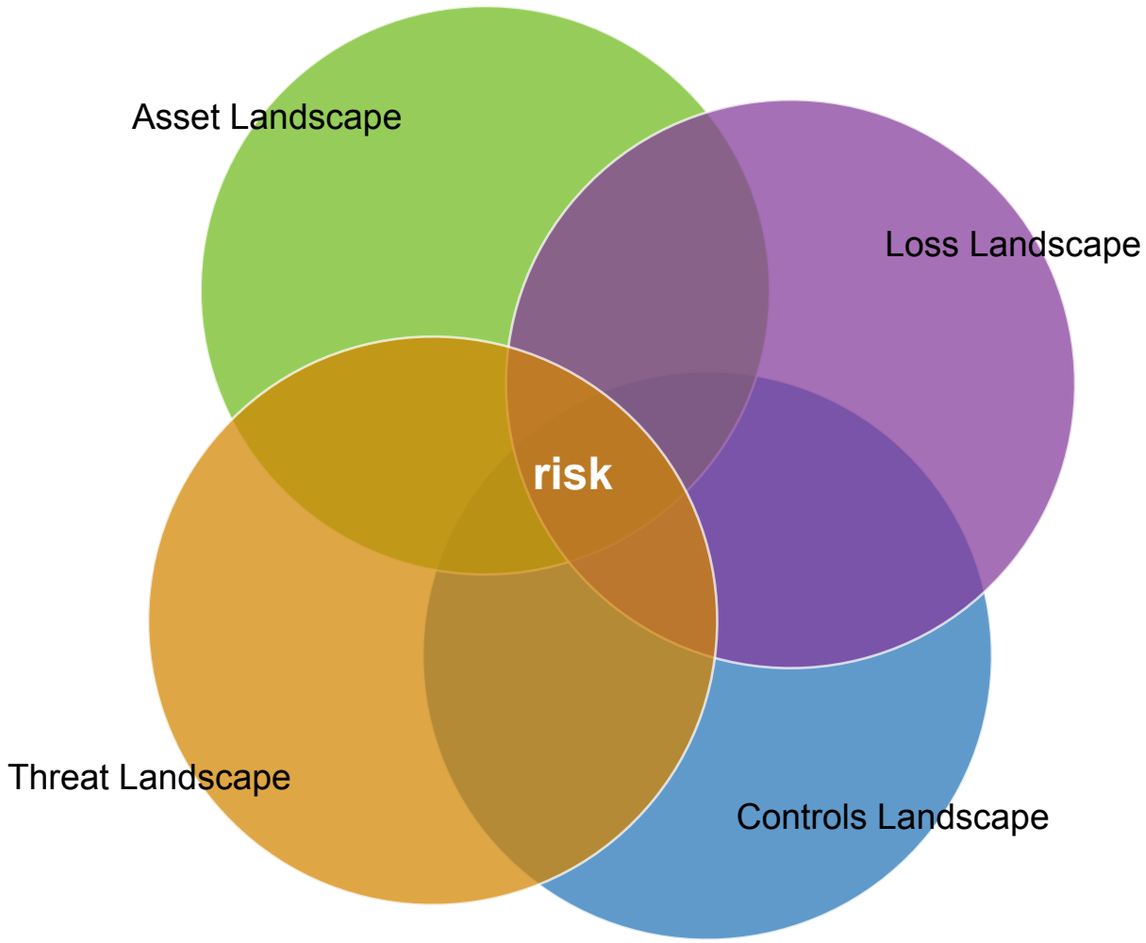
Cybertrust Security

VerIS - a Framework for Gathering Risk Management Information from Security Incidents

Wade Baker
Alex Hutton
Chris Porter
Risk Intelligence
Verizon Cybertrust Security

Cybertrust Security

Verizon Risk Intelligence View of Information Risk Management

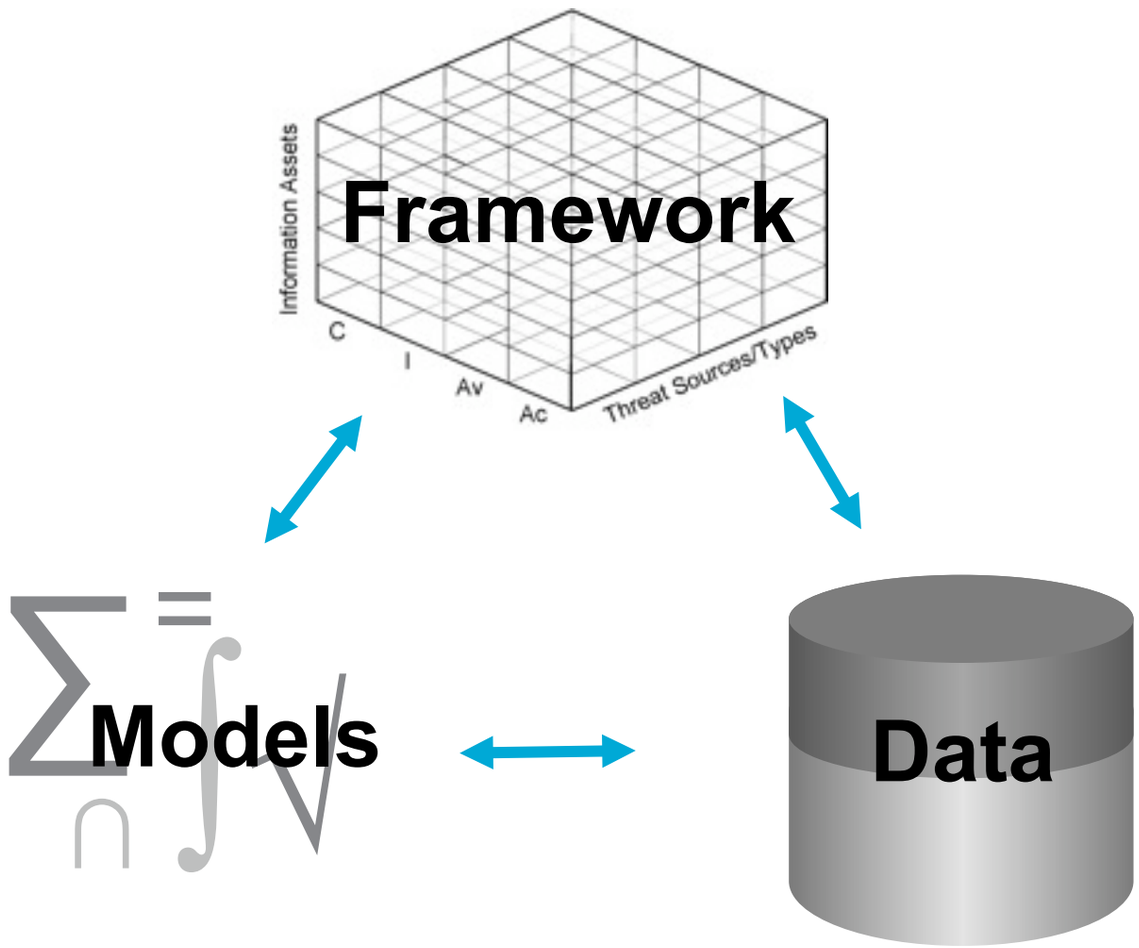


ANY USEFUL DATA WILL BE INFORMATION ABOUT ONE (OR MORE) OF THE LANDSCAPES

(or derived values created by modeling the interactions between landscape data)

