RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-02

Advancing Information Risk Practices

MODERATOR: **Evan Wheeler**

Executive Director, Operational Risk Management
DTCC

PANELISTS:

Marshall Kuypers
PhD Candidate
Stanford University

Jay Jacobs
Sr. Data Scientist
BitSight Technologies

Jack Jones
EVP Research & Development
RiskLens

Wade Baker
VP, Innovation & Analytics
ThreatConnect

#RSAC

Advancing Information Risk Practices

Start Time	Title	Presenter
1:30 PM	Practical Quantitative Risk Analysis in Cyber Systems	Marshall Kuypers
2:25 PM	Exploring Your Data: Risk Visualization Techniques	Jay Jacobs
3:15 PM	BREAK	
3:30 PM	Third Party Risk Assessment: Death by 800 Questions	Jack Jones
4:15 PM	The Marriage of Threat Intelligence and Risk Assessment	Wade Baker

RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

Practical Quantitative Risk Analysis in Cyber Systems

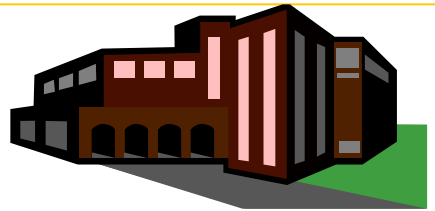
Marshall Kuypers[A] (Presenting)

Dr. Elisabeth Pate-Cornell[B]

[A]PhD Student
Stanford University

[B]Professor, Management Science and Engineering
Stanford University

Significant uncertainty surrounds cyber security investment



Open DLP

Data loss prevention

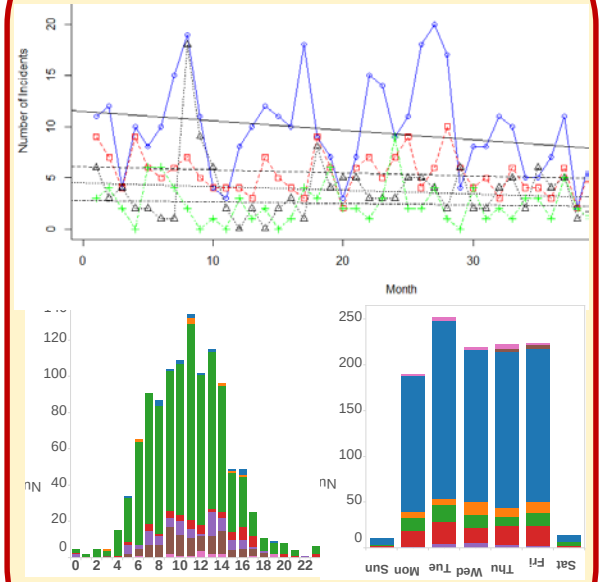
Two-factor authentication

CROWDSTRIKE

Subscription for threat intel

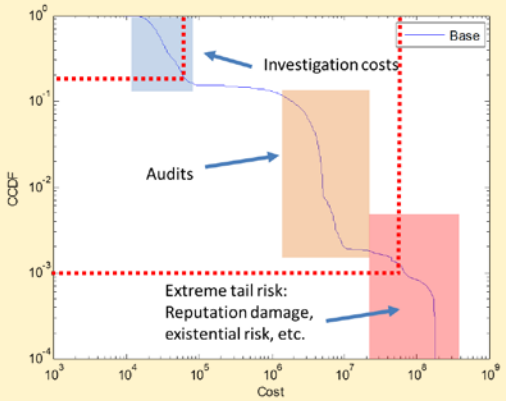
Cyber risk is quantifiable!

The data exist!



And you need them!

The models exist!



And you need them!

Quantitative risk is super useful!

And you need it!

