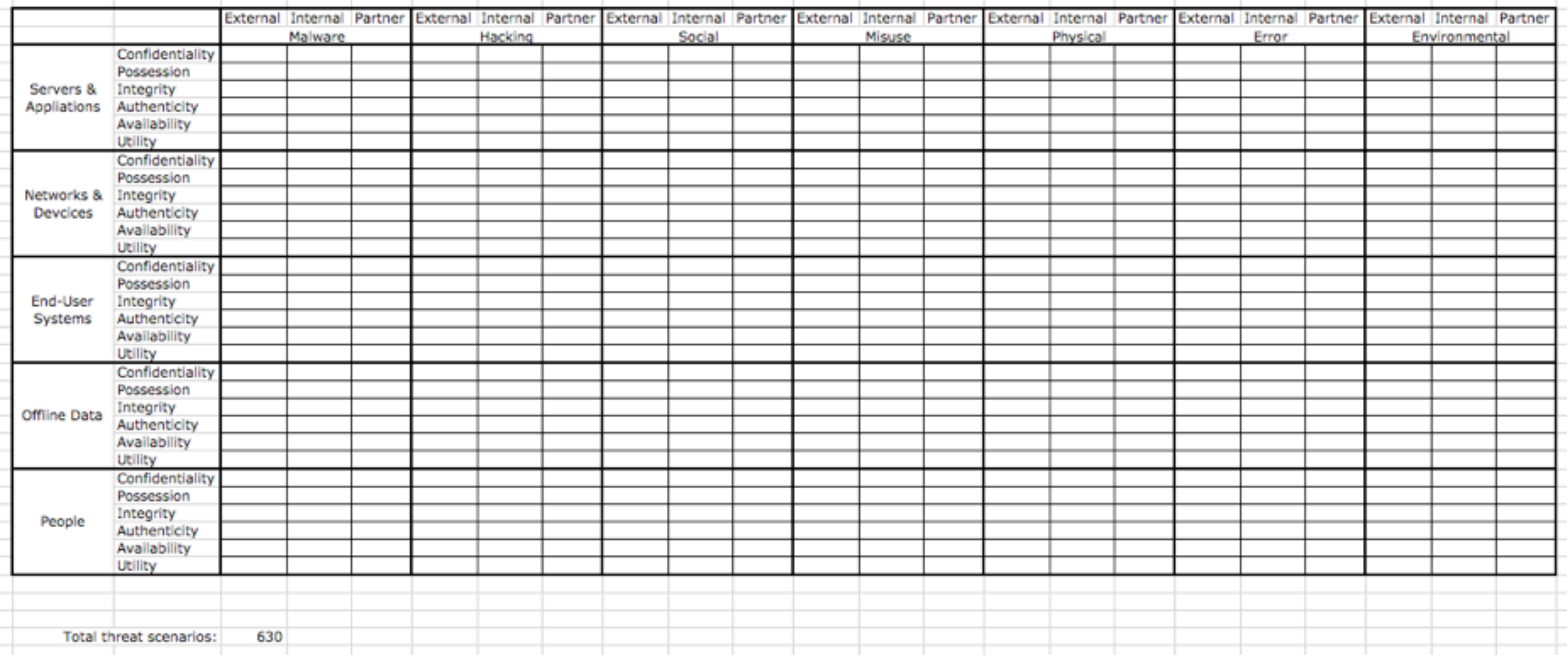
Using VERIS (DBIR) Data

(Verizon’s Internal Model)

- Traditional GRC dictates “likelihood & impact”
- VERIS Data can be used to in “traditional” risk management
  - weights
  - distribution development

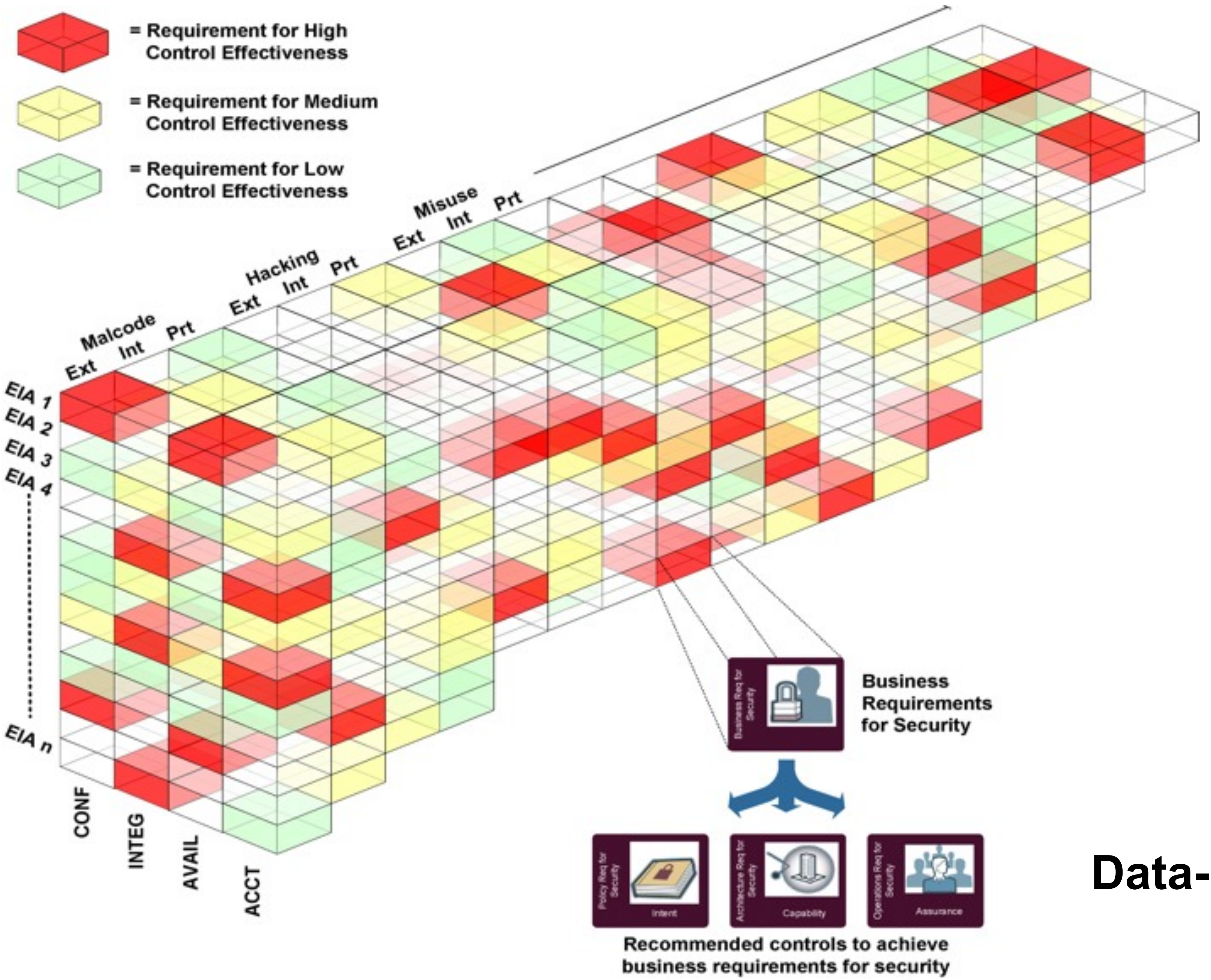
Using VERIS (DBIR) Data

(Verizon's Internal Model)



		External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner
			Malware			Hacking			Social			Misuse			Physical			Error			Environmental	
Servers & Appliations	Confidentiality																					
	Possession																					
	Integrity																					
	Authenticity																					
	Availability																					
	Utility																					
Networks & Devcices	Confidentiality																					
	Possession																					
	Integrity																					
	Authenticity																					
	Availability																					
	Utility																					
End-User Systems	Confidentiality																					
	Possession																					
	Integrity																					
	Authenticity																					
	Availability																					
	Utility																					
Offline Data	Confidentiality																					
	Possession																					
	Integrity																					
	Authenticity																					
	Availability																					
	Utility																					
People	Confidentiality																					
	Possession																					
	Integrity																					
	Authenticity																					
	Availability																					
	Utility																					
	Total threat scenarios:	630																				