Cybertrust Security

Risk Management: Operating Model



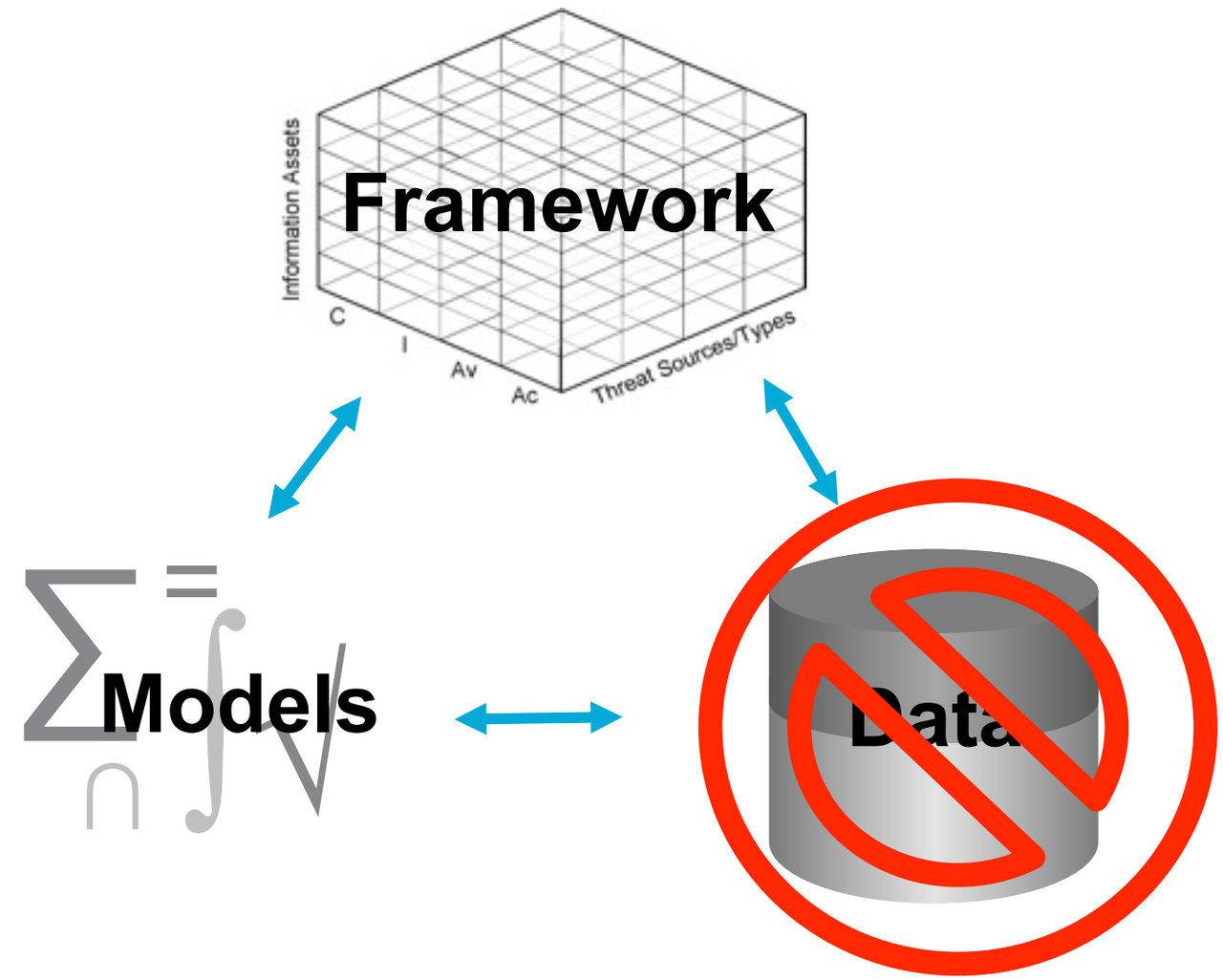
verizon
Cybertrust Security

Problems in Information Risk Management

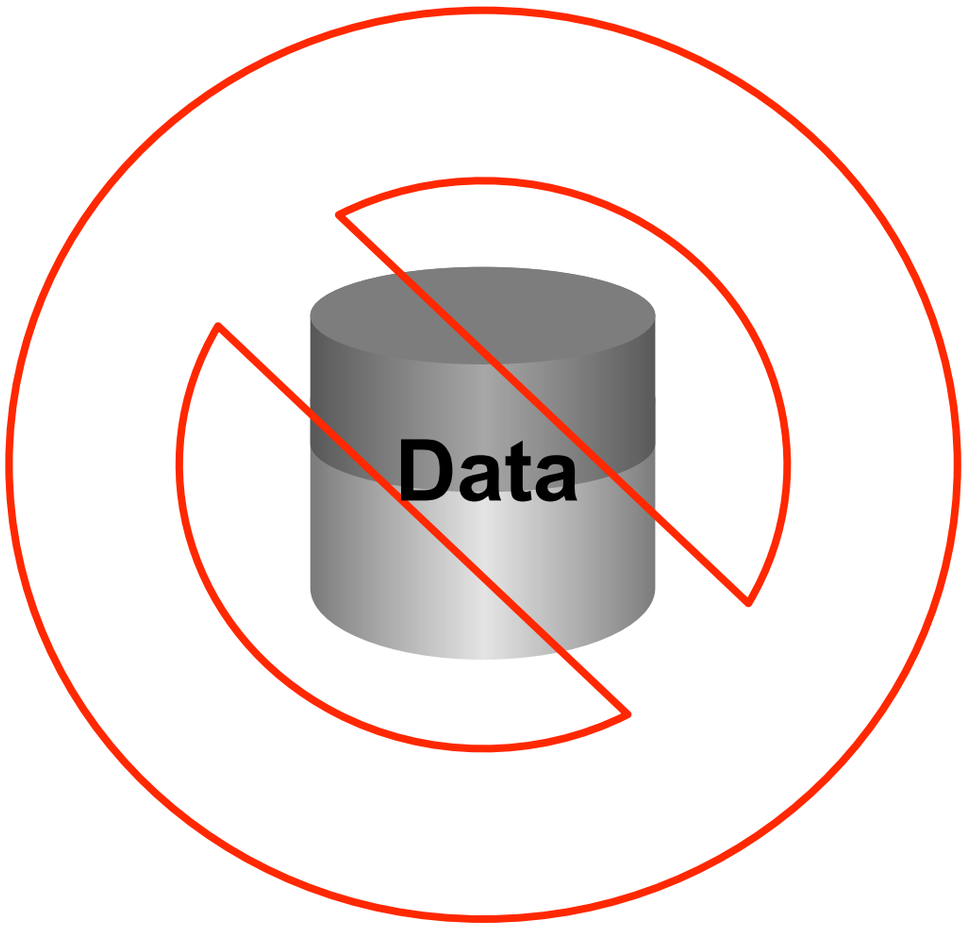
- data / frameworks / models
  - equivocality & uncertainty