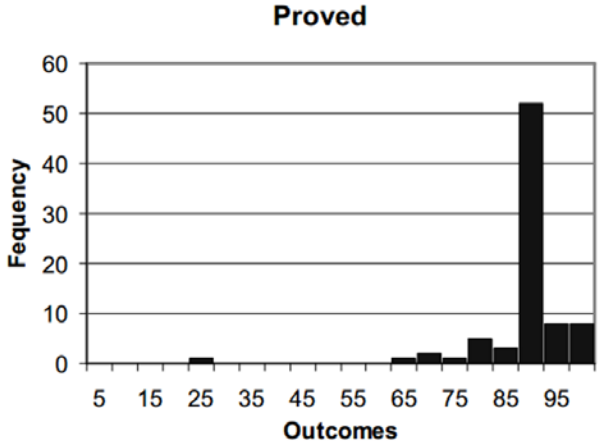
Current methods are limiting

PSAT

Hand Waving

Likelihood	Impact: Minor	Impact: Moderate	Impact: Major
Very likely	Medium 2	High 3	Extreme 5
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2

What is the chance it will happen?



McLane, Gouveia, et al

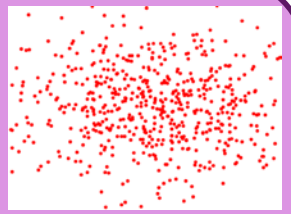
Our intuition is really terrible

Ask Doctors if they recommend surgery if:

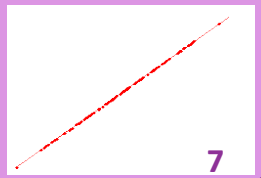
One month survival rate is 90% — 84%

There is a 10% mortality in the first month — 50%

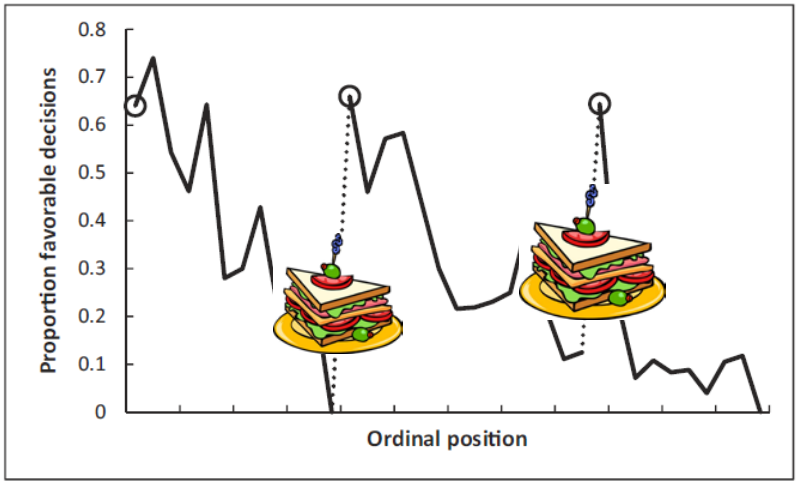
How happy are you these days?
How many dates did you have last month?



How many dates did you have last month?
How happy are you these days?



Parole decisions in Israeli Prisons



Extraneous factors in judicial decisions
Shai Danzigera, Jonathan Levavb, and Liora Avnaim-Pessoa