What VERIS Does


🟥 = Requirement for High Control Effectiveness

🟨 = Requirement for Medium Control Effectiveness

🟩 = Requirement for Low Control Effectiveness

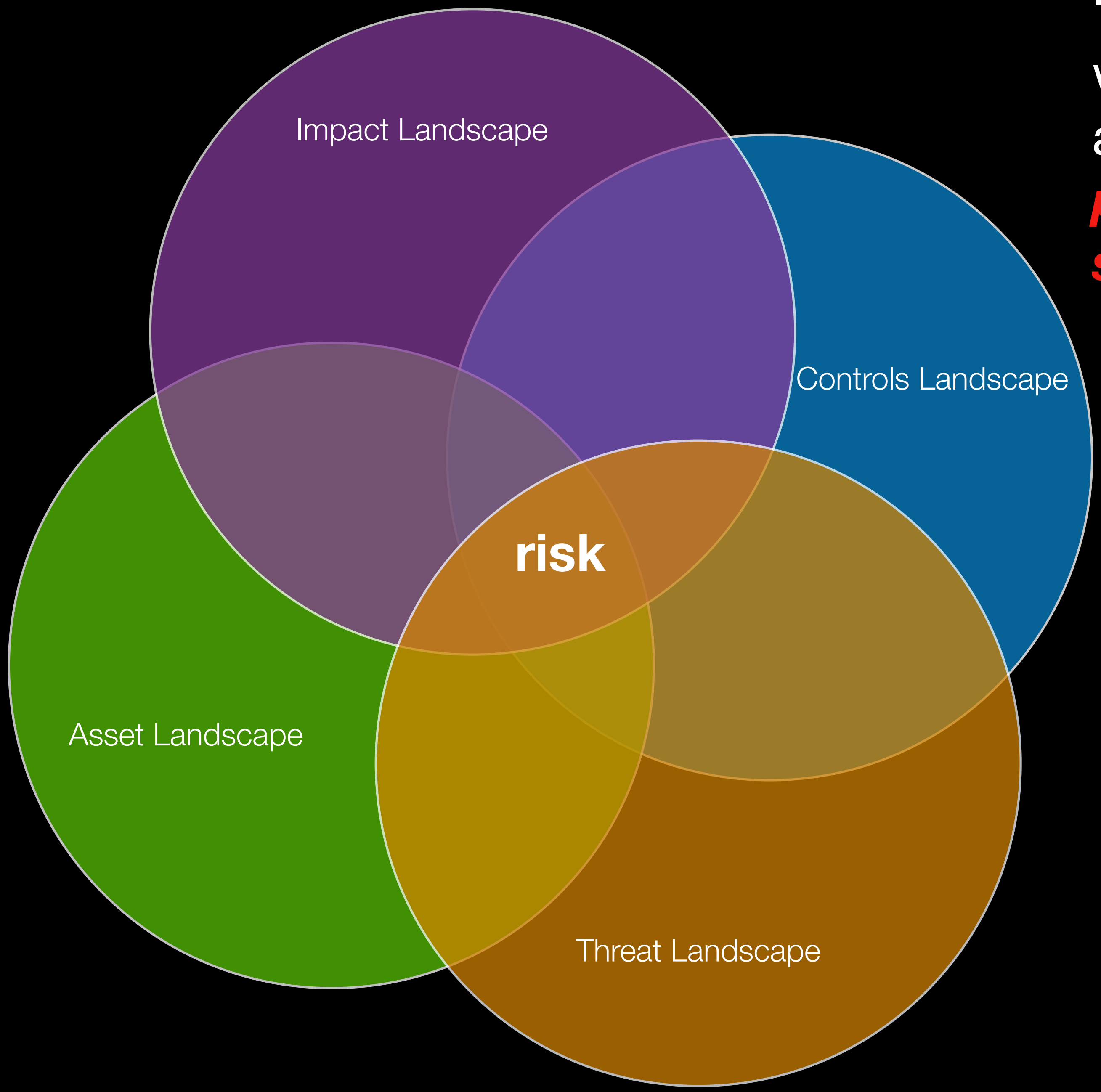
Business Requirements for Security

Recommended controls to achieve business requirements for security

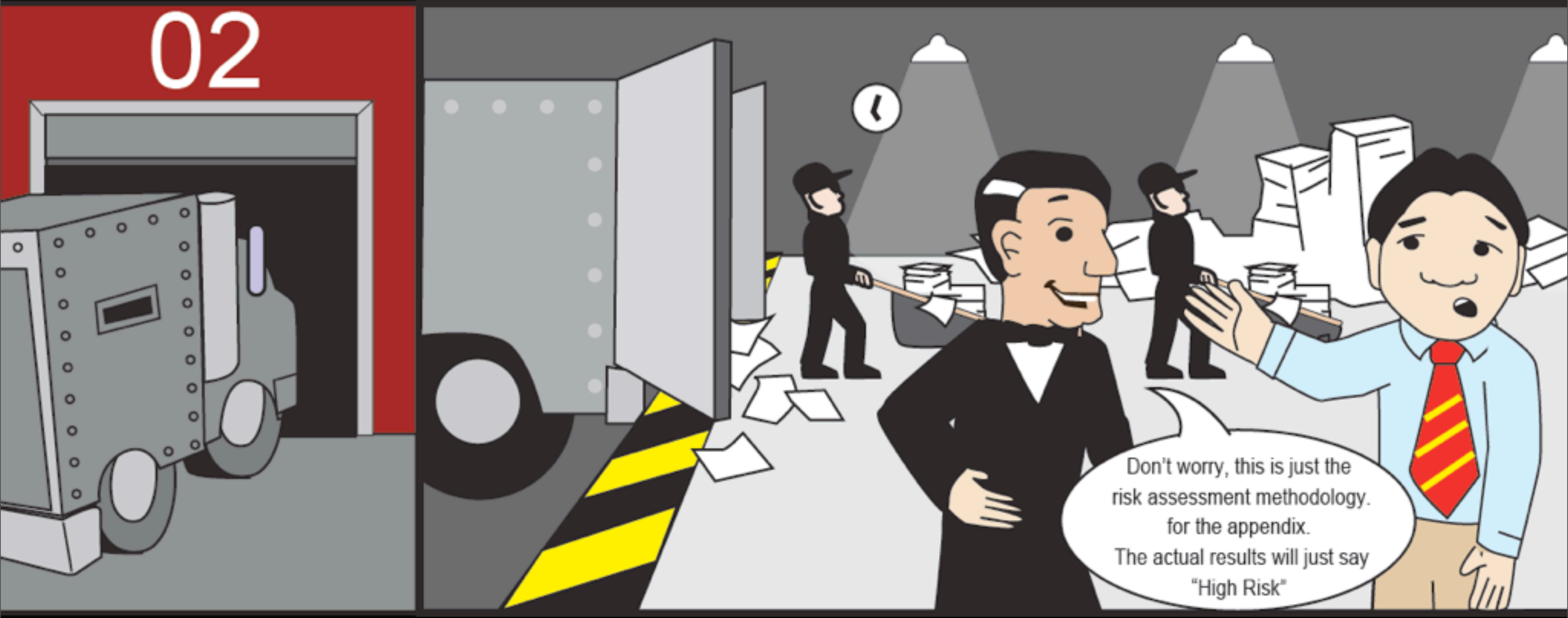
Data-driven decisions

Friederich Hayek invades my dreams to give me visions of a future approach

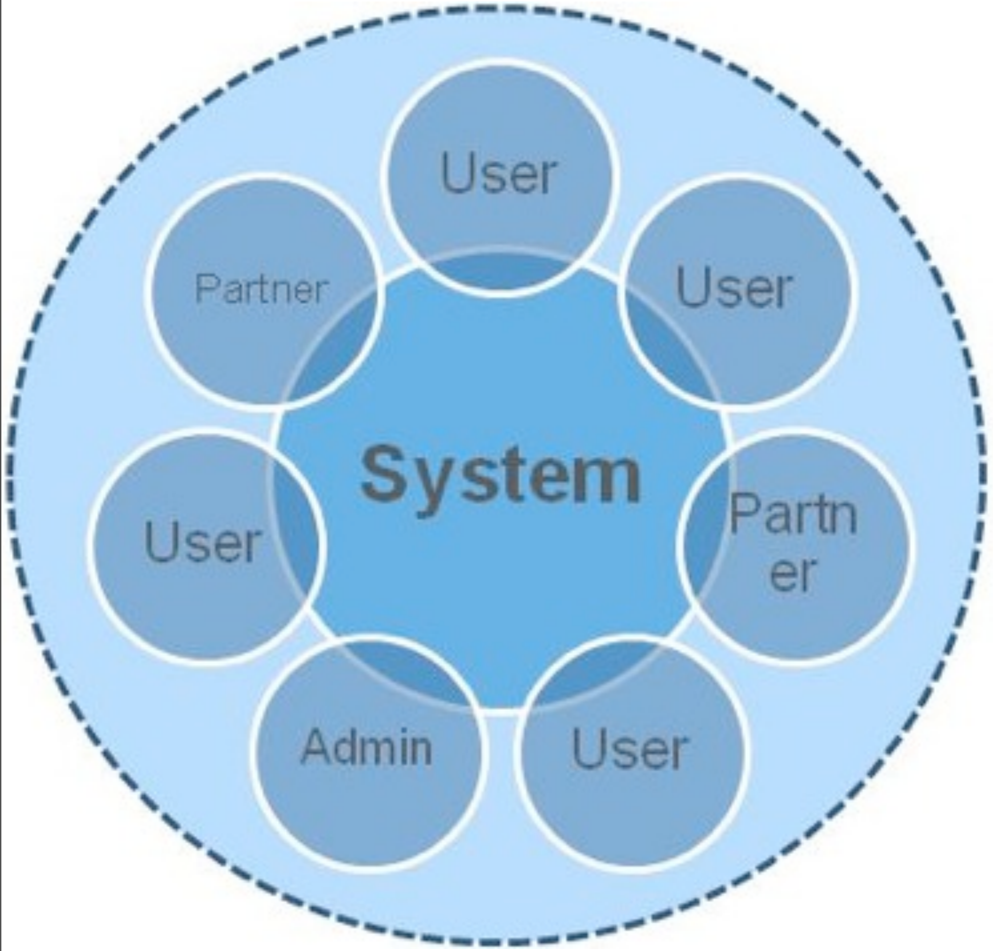
or, “How Jose Cardenal's sweet afro could change the industry!”

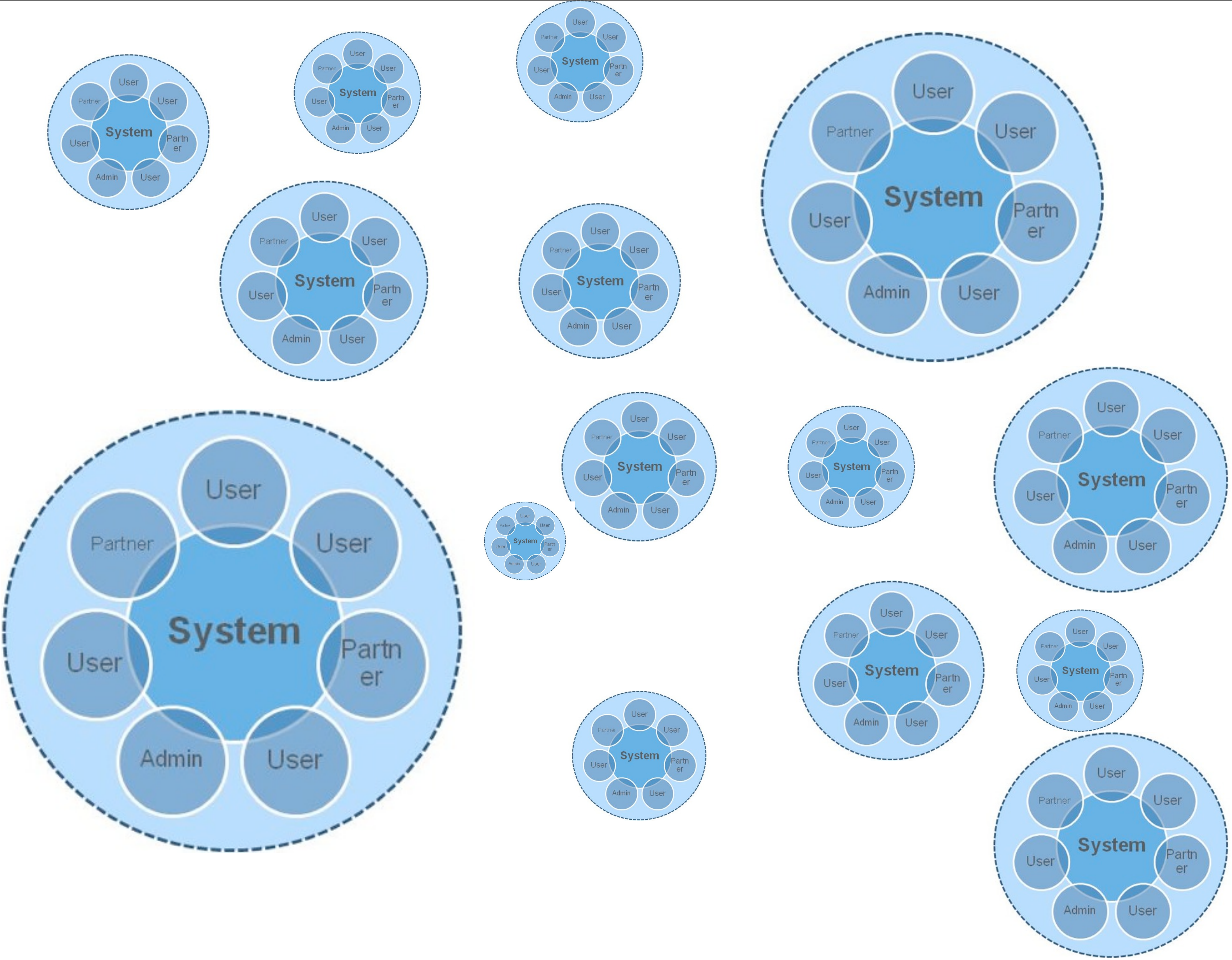


the synthesis of information creates a "one true risk statement" which overtime becomes a ***multitude of probabilistic point statements***


02
Don't worry, this is just the risk assessment methodology. for the appendix.
The actual results will just say "High Risk"