Cybertrust Security

Risk Management: Operating Model

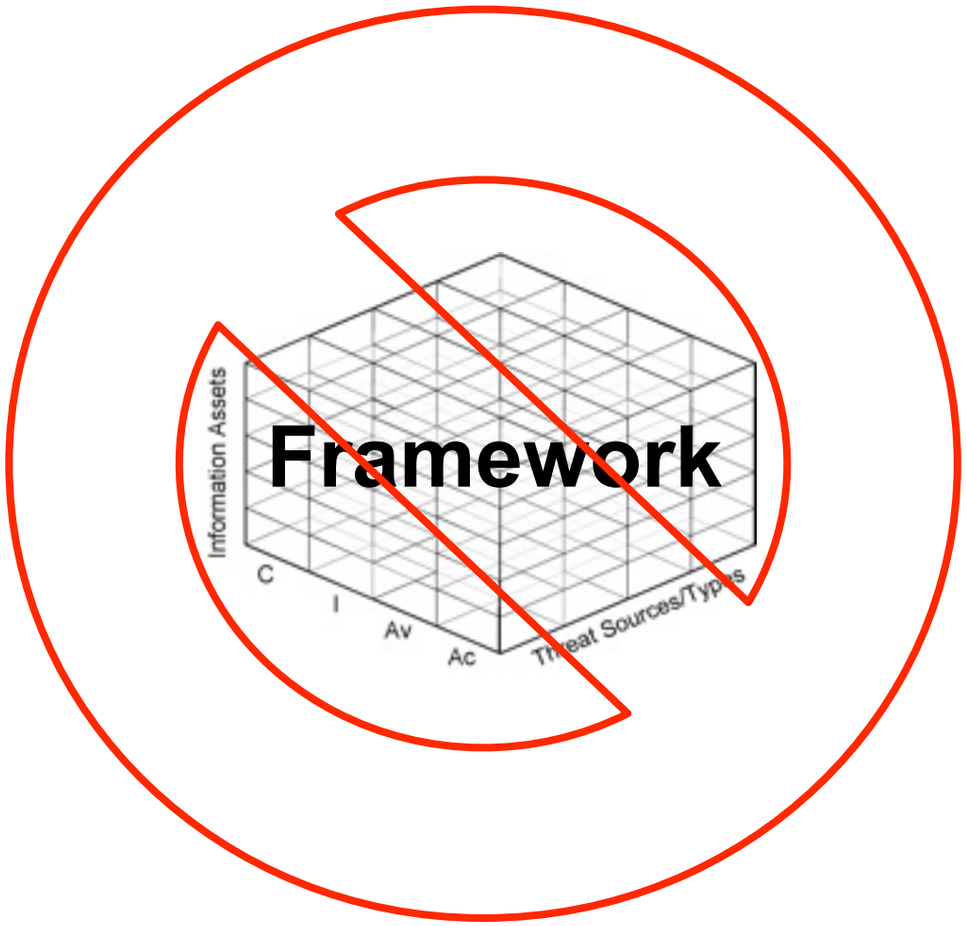


Cybertrust Security

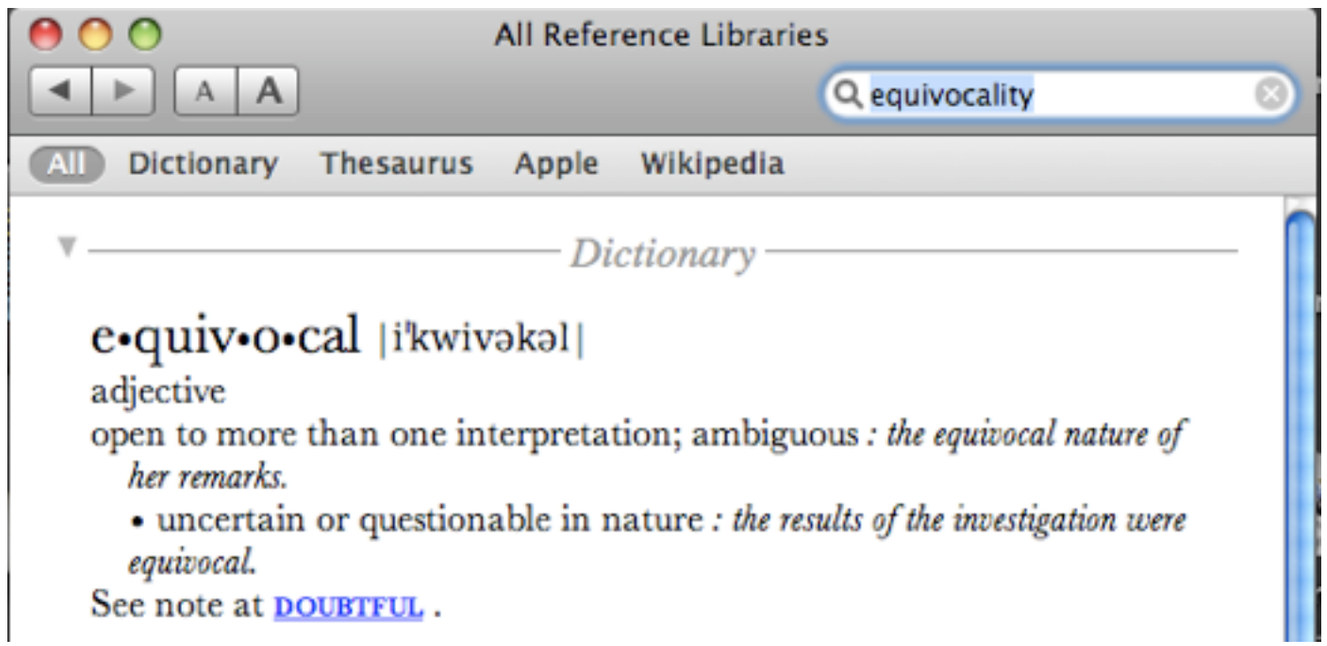


=UNCERTAINTY

verizon
Cybertrust Security



=EQUIVOCALITY



verizon