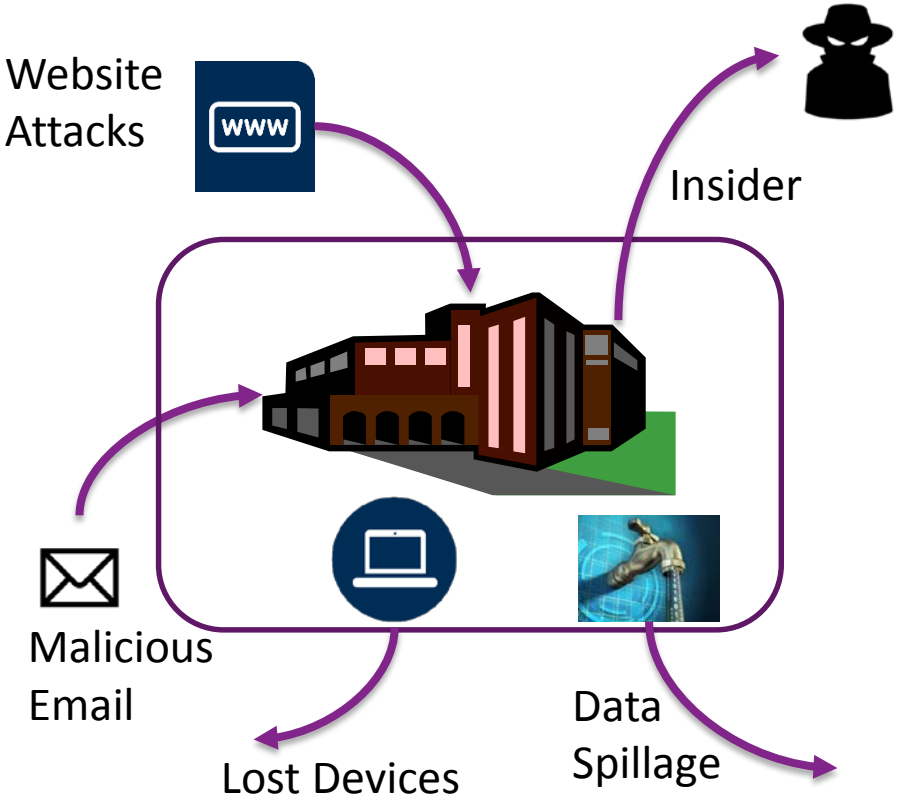
Data help us make better decisions

1

Malicious Insider

375

Website Compromises



The data exist!

Incident Management Systems

Date
Time to resolve (hours)
Type of incident

Not log data!

High level incident categories

Incident type tag
- #Lost device
- #Website defacement
- #Phishing email
- #Intern's website

Sergey Brin's Home Page

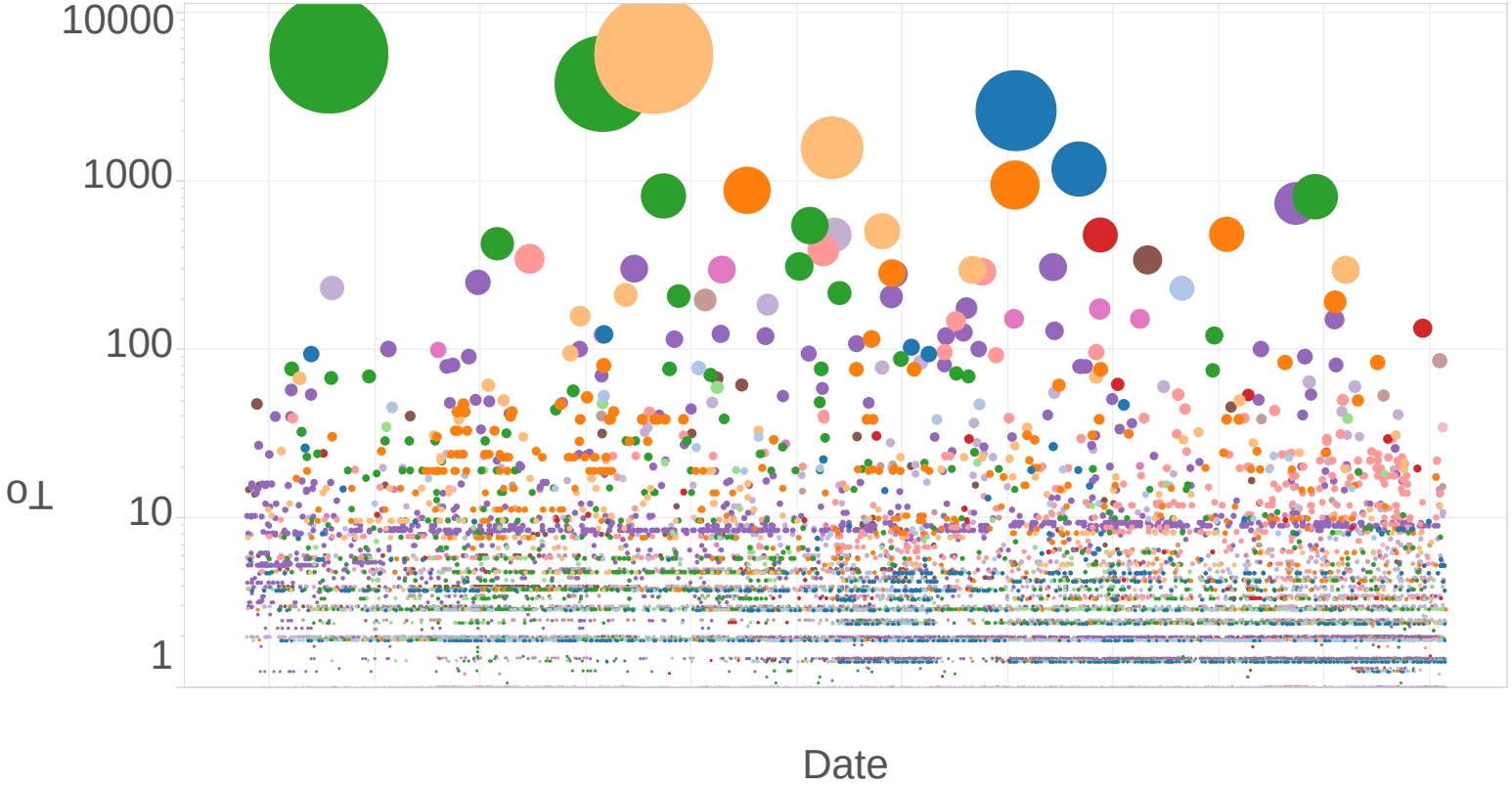
Ph.D. student in Computer Science at Stanford - sergey@cs.stanford.edu