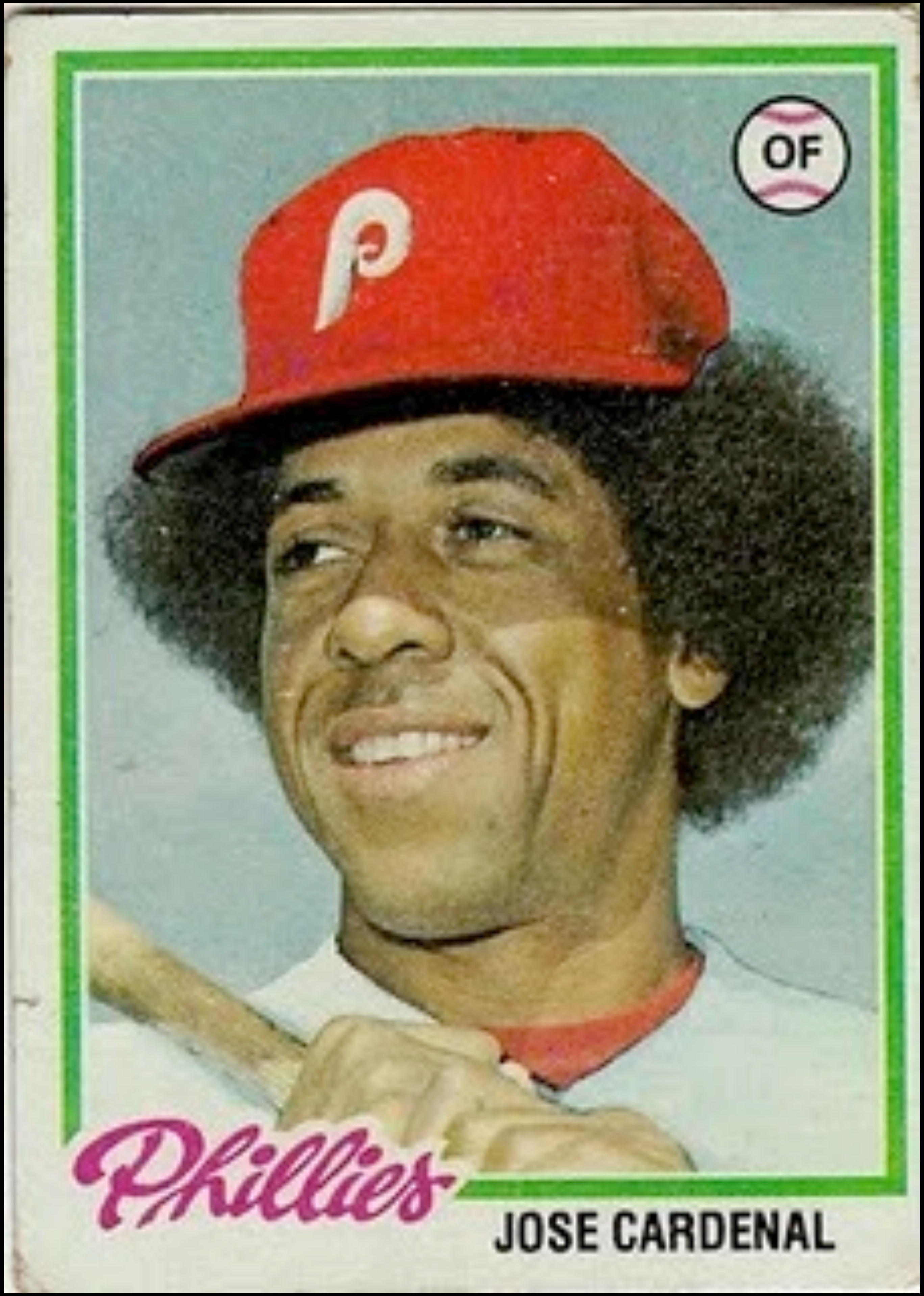
from Mark Curphey's SecurityBull$#!*

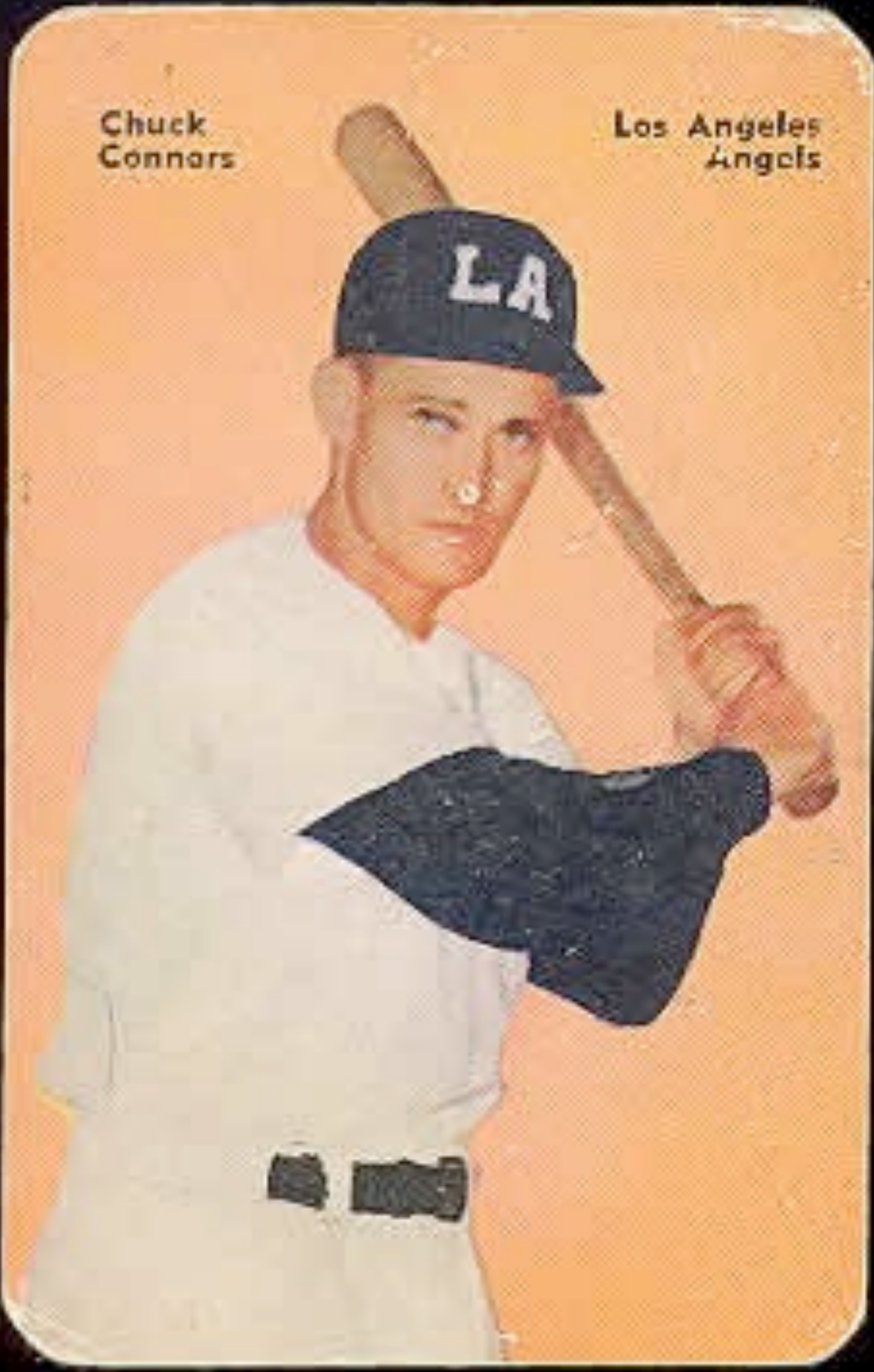

User
Partner
User
System
User
Partn
er
Admin
User

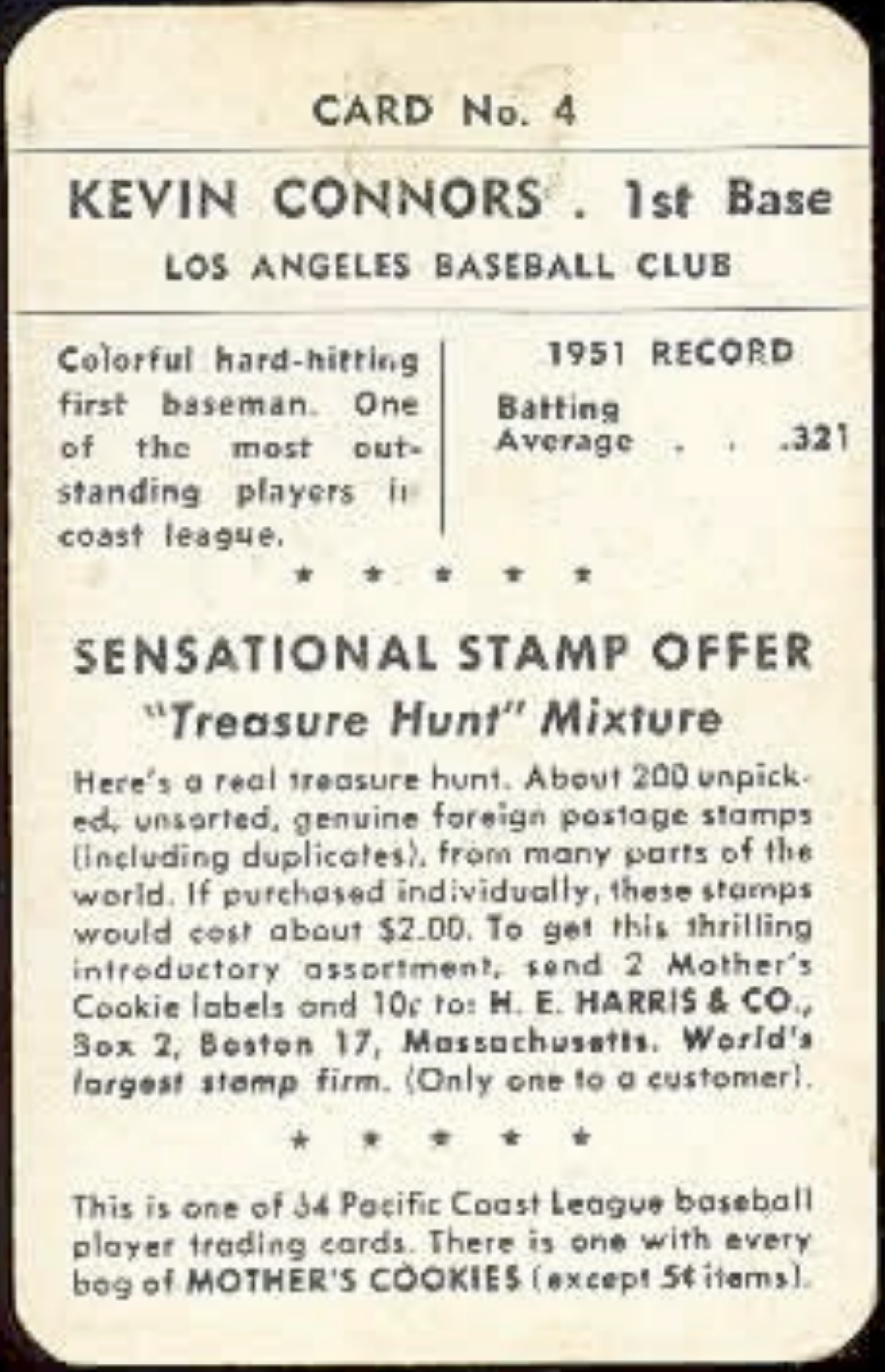

User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User
User
Partner
User
System
User
Partn er
Admin
User

These “risk” statements you’re making, I don’t think you’re doing it right.

- (Chillin’ Friederich Hayek)


OF
Phillies
JOSE CARDENAL





CARD No. 4

KEVIN CONNORS . 1st Base

LOS ANGELES BASEBALL CLUB

Colorful hard-hitting first baseman. One of the most outstanding players in coast league.