Cybertrust Security

Lessons from Organizational Theory

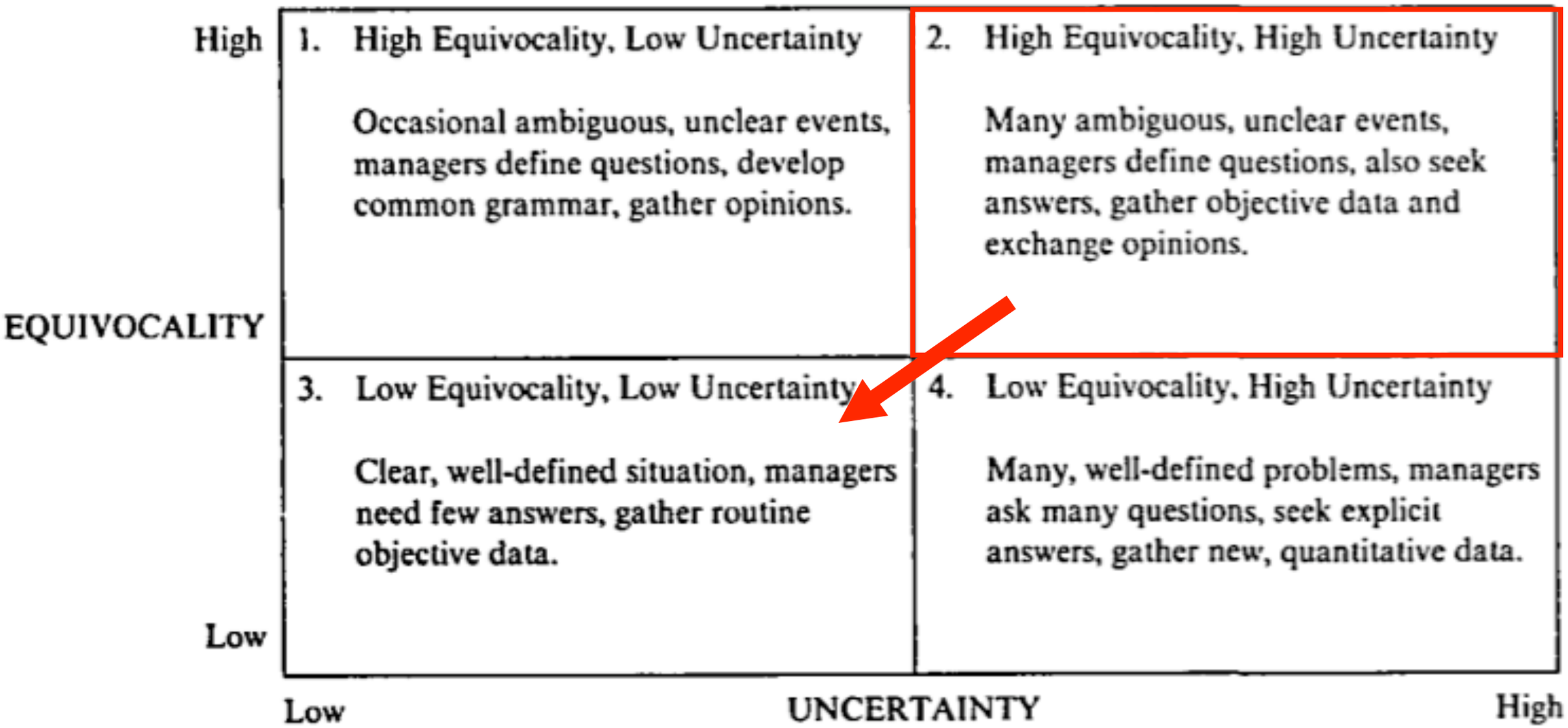


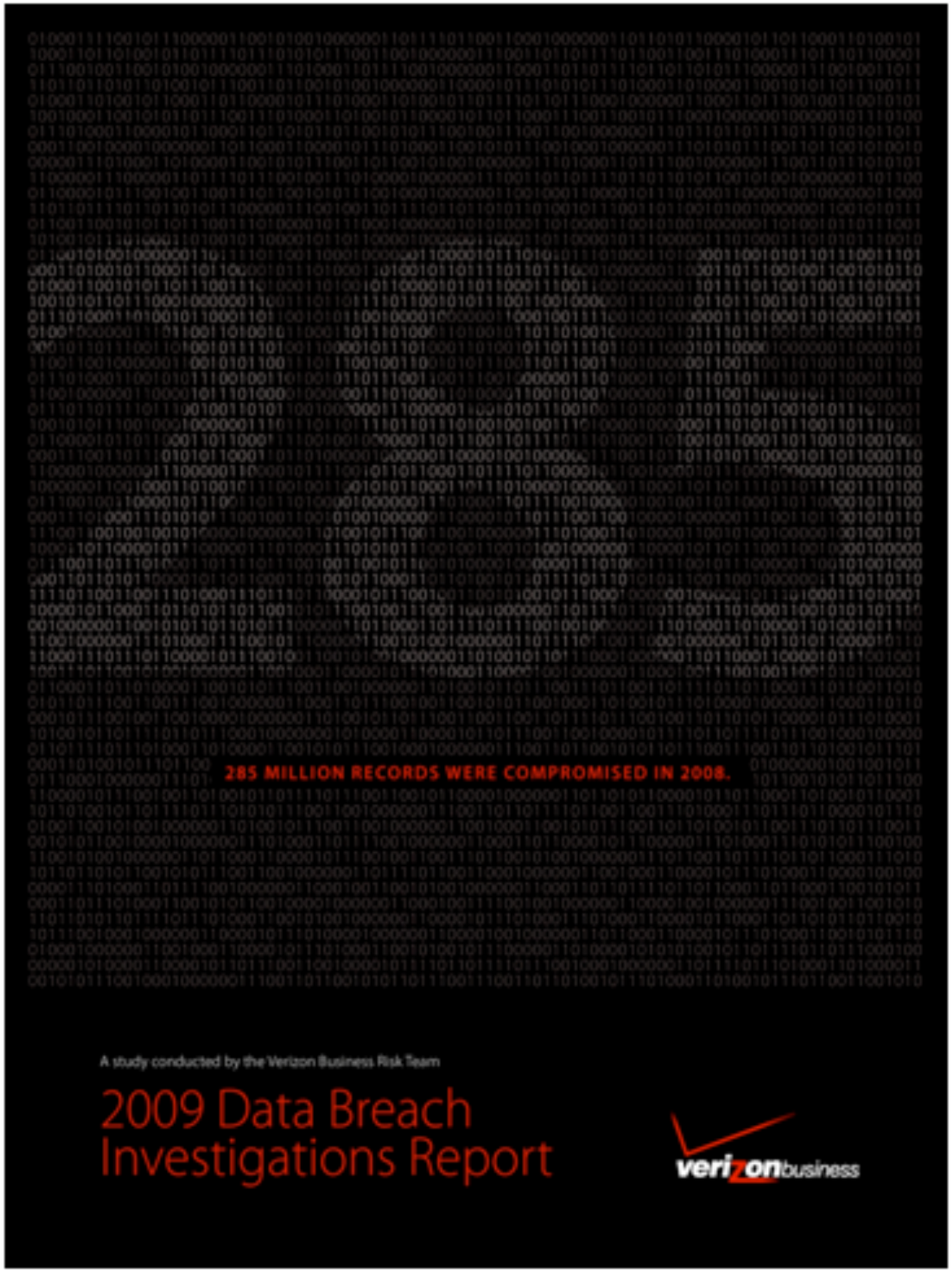
FIGURE 1. Hypothesized Framework of Equivocality and Uncertainty on Information Requirements.