Currently I am at Google.

Lots of data exist

Academic research
Lawsuits
Expert knowledge

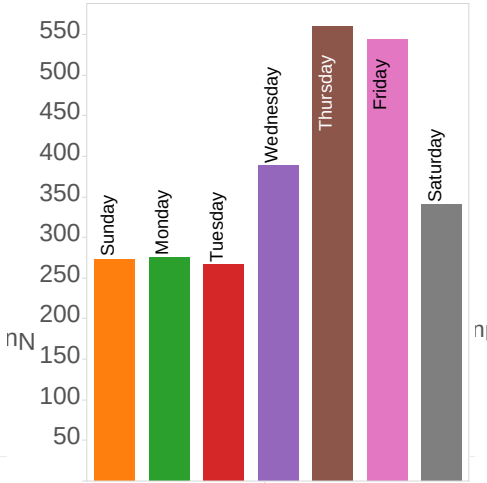
Case study: 60K incidents at a large org

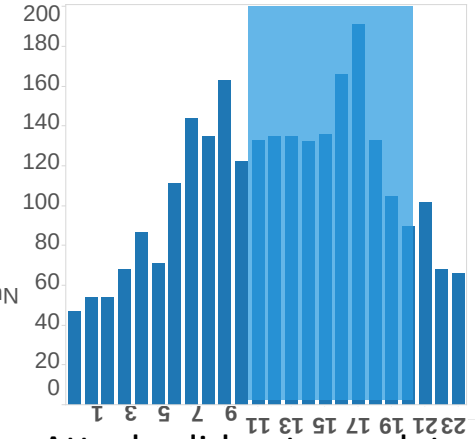


Incident data is priceless

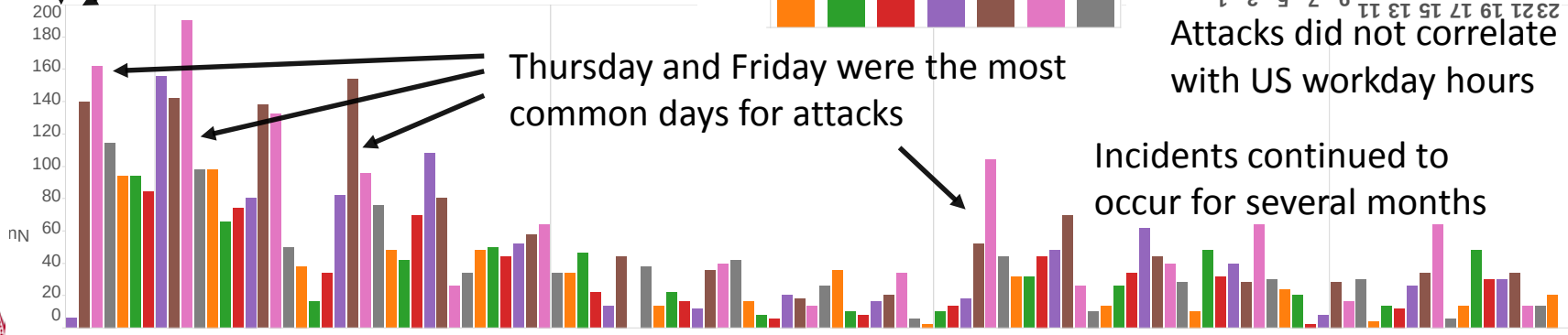
Shellshock publically announced on September 24th, 2014