1951 RECORD

Batting Average . . .321

* * * * *

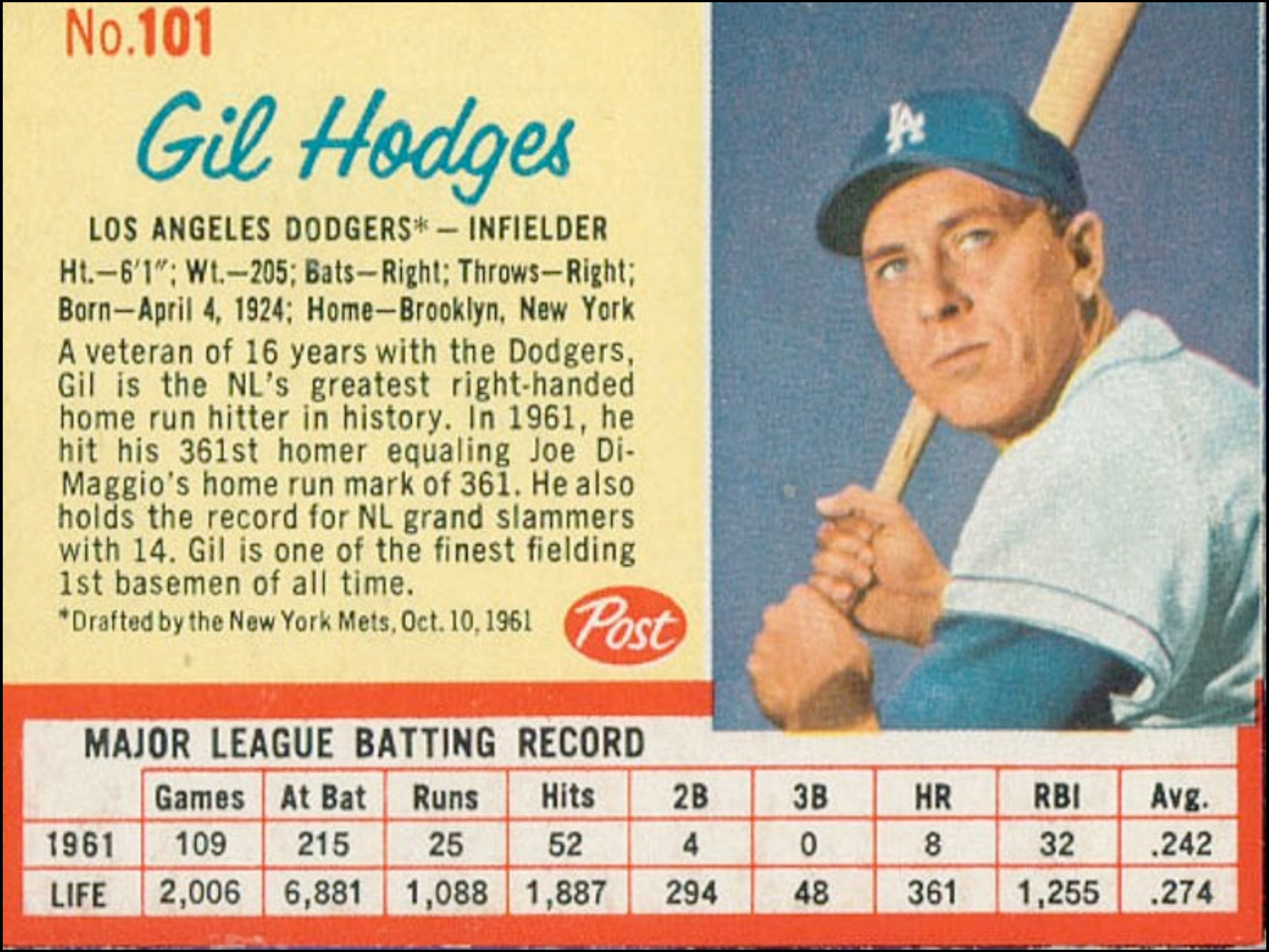
SENSATIONAL STAMP OFFER

"Treasure Hunt" Mixture

Here's a real treasure hunt. About 200 unpicked, unsorted, genuine foreign postage stamps (including duplicates), from many parts of the world. If purchased individually, these stamps would cost about $2.00. To get this thrilling introductory assortment, send 2 Mother's Cookie labels and 10¢ to: **H. E. HARRIS & CO., Box 2, Boston 17, Massachusetts. World's largest stamp firm.** (Only one to a customer).

* * * * *

This is one of 64 Pacific Coast League baseball player trading cards. There is one with every bag of **MOTHER'S COOKIES** (except 5¢ items).



No.101

Gil Hodges

LOS ANGELES DODGERS* – INFIELDER

Ht.–6'1"; Wt.–205; Bats–Right; Throws–Right; Born–April 4, 1924; Home–Brooklyn, New York

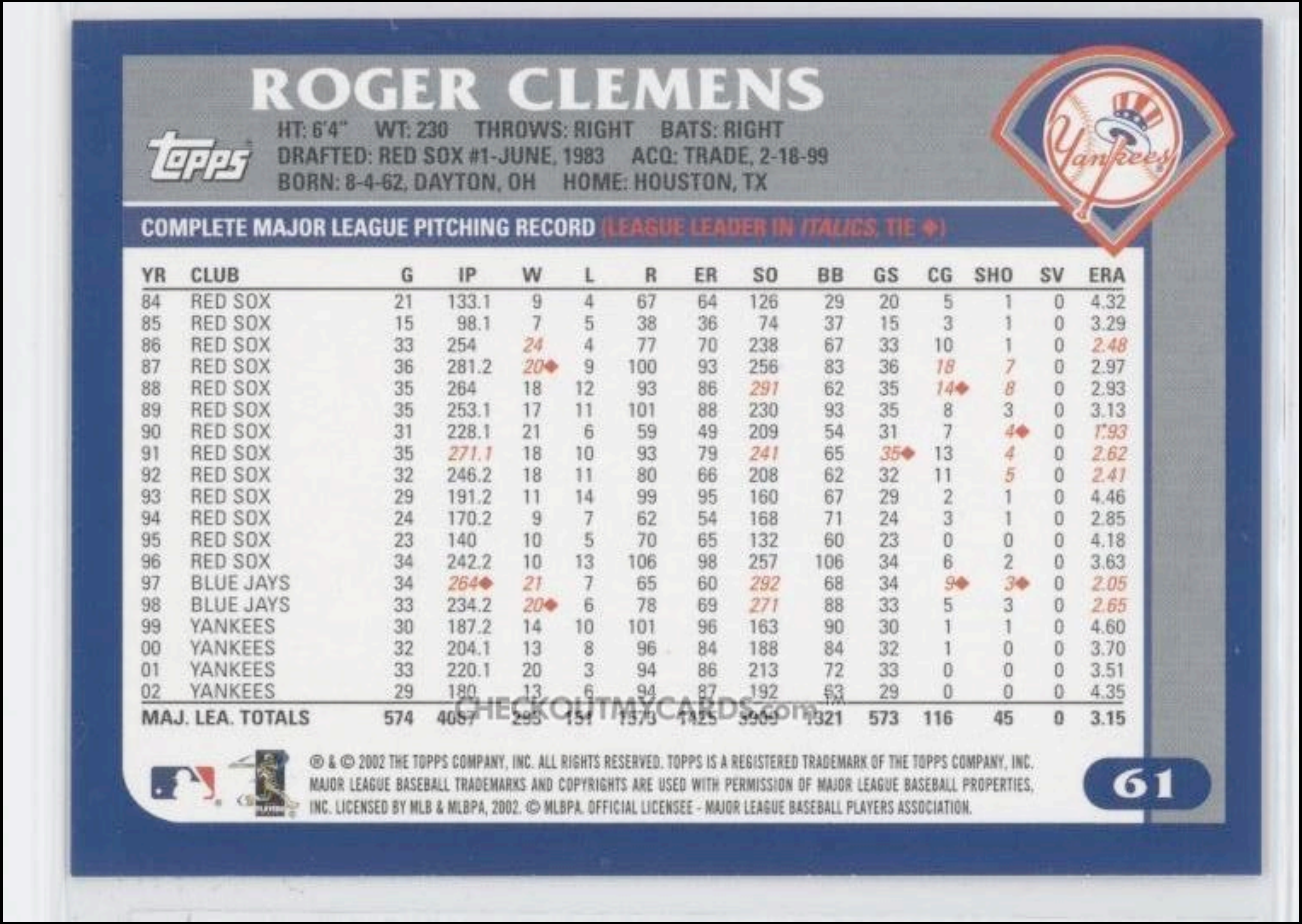
A veteran of 16 years with the Dodgers, Gil is the NL's greatest right-handed home run hitter in history. In 1961, he hit his 361st homer equaling Joe DiMaggio's home run mark of 361. He also holds the record for NL grand slammers with 14. Gil is one of the finest fielding 1st basemen of all time.

*Drafted by the New York Mets, Oct. 10, 1961

Post

MAJOR LEAGUE BATTING RECORD

	Games	At Bat	Runs	Hits	2B	3B	HR	RBI	Avg.
1961	109	215	25	52	4	0	8	32	.242
LIFE	2,006	6,881	1,088	1,887	294	48	361	1,255	.274



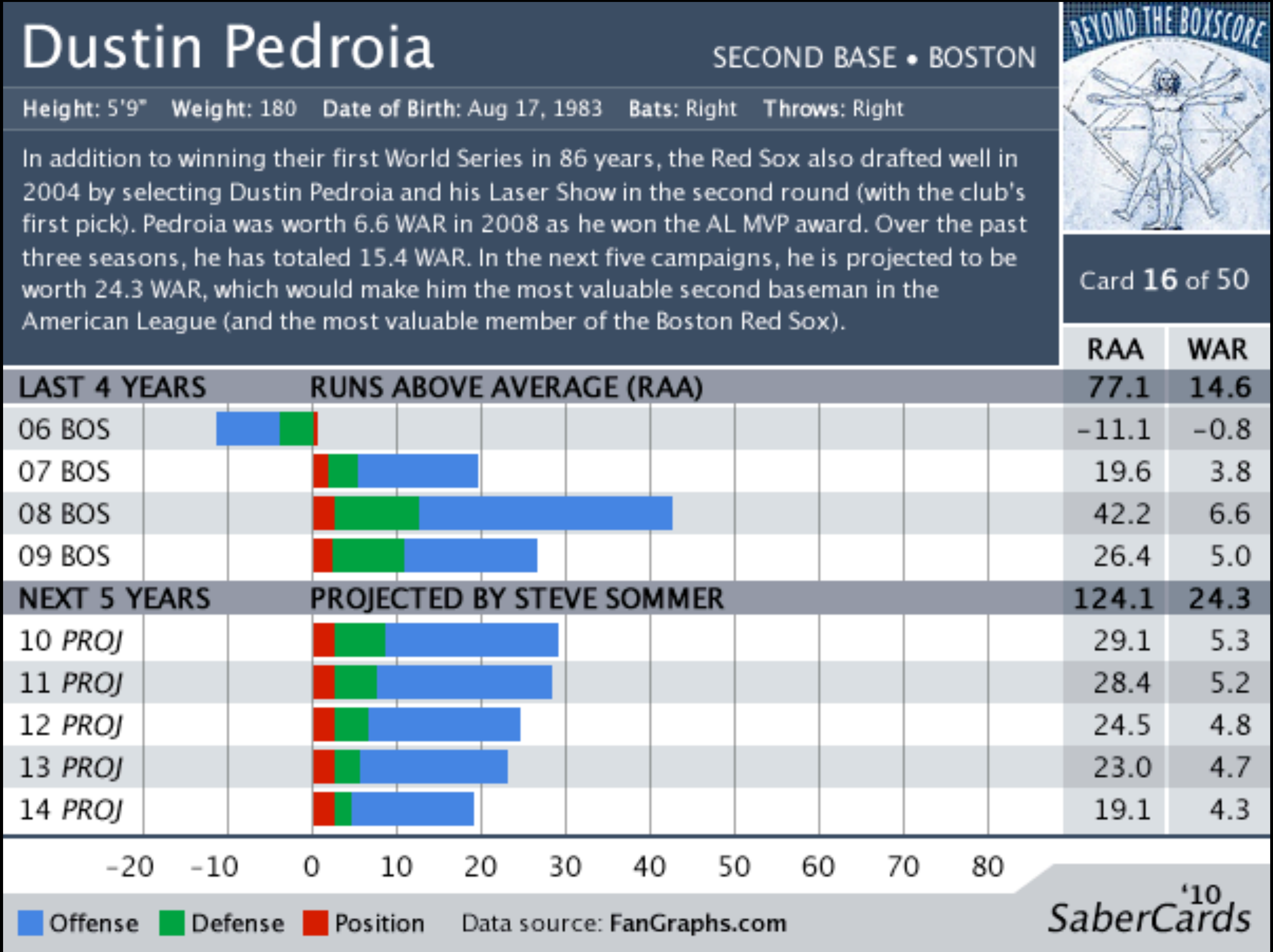
ROGER CLEMENS

HT: 6'4" WT: 230 THROWS: RIGHT BATS: RIGHT
DRAFTED: RED SOX #1-JUNE, 1983 ACQ: TRADE, 2-18-99
BORN: 8-4-62, DAYTON, OH HOME: HOUSTON, TX