DAFT, R. AND LENGEL, R. 1986. Organizational Information Requirements, Media Richness and Structural Design. *Management Science, 32*, 4, 554-569.

verizon
Cybertrust Security

Verizon has shared data

Cybertrust Security



- 2009 – over 600 cases
- 2010 – between 1000 & 1400

Cybertrust Security

Verizon is sharing our framework

Cybertrust Security

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

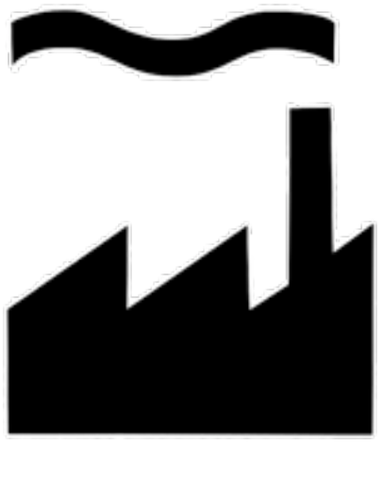
Cybertrust Security

What makes up the VerIS framework?

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

Cybertrust Security

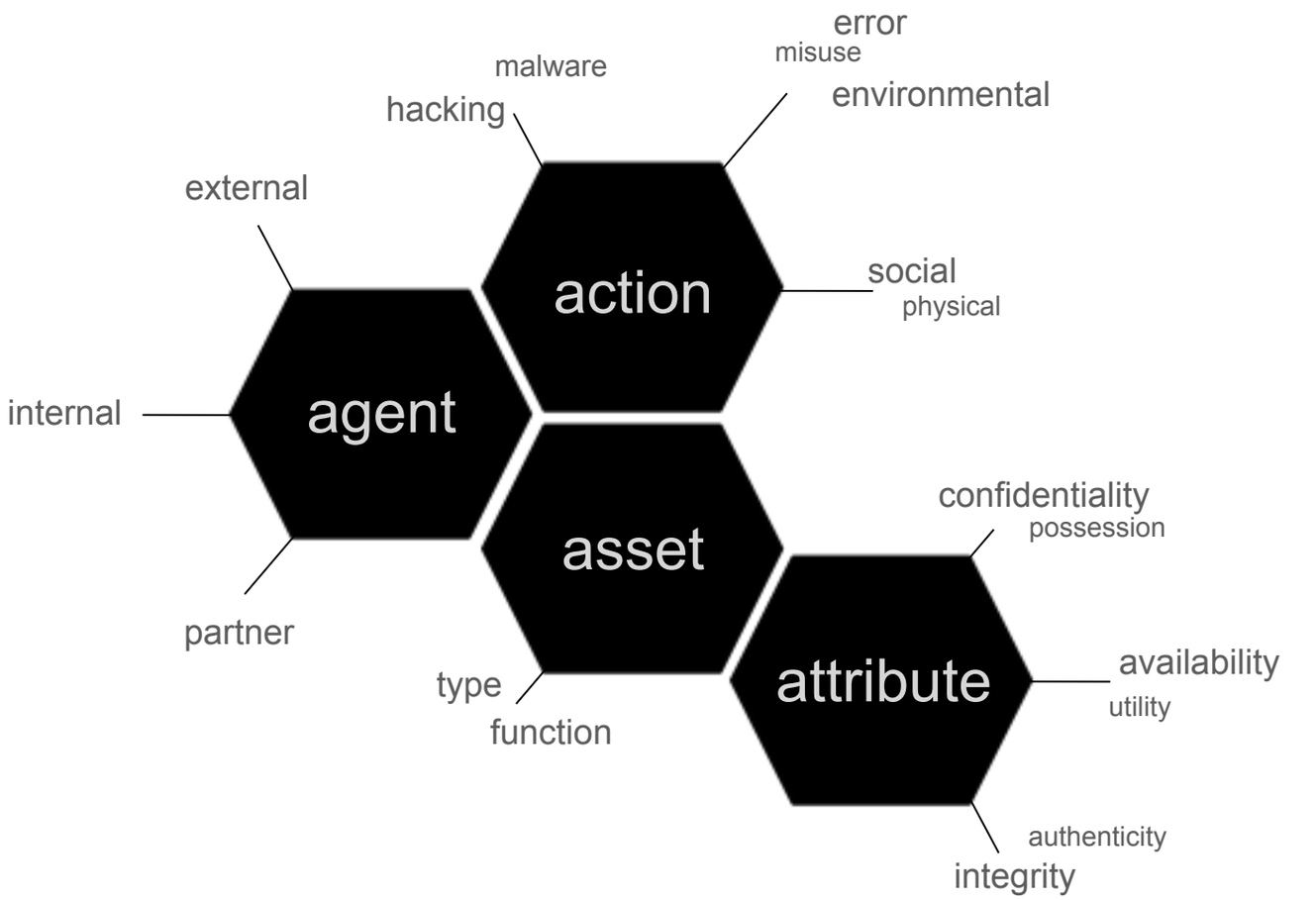
demographics



- company industry
- company size
- geographic location
  - of business unit in incident
- size of security department