Within 5 hours, a shellshock attack was detected





Attacks did not correlate with US workday hours

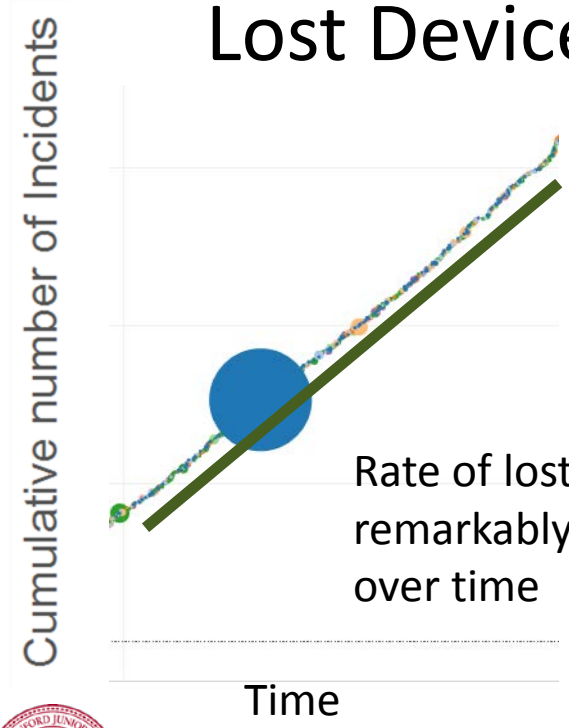


Thursday and Friday were the most common days for attacks

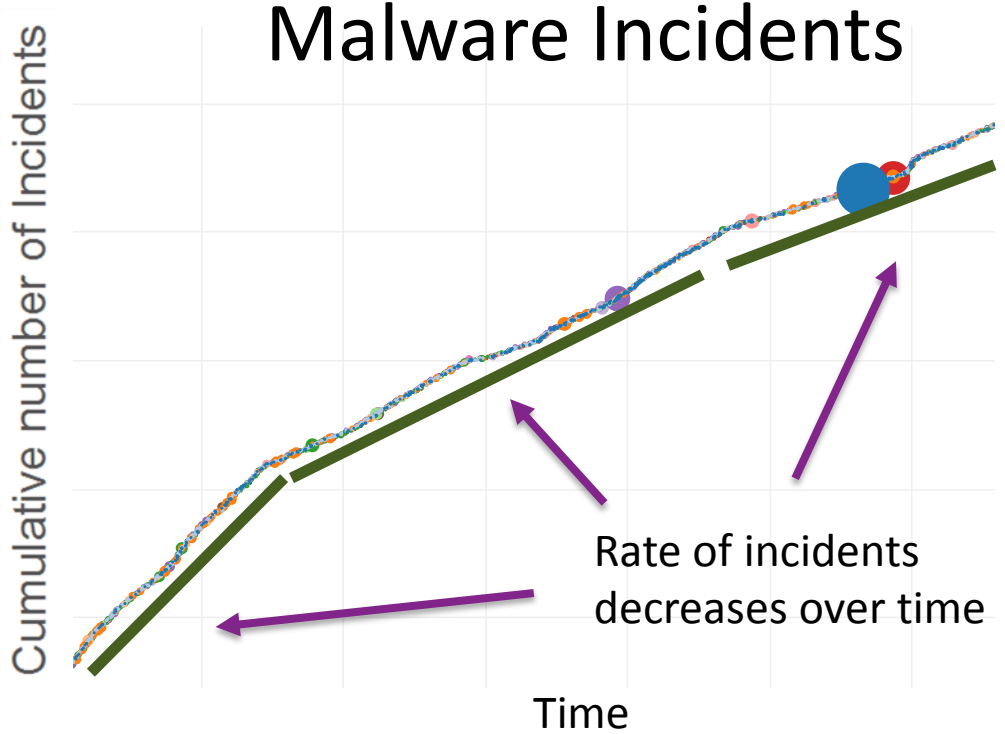
Incidents continued to occur for several months