COMPLETE MAJOR LEAGUE PITCHING RECORD (LEAGUE LEADER IN *ITALICS*, TIE ◆)

YR	CLUB	G	IP	W	L	R	ER	SO	BB	GS	CG	SHO	SV	ERA
84	RED SOX	21	133.1	9	4	67	64	126	29	20	5	1	0	4.32
85	RED SOX	15	98.1	7	5	38	36	74	37	15	3	1	0	3.29
86	RED SOX	33	254	*24*	4	77	70	238	67	33	10	1	0	*2.48*
87	RED SOX	36	281.2	*20*◆	9	100	93	256	83	36	*18*	*7*	0	2.97
88	RED SOX	35	264	18	12	93	86	*291*	62	35	*14*◆	*8*	0	2.93
89	RED SOX	35	253.1	17	11	101	88	230	93	35	8	3	0	3.13
90	RED SOX	31	228.1	21	6	59	49	209	54	31	7	*4*◆	0	*1.93*
91	RED SOX	35	*271.1*	18	10	93	79	*241*	65	*35*◆	13	*4*	0	*2.62*
92	RED SOX	32	246.2	18	11	80	66	208	62	32	11	*5*	0	*2.41*
93	RED SOX	29	191.2	11	14	99	95	160	67	29	2	1	0	4.46
94	RED SOX	24	170.2	9	7	62	54	168	71	24	3	1	0	2.85
95	RED SOX	23	140	10	5	70	65	132	60	23	0	0	0	4.18
96	RED SOX	34	242.2	10	13	106	98	257	106	34	6	2	0	3.63
97	BLUE JAYS	34	*264*◆	*21*	7	65	60	*292*	68	34	*9*◆	*3*◆	0	*2.05*
98	BLUE JAYS	33	234.2	*20*◆	6	78	69	*271*	88	33	5	3	0	*2.65*
99	YANKEES	30	187.2	14	10	101	96	163	90	30	1	1	0	4.60
00	YANKEES	32	204.1	13	8	96	84	188	84	32	1	0	0	3.70
01	YANKEES	33	220.1	20	3	94	86	213	72	33	0	0	0	3.51
02	YANKEES	29	180	13	6	94	87	192	63	29	0	0	0	4.35
MAJ. LEA. TOTALS		**574**	**4087**	**293**	**151**	**1573**	**1425**	**3909**	**1321**	**573**	**116**	**45**	**0**	**3.15**

61



Dustin Pedroia

SECOND BASE • BOSTON

Height: 5'9" **Weight:** 180 **Date of Birth:** Aug 17, 1983 **Bats:** Right **Throws:** Right

In addition to winning their first World Series in 86 years, the Red Sox also drafted well in 2004 by selecting Dustin Pedroia and his Laser Show in the second round (with the club's first pick). Pedroia was worth 6.6 WAR in 2008 as he won the AL MVP award. Over the past three seasons, he has totaled 15.4 WAR. In the next five campaigns, he is projected to be worth 24.3 WAR, which would make him the most valuable second baseman in the American League (and the most valuable member of the Boston Red Sox).

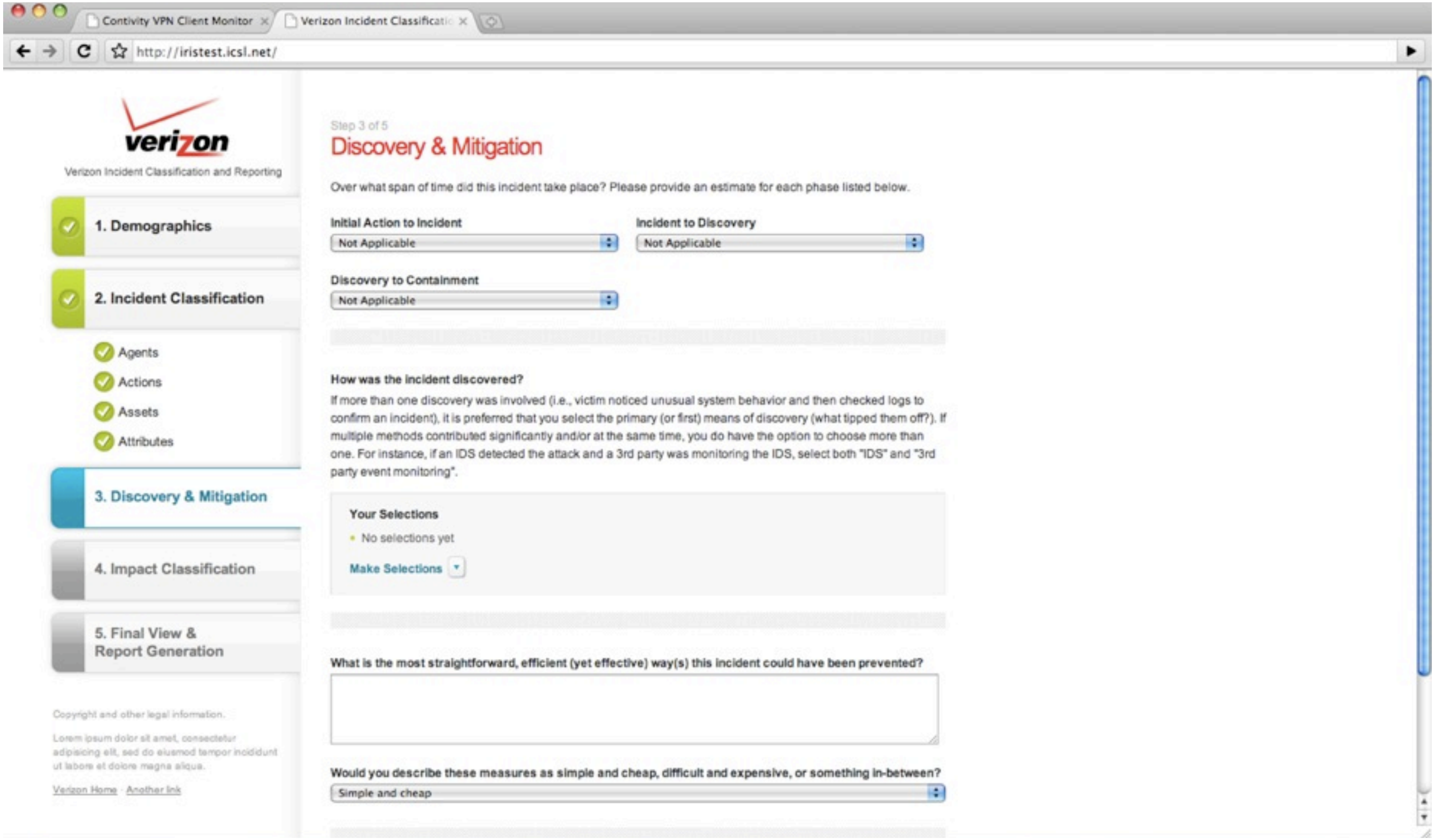
Card 16 of 50

LAST 4 YEARS	RUNS ABOVE AVERAGE (RAA)	RAA	WAR
		77.1	14.6
06 BOS		-11.1	-0.8
07 BOS		19.6	3.8
08 BOS		42.2	6.6
09 BOS		26.4	5.0
NEXT 5 YEARS	**PROJECTED BY STEVE SOMMER**	**124.1**	**24.3**
10 *PROJ*		29.1	5.3
11 *PROJ*		28.4	5.2
12 *PROJ*		24.5	4.8
13 *PROJ*		23.0	4.7
14 *PROJ*		19.1	4.3

🟦 Offense 🟩 Defense 🟥 Position Data source: FanGraphs.com

'10 SaberCards

VERIS Software (shhhhhh)


Contivity VPN Client Monitor
Verizon Incident Classificatio
http://iristest.icsl.net/
verizon
Verizon Incident Classification and Reporting
1. Demographics
2. Incident Classification
Agents
Actions
Assets
Attributes
3. Discovery & Mitigation
4. Impact Classification
5. Final View & Report Generation

Step 3 of 5

Discovery & Mitigation

Over what span of time did this incident take place? Please provide an estimate for each phase listed below.

Initial Action to Incident: Not Applicable	Incident to Discovery: Not Applicable
Discovery to Containment: Not Applicable	

How was the incident discovered?

If more than one discovery was involved (i.e., victim noticed unusual system behavior and then checked logs to confirm an incident), it is preferred that you select the primary (or first) means of discovery (what tipped them off?). If multiple methods contributed significantly and/or at the same time, you do have the option to choose more than one. For instance, if an IDS detected the attack and a 3rd party was monitoring the IDS, select both "IDS" and "3rd party event monitoring".

Your Selections

- No selections yet

Make Selections

What is the most straightforward, efficient (yet effective) way(s) this incident could have been prevented?

Would you describe these measures as simple and cheap, difficult and expensive, or something in-between?

Simple and cheap

Copyright and other legal information.