Cybertrust Security

incident classification



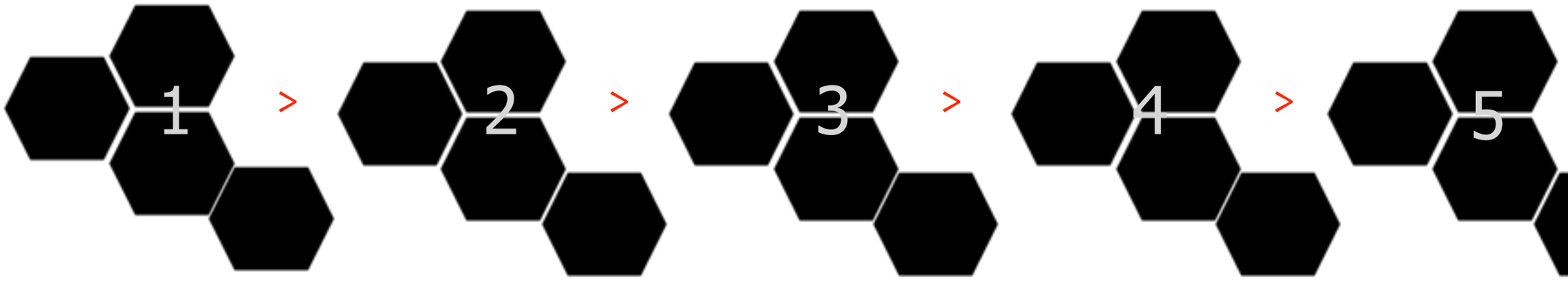
- agent
  - what acts against us
- asset
  - what the agent acts against
- action
  - what the agent does to the asset
- attribute
  - the result of the agent's action against the asset

Cybertrust Security

incident classification

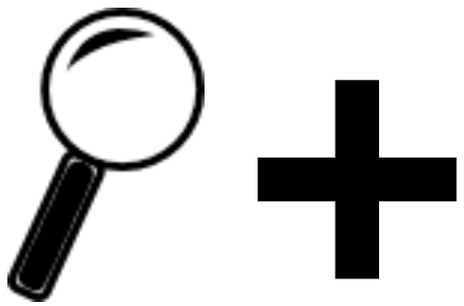
a⁴ event model

the series of events (a⁴) creates an “attack model”



verizon
Cybertrust Security

discovery & mitigation



- incident timeline
- discovery method
- evidence sources
- control capability
- corrective action

- most straightforward manner in which the incident could be prevented
- the cost of preventative controls

Cybertrust Security

Impact classification

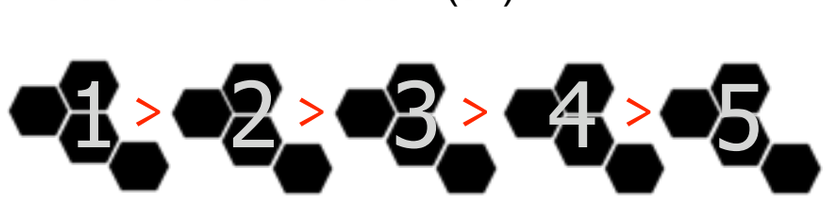
- impact categorization
  - sources of Impact (direct, indirect)
  - *similar to iso 27005/FAIR*
- impact estimation
  - distribution for amount of impact
- impact qualification
  - relative impact rating

Cybertrust Security

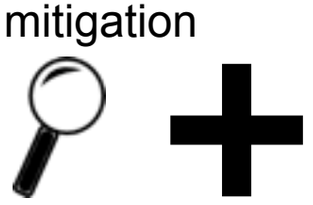
incident narrati[illegible] incident metrics

demographics

incident classification (a^4)



discovery & mitigation



impact classification

verizon
Cybertrust Security

case studies → data set

demographics	incident classification (a^4)	discovery & mitigation	impact classification
a	1 > 2 > 3 > 4 > 5	+	$ $ $
b	1 > 2 > 3 > 4 > 5	+	$ $ $
c	1 > 2 > 3 > 4 > 5	+	$ $ $
d	1 > 2 > 3 > 4 > 5	+	$ $ $
e	1 > 2 > 3 > 4 > 5	+	$ $ $
f	1 > 2 > 3 > 4 > 5	+	$ $ $

verizon
Cybertrust Security

data set → knowledge & wisdom

	demographics	incident classification (a^4)	discovery & mitigation	impact classification
a		1 > 2 > 3 > 4 > 5	+	$ $ $
b		1 > 2 > 3 > 4 > 5	+	$ $ $
c		1 > 2 > 3 > 4 > 5	+	$ $ $
d		1 > 2 > 3 > 4 > 5	+	$ $ $
e		1 > 2 > 3 > 4 > 5	+	$ $ $
f		1 > 2 > 3 > 4 > 5	+	$ $ $

threat modeling

demographics	incident classification (a^4)	discovery & mitigation	impact classification
a	1 > 2 > 3 > 4 > 5	+	$ $ $
b	1 > 2 > 3 > 4 > 5	+	$ $ $
c	1 > 2 > 3 > 4 > 5	+	$ $ $
d	1 > 2 > 3 > 4 > 5	+	$ $ $
e	1 > 2 > 3 > 4 > 5	+	$ $ $
f	1 > 2 > 3 > 4 > 5	+	$ $ $

threat modeling

demographics	incident classification (a^4)	discovery & mitigation	impact classification
a	1 > 2 > 3 > 4 > 5	+	$ $ $
b	1 > 2 > 3 > 4 > 5	+	$ $ $
c	1 > 2 > 3 > 4 > 5	+	$ $ $
d	1 > 2 > 3 > 4 > 5	+	$ $ $
e	1 > 2 > 3 > 4 > 5	+	$ $ $
f	1 > 2 > 3 > 4 > 5	+	$ $ $