The frequency of incidents can be quantified

Lost Devices



Malware Incidents



Develop a useful model

Website Attacks | Malicious Email | Data Spillage | Lost Devices | Malware (browse/ USB) | Other

Internet

Organization

Cost Model

Direct Cost	Disclosure Costs (PII)	Intellectual Property
Investigation/ Remediation	Business interruption/ downtime	Reputation Damage

Use dollars

Use distributions, not averages

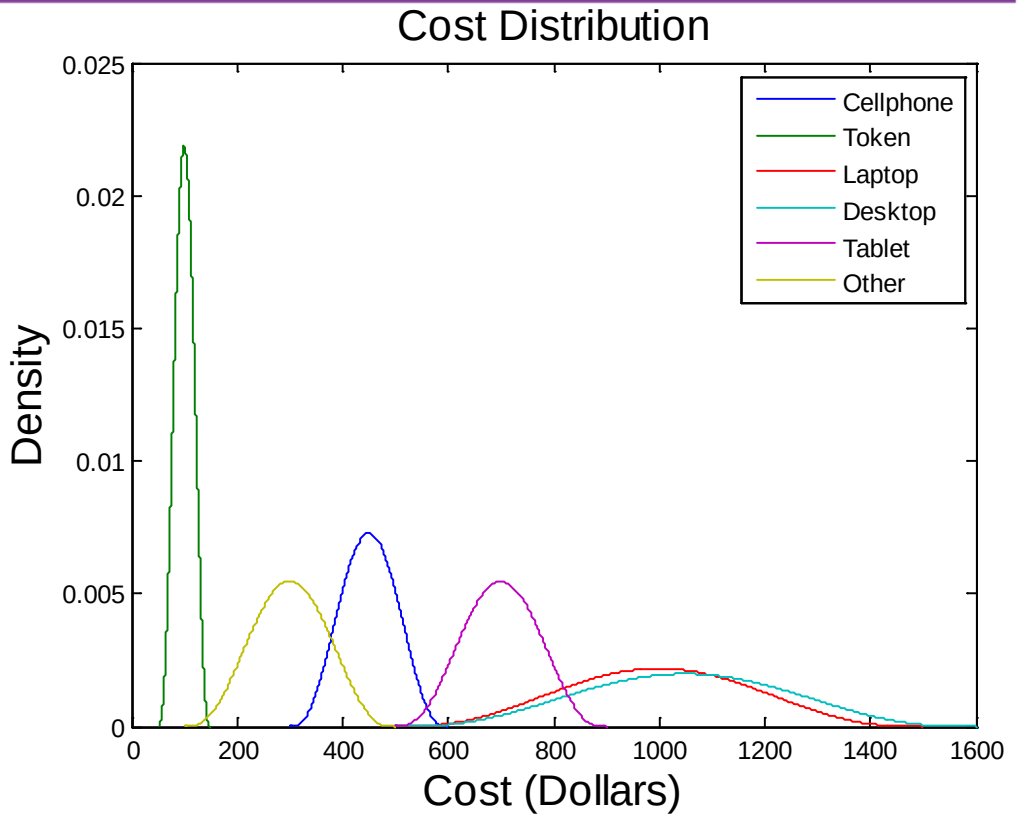
Direct costs are well understood

Probability	Device	Average Cost
0.34	Cellphone	$400
0.32	Token	$100
0.20	Laptop	$1000
0.07	Other	$300
0.05	Desktop	$1000
0.02	Tablet	$700