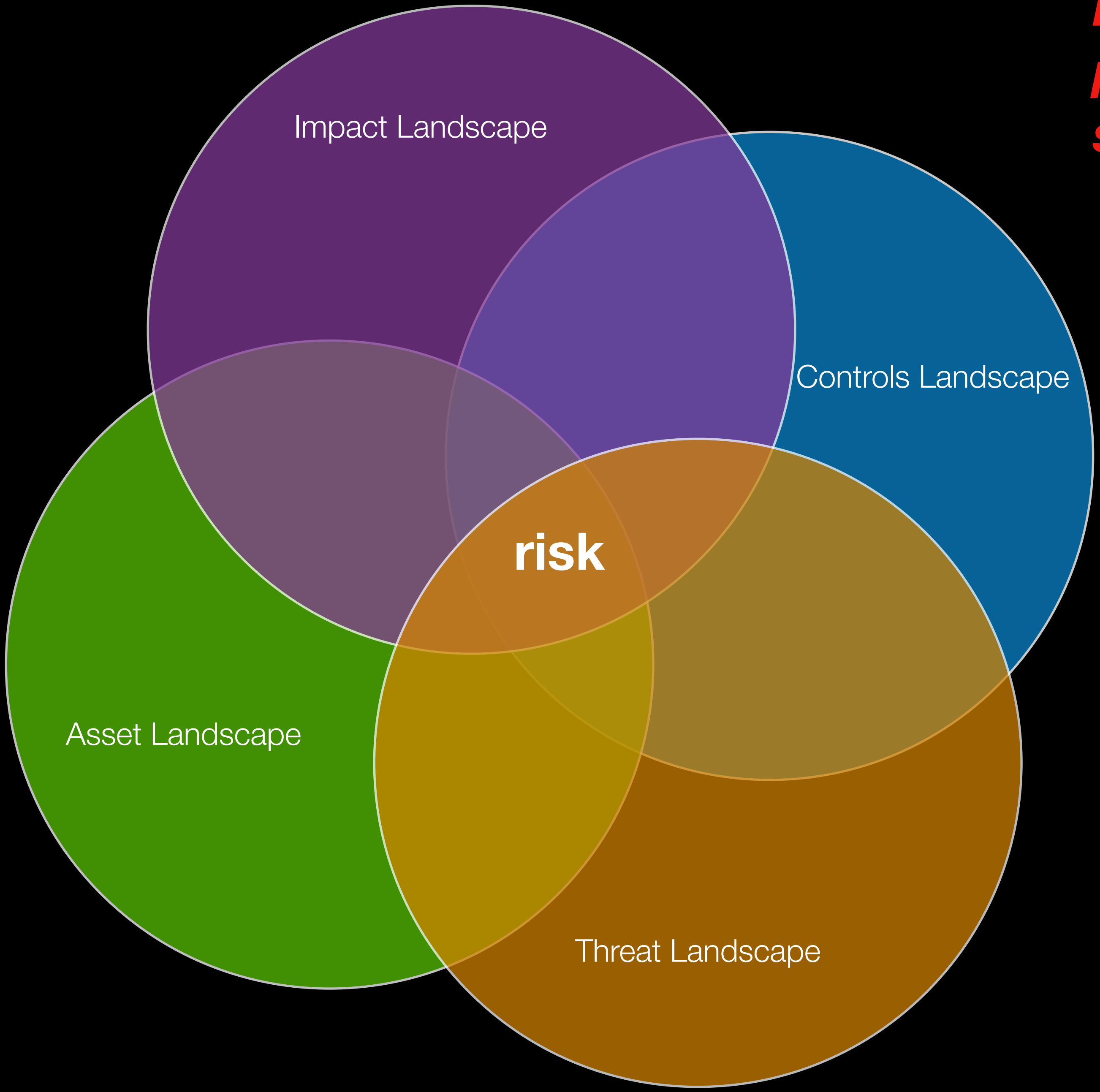
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Verizon Home · Another link

Using VERIS (DBIR) Data

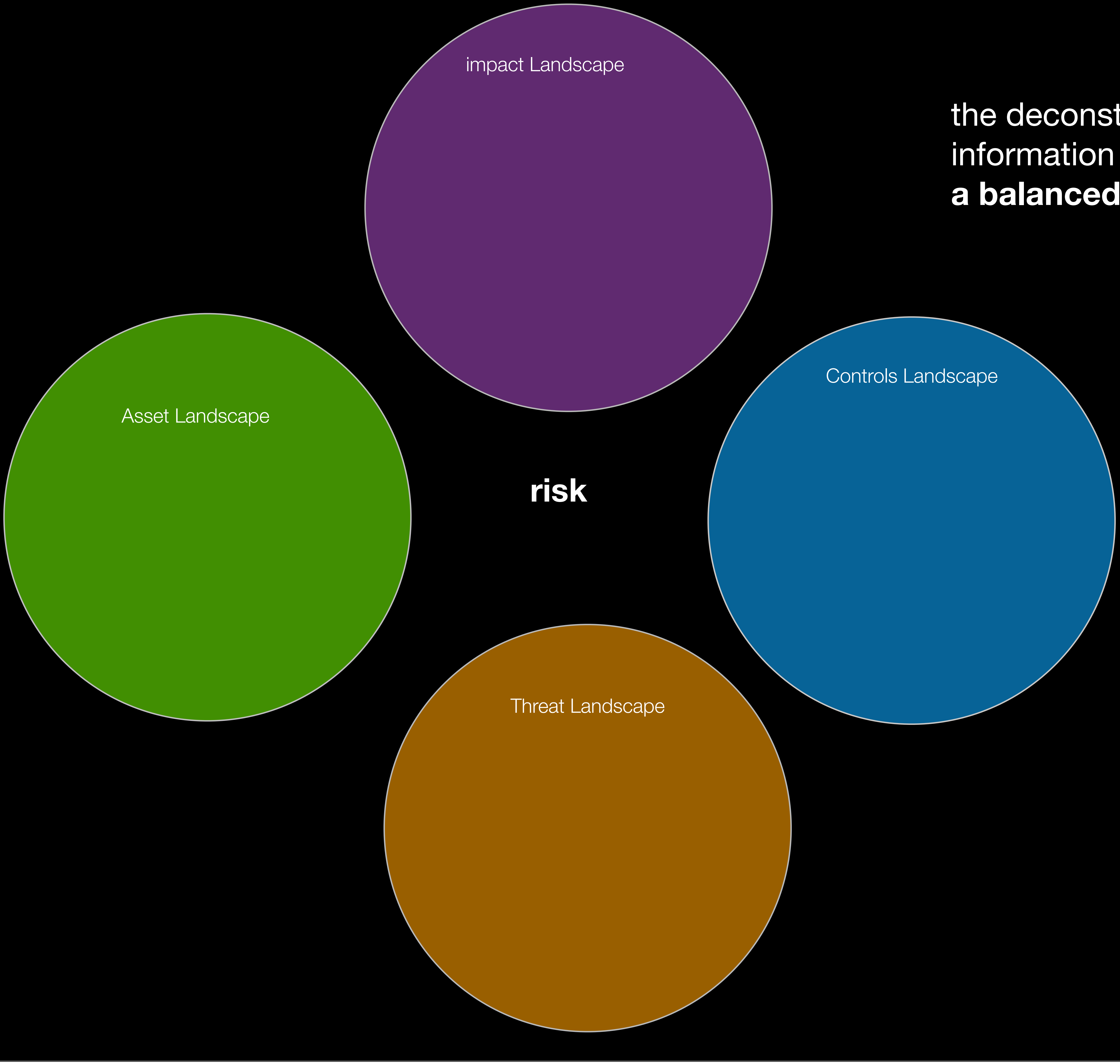
(data sharing)

- VERIS data can provide comparative analytics
- This would be extremely useful in a notional view of risk management
- Incidents are evidence of (in) effectiveness
    - hey Richard, time framing VERIS events might help answer the “why 2 hours” question you get!

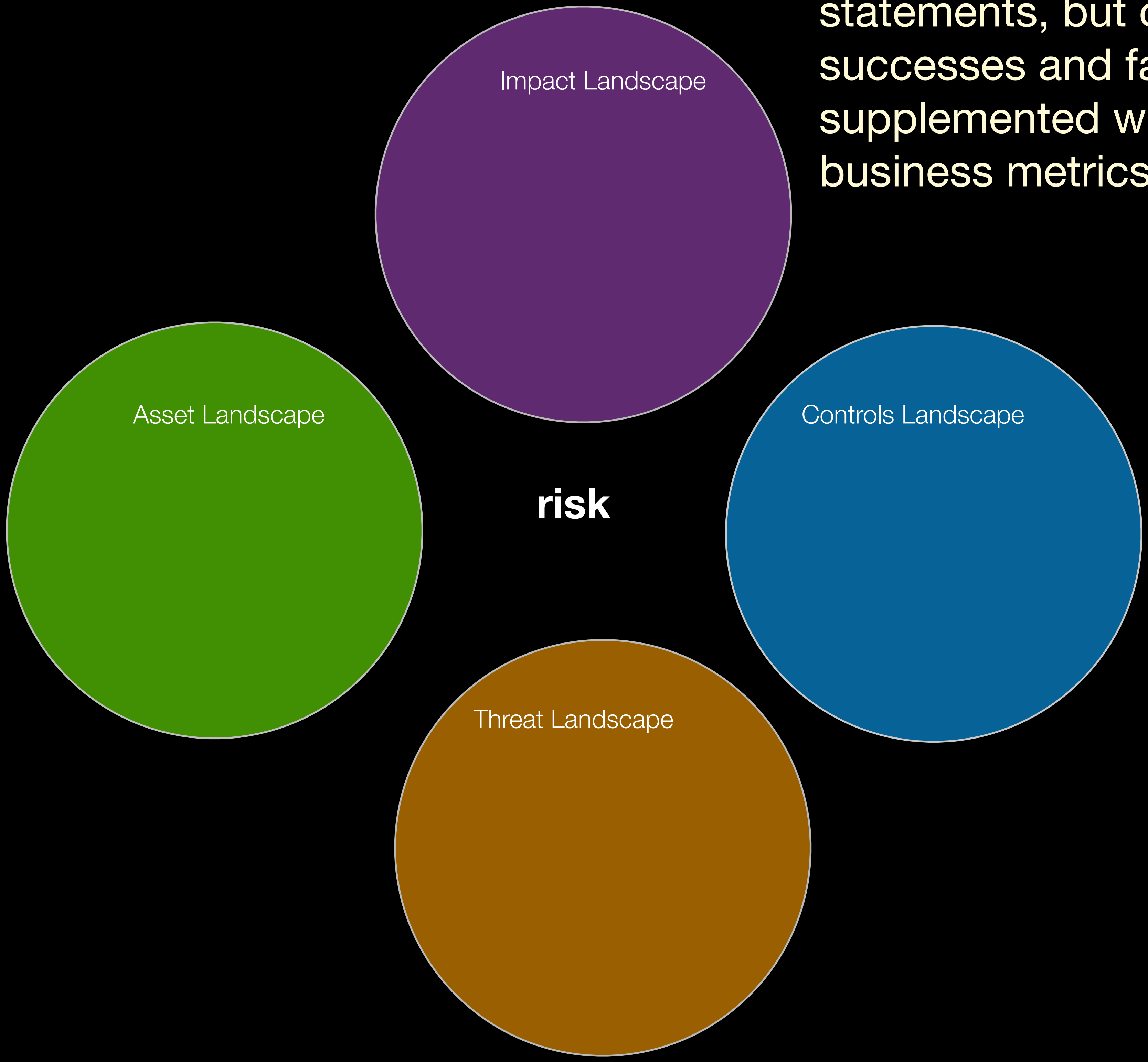


multitude of probabilistic point statements...

the deconstruction of risk information to create **a balanced scorecard?**



a VERIS-data based scorecard with synthesis not based on probabilistic point statements, but on correlation to successes and failures (can/should be supplemented with other operational and business metrics).