impact modeling

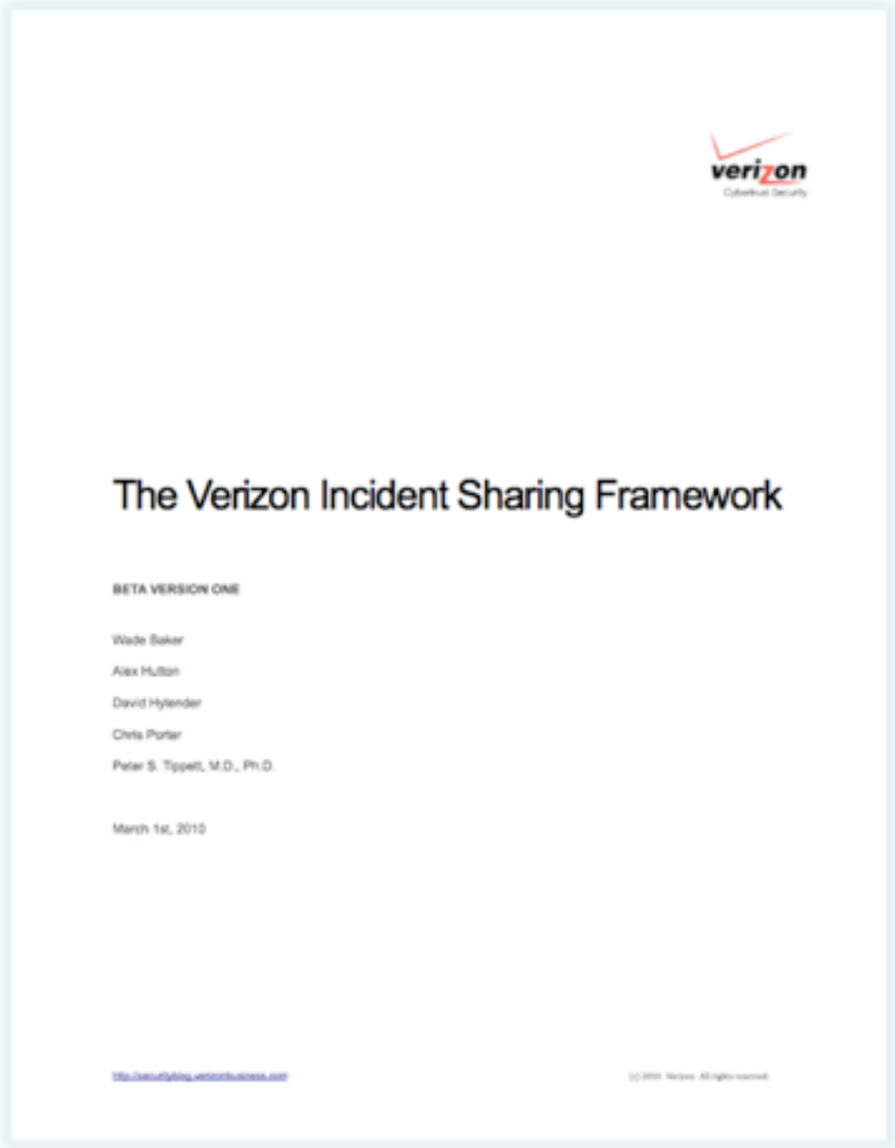
demographics	incident classification (a^4)	discovery & mitigation	impact classification
a	1 > 2 > 3 > 4 > 5	+	$ $ $
b	1 > 2 > 3 > 4 > 5	+	$ $ $
c	1 > 2 > 3 > 4 > 5	+	$ $ $
d	1 > 2 > 3 > 4 > 5	+	$ $ $
e	1 > 2 > 3 > 4 > 5	+	$ $ $
f	1 > 2 > 3 > 4 > 5	+	$ $ $

verizon
Cybertrust Security

impact modeling

demographics	incident classification (a^4)	discovery & mitigation	impact classification
a	1 > 2 > 3 > 4 > 5	+	$ $ $
b	1 > 2 > 3 > 4 > 5	+	$ $ $
c	1 > 2 > 3 > 4 > 5	+	$ $ $
d	1 > 2 > 3 > 4 > 5	+	$ $ $
e	1 > 2 > 3 > 4 > 5	+	$ $ $
f	1 > 2 > 3 > 4 > 5	+	$ $ $

Cybertrust Security



The Verizon Incident Sharing Framework

BETA VERSION ONE

Wade Baker
Alex Hutton
David Hylender
Chris Porter
Peter S. Tippett, M.D., Ph.D.