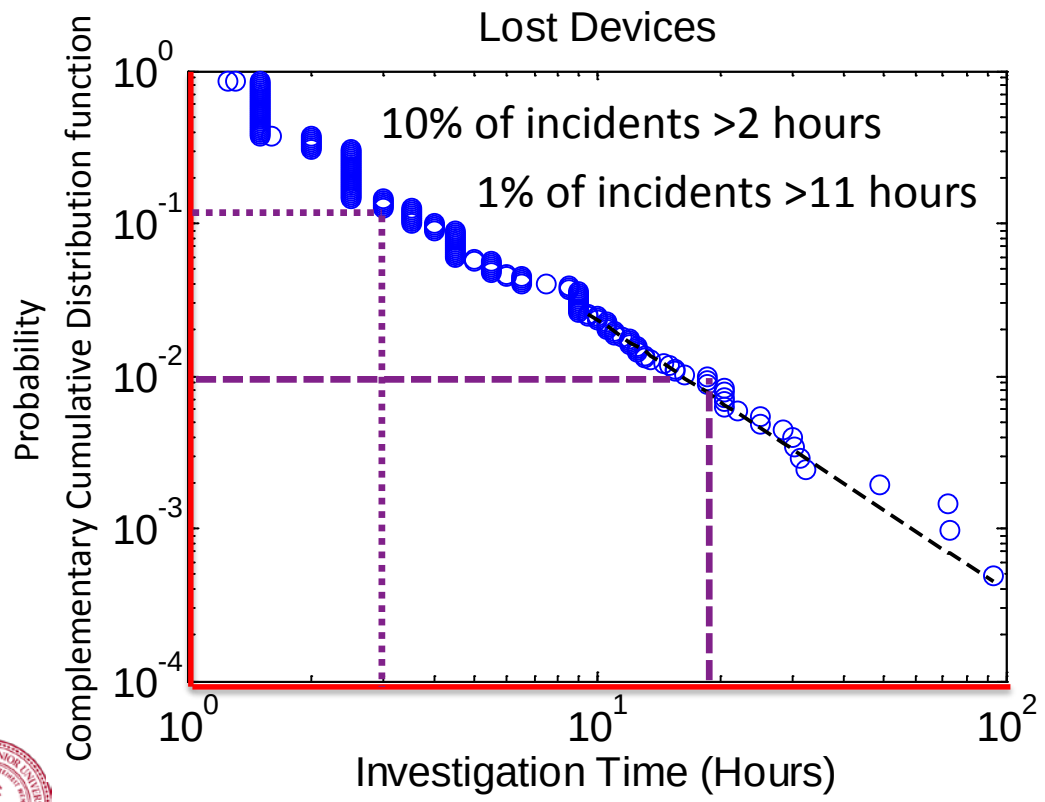
Equipment Losses

DDoS
Distributed Denial of Service Protection

Extortion



Investigation costs are well understood



Large Events are NOT outliers

No ‘average’ or ‘typical’ cyber breach

Standard deviations and some risk metrics (value at risk) are not valid

Largest incident can be more impactful than all other incidents combined!