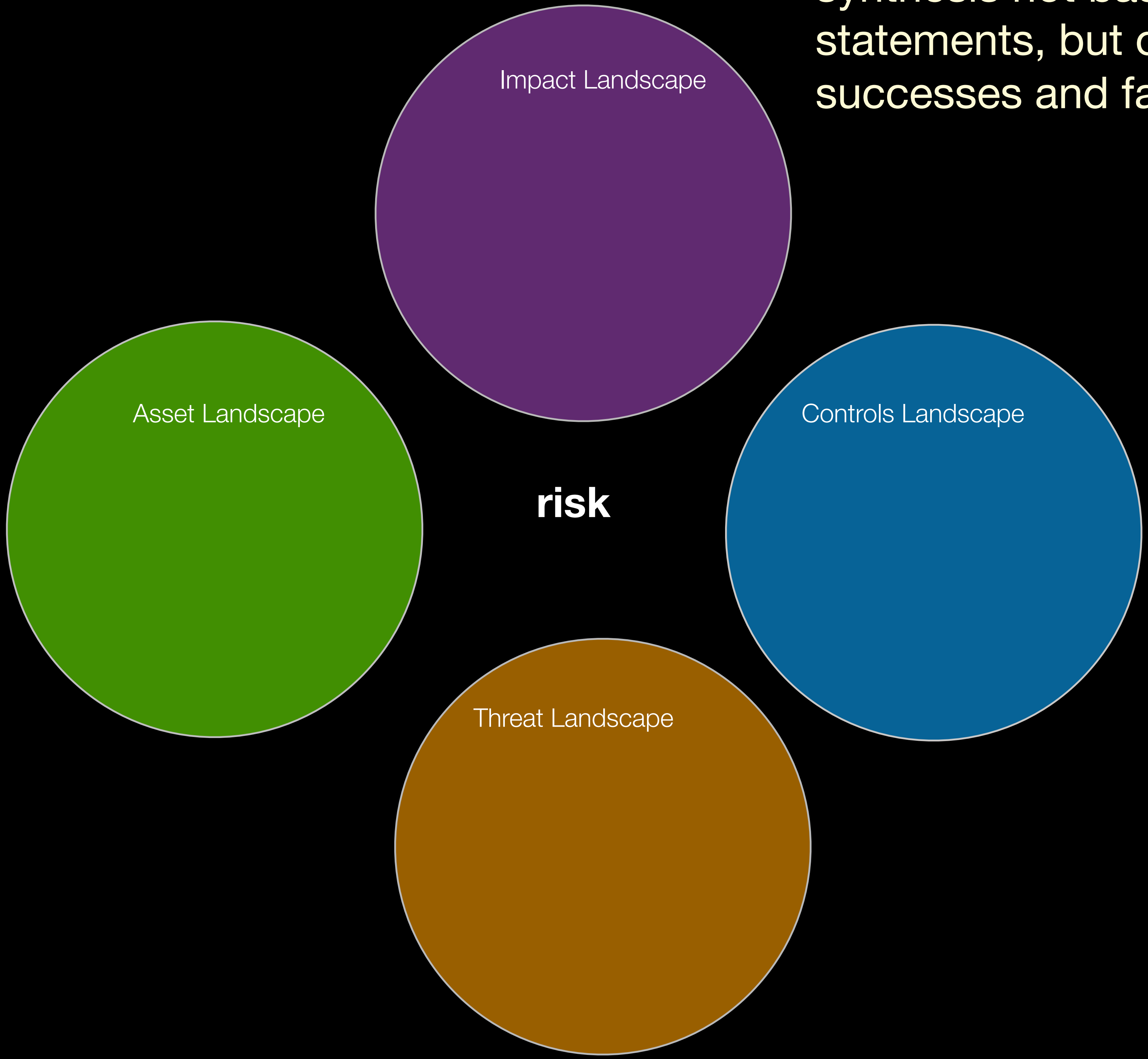
Threats
Frequencies
Capabilities
    Variety
    (Patterns of tactics)

Assets
Frequencies in incidents
vulnerability management
capability & management
metrics

Controls
capability & management
metrics
incidents back to decision
management

Impact
histories (internal, external)

a VERIS-data based scorecard with synthesis not based on probabilistic point statements, but on correlation to successes and failures.



Informative:
(We know these traits are more indicative of "failures" or "successes" - *esp. if we could ever build on Visible Ops for Security research*)

Comparative:
("We rank well" or "We suck eggs")

Business Relevant:
("Sucking eggs at these things leads to these sorts of compromise which leads to losses somewhere in this distribution.")

evidence based medicine, meet information security

What is evidence-based risk management?

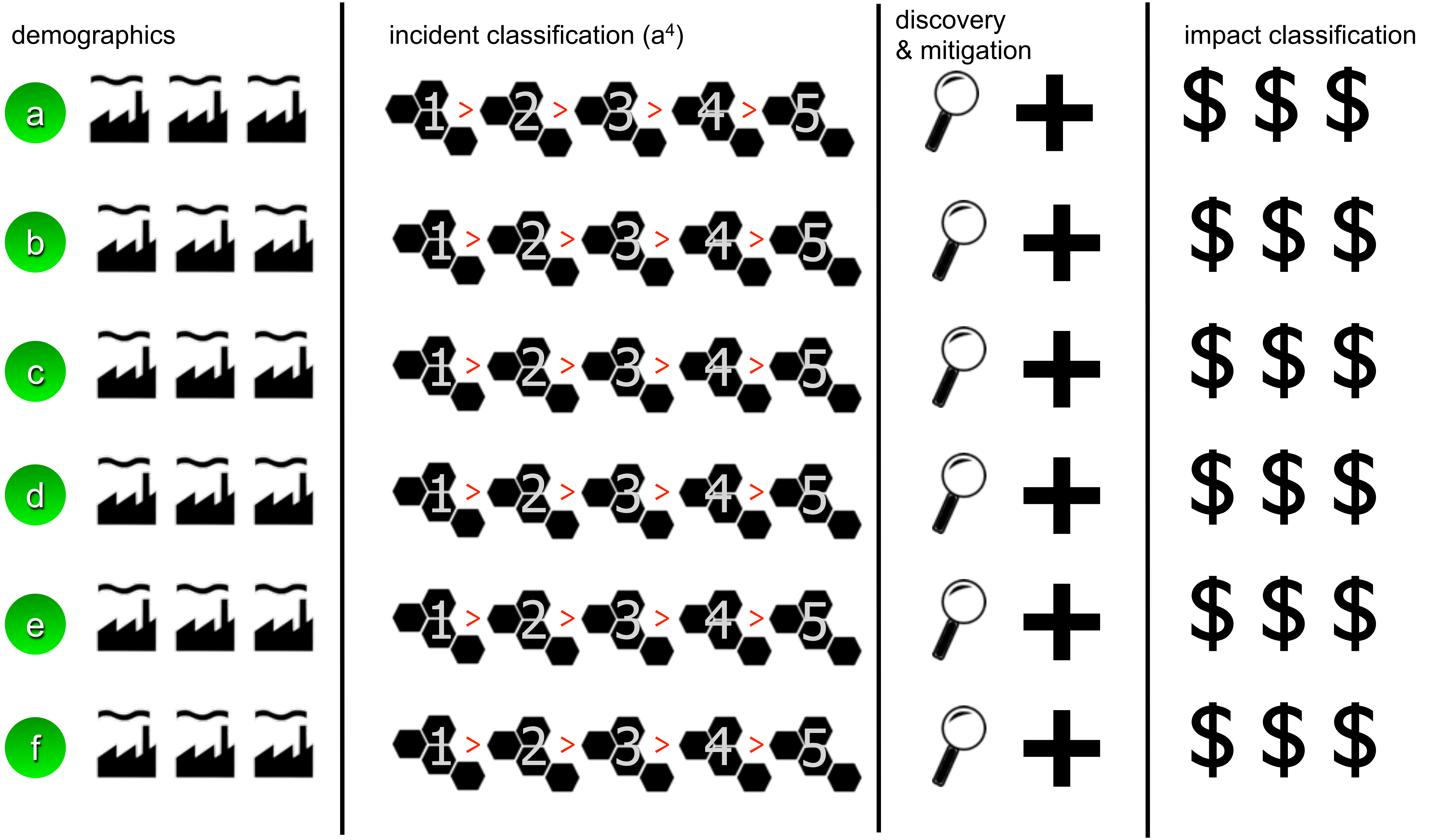
a deconstructed, notional view of risk

Risk Modeling becomes Operationally Important

Patterns are cool.

- (Chillin' Friederich Hayek)

case studies → data set

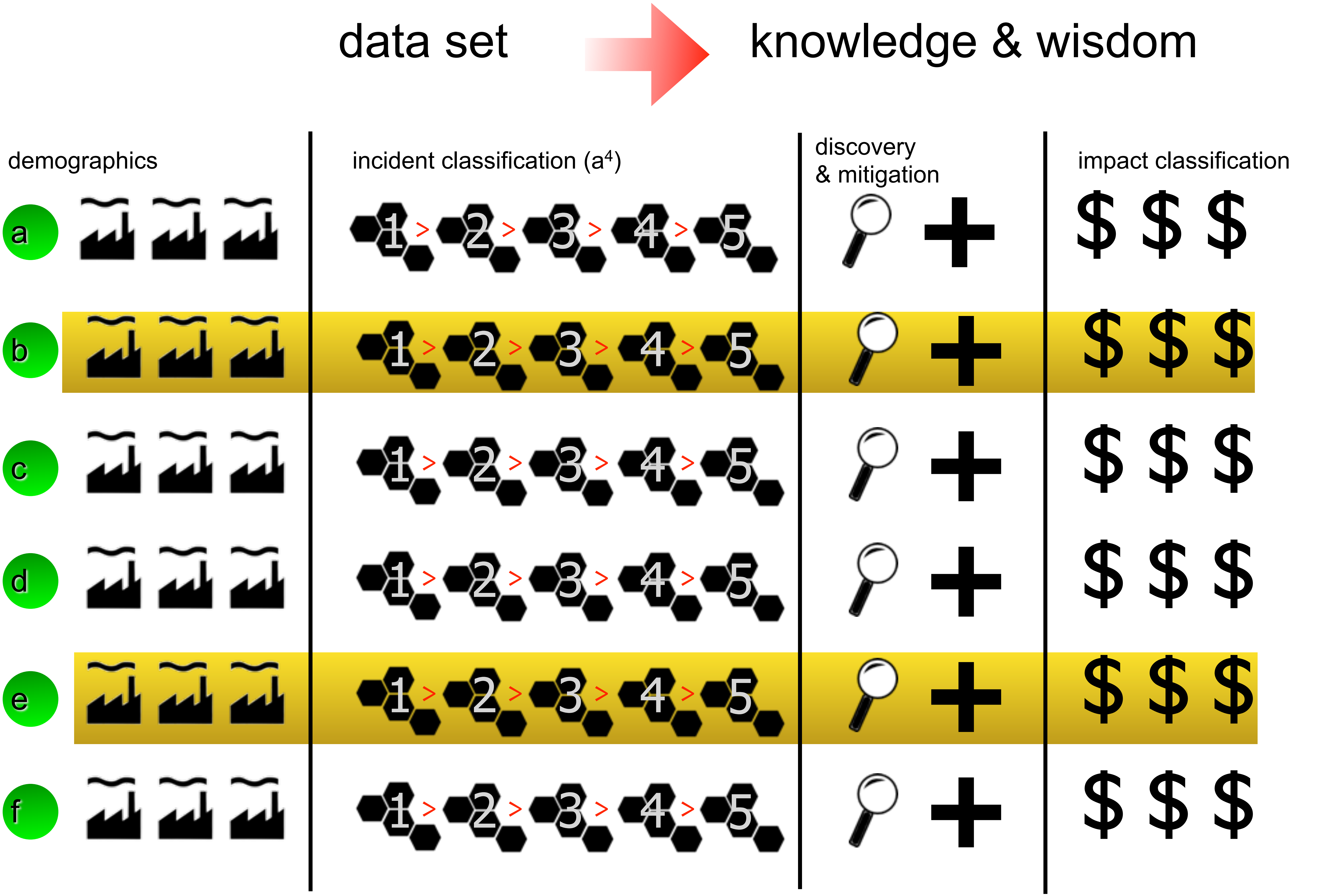


demographics

incident classification (a⁴)

discovery
& mitigation

impact classification



data set → knowledge & wisdom

demographics

incident classification (a^4)