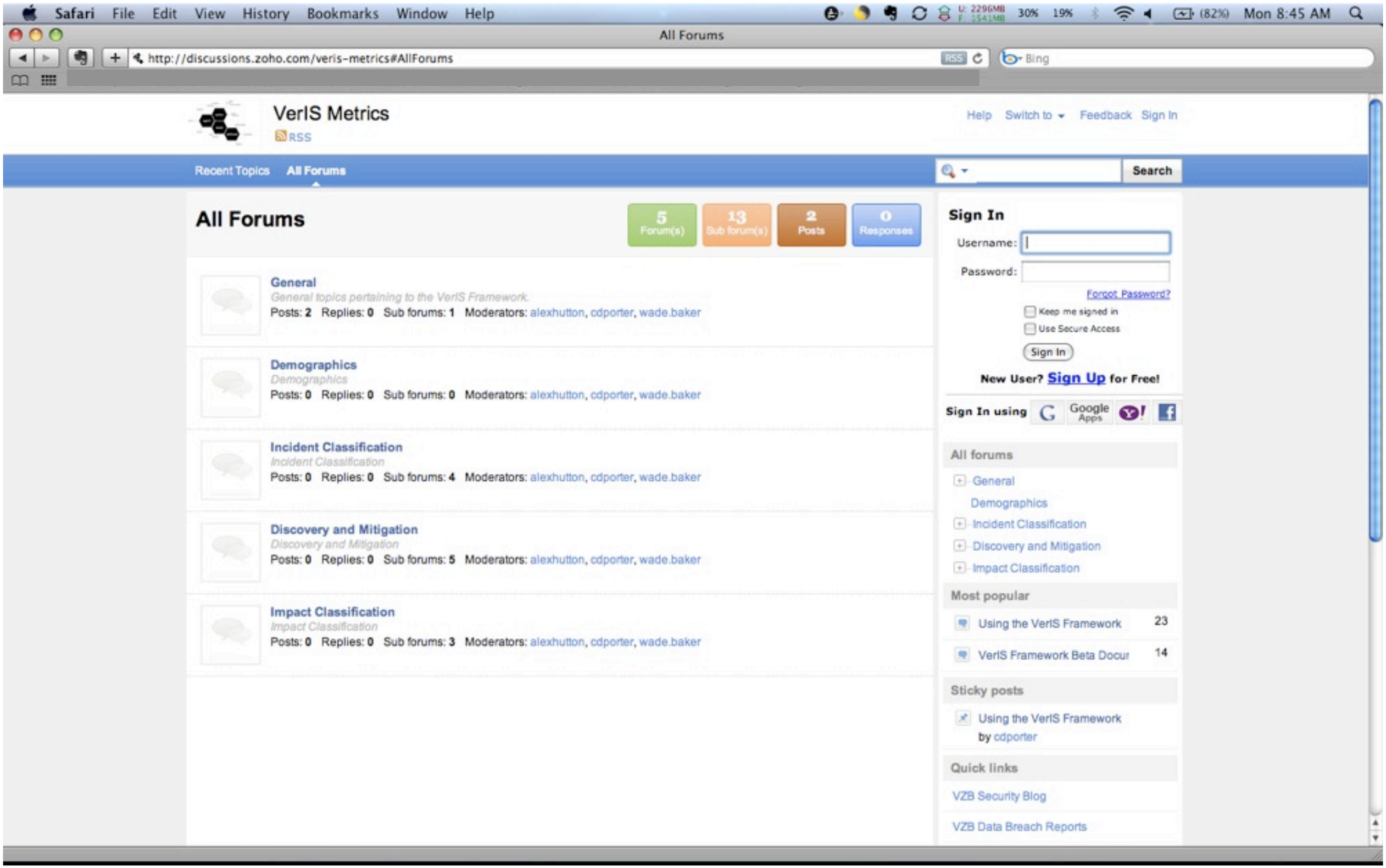
March 1st, 2010

1 1.1 2 Date of the Incident

3 ***Purpose:***	Facilitates trending over time.
Notes: 4	Select the month and year the incident occurred.
5 ***Question Type:***	Single Select for Month; Number field for Year
Suggested Options: 6	• Month: [List of months]
Miscellaneous: 7	While the exact date of the incident could be used, the month and year allows trending and provides some measure of de-identification for data sharing purposes. Using only the year provides even more.

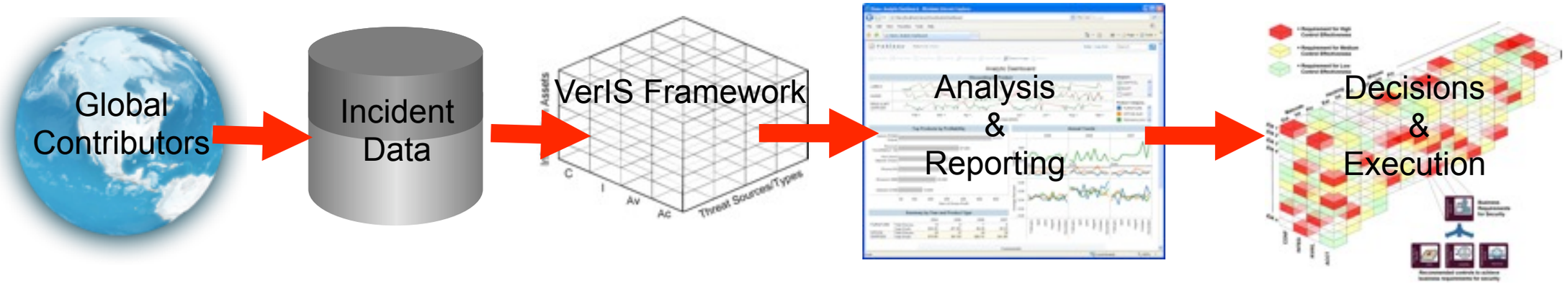
1.1 Date of the Incident

Purpose:	Facilitates trending over time.
Notes:	Select the month and year the incident occurred.
Question Type:	Single Select for Month; Number field for Year
Suggested Options:	• Month: [List of months] • Year: NA
Miscellaneous:	While the exact date of the incident could be used, the month and year allows trending and provides some measure of de-identification for data sharing purposes. Using only the year provides even more.


Safari File Edit View History Bookmarks Window Help
Mon 8:45 AM
All Forums
http://discussions.zoho.com/veris-metrics#AllForums
Bing
VerIS Metrics
RSS
Help Switch to Feedback Sign In
Recent Topics All Forums
Search
All Forums
5 Forum(s)
13 Sub forum(s)
2 Posts
0 Responses
General
General topics pertaining to the VerIS Framework.
Posts: 2 Replies: 0 Sub forums: 1 Moderators: alexhutton, cdporter, wade.baker
Demographics
Demographics
Posts: 0 Replies: 0 Sub forums: 0 Moderators: alexhutton, cdporter, wade.baker
Incident Classification
Incident Classification
Posts: 0 Replies: 0 Sub forums: 4 Moderators: alexhutton, cdporter, wade.baker
Discovery and Mitigation
Discovery and Mitigation
Posts: 0 Replies: 0 Sub forums: 5 Moderators: alexhutton, cdporter, wade.baker
Impact Classification
Impact Classification
Posts: 0 Replies: 0 Sub forums: 3 Moderators: alexhutton, cdporter, wade.baker
Sign In
Username:
Password:
Forgot Password?
Keep me signed in
Use Secure Access
Sign In
New User? Sign Up for Free!
Sign In using
Google Apps
All forums
General
Demographics
Incident Classification
Discovery and Mitigation
Impact Classification
Most popular
Using the VerIS Framework 23
VerIS Framework Beta Docu 14
Sticky posts
Using the VerIS Framework
by cdporter
Quick links
VZB Security Blog
VZB Data Breach Reports

Cybertrust Security

VerIS Projects



Cybertrust Security

- **Use the framework internally.**

Anyone is free to use the VerIS framework to aid the tracking and reporting of incidents within their organization. We hope those that do will share some of the interesting and innovative ways they are using the metrics in their security program.

- **Use the framework cooperatively.**

Organizations within an existing information exchange, consortium, or other types of partnerships can leverage the VerIS framework for improved data sharing.

- **Share data with others.**

As the ultimate goal of the VerIS Framework is to foster information sharing, we hope users will consider how they might responsibly share data with others. We're working on ways to help facilitate this, and our IR team will continue to do so via the DBIR. We also invite others with access to a large number of incidents from many organizations to use the framework and report their findings. We'd love to see a large number of accessible and comparable datasets in the not-so-distant future.

- **Promote the framework externally.**

Every cause needs a champion, and this one could use many. If you find the VerIS Framework useful or believe it to be beneficial to the community, we'd appreciate you letting others know.

verizon
Cybertrust Security

Advisory Board

Richard Bejtlich

Andrew Bonillo

Chris Carlson

Dan Geer

Jeremiah Grossman

Jake Kouns

Rich Mogull

Cybertrust Security

Questions Slide

- Your Turn!