discovery
& mitigation

impact classification

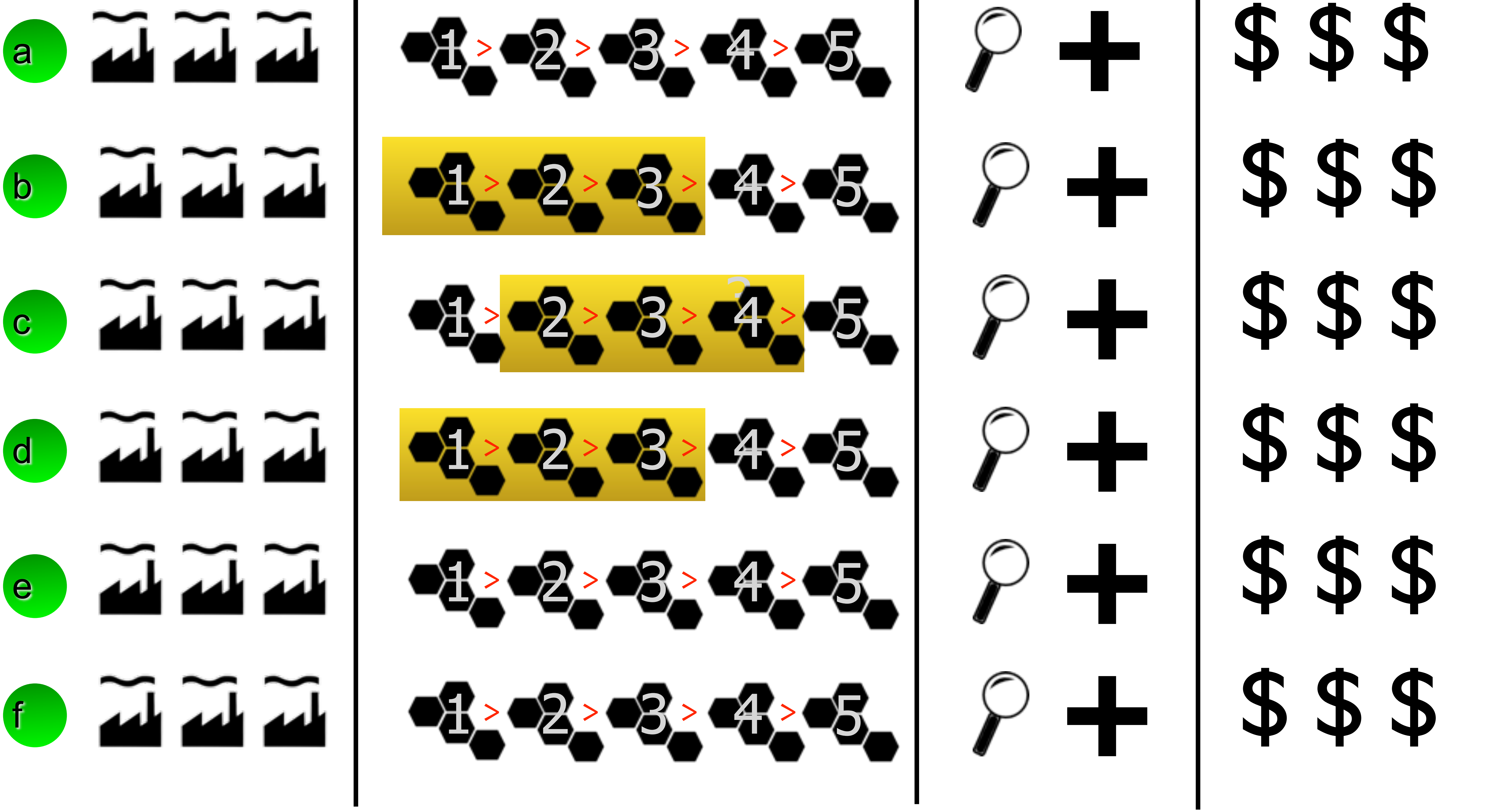
threat information

demographics

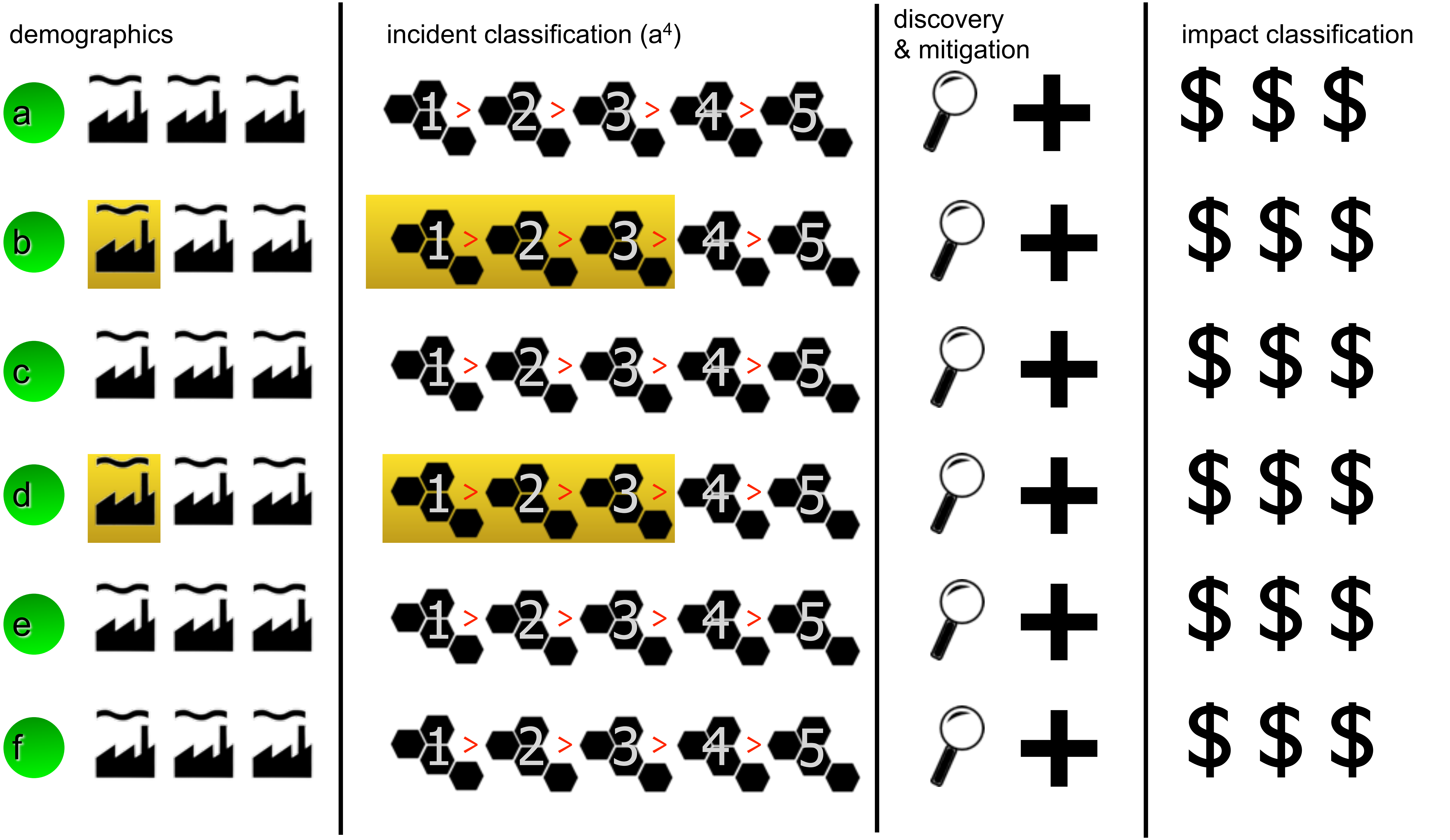
incident classification (a^4)

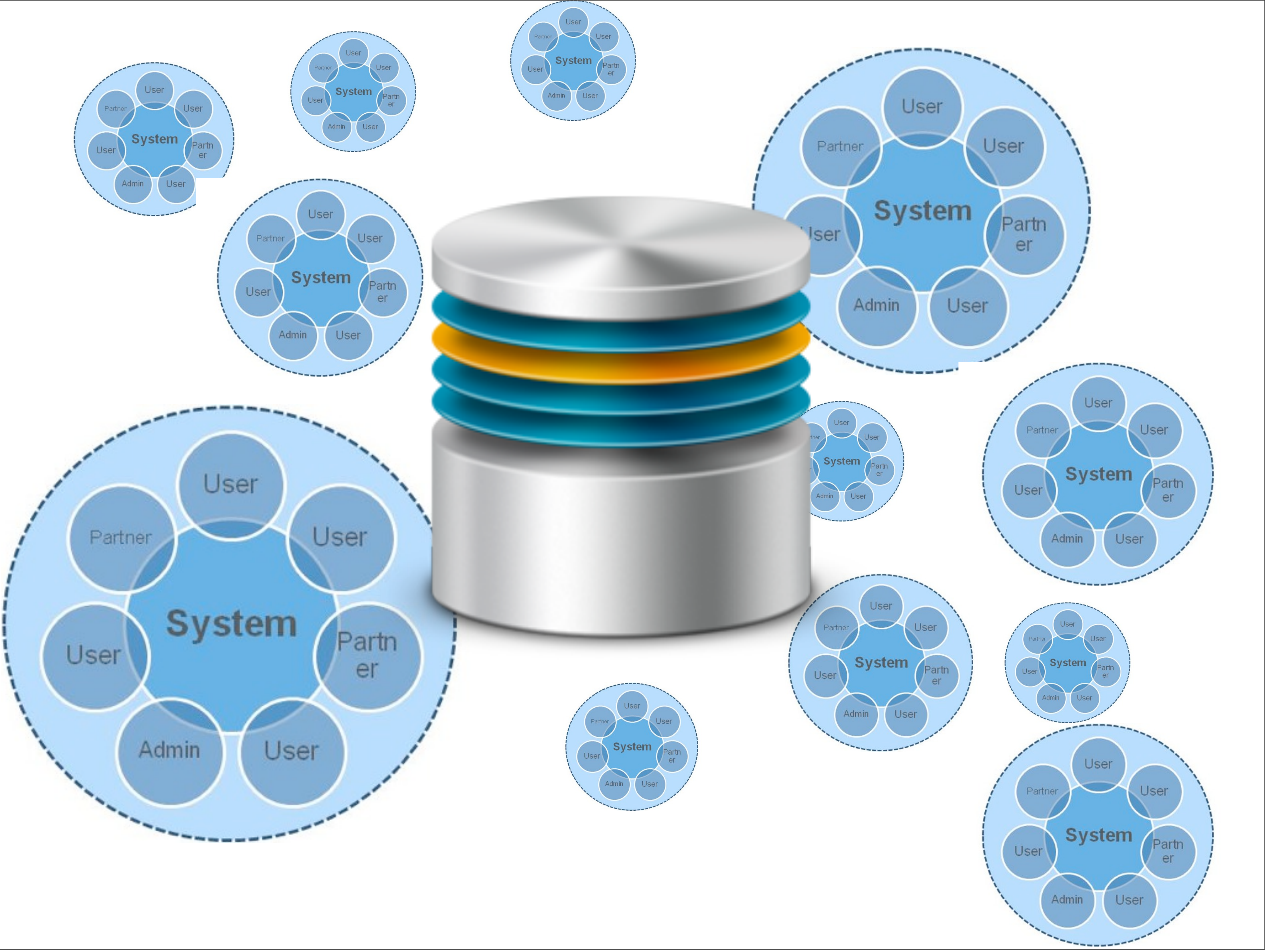
discovery
& mitigation

impact classification



threat information - shared data




User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
User
System
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User
User
Partner
User
System
User
Partn
er
Admin
User

evidence-based risk management:

data driven treatment.

verizon
Cybertrust Security

https://verisframework.wiki.zoho.com

@alexhutton