Reputation damage can be assessed

We can quantify data spillage risk

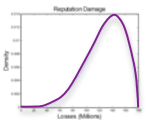
Rate of spillage incidents

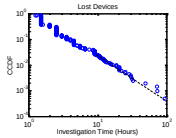
λ

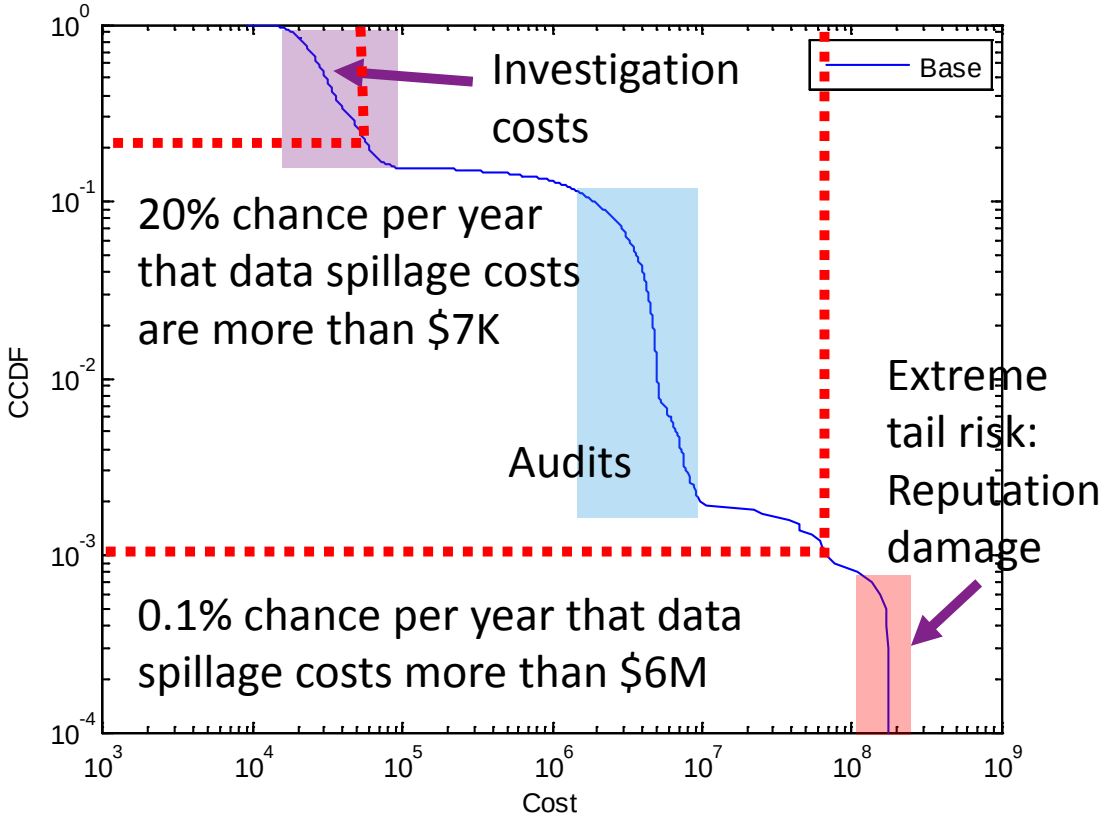
Yearly Rate: 50

Impact Distributions (Data Spillage)

- Investigation
- PII Fines
- Reputation
- IP Loss

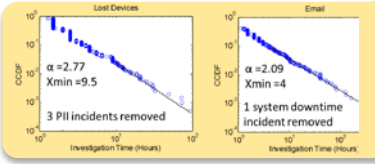




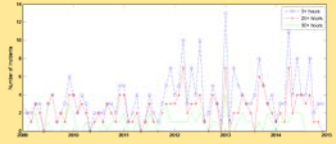


Security investments are analyzed and prioritized

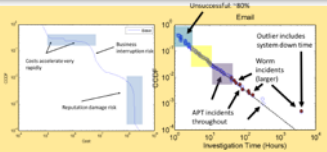
Case study on a large organization



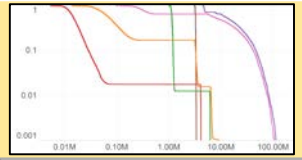
Full disk encryption is a **good investment** with a **4 to 1 benefit-cost** ratio**.**



Data loss prevention is found to be a **poor investment,** given the **technology maturity.**



Supply chain risk and the threat of **malicious insiders** is found to be **low.**



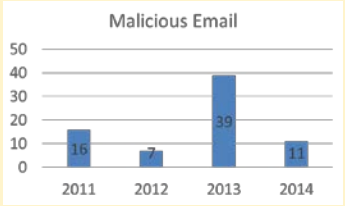
Poor website and **network security** is a **major risk,** and requires **significant security investment.**

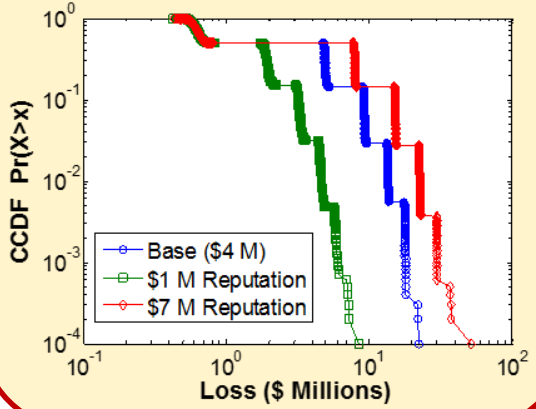
You can get started by…

Collect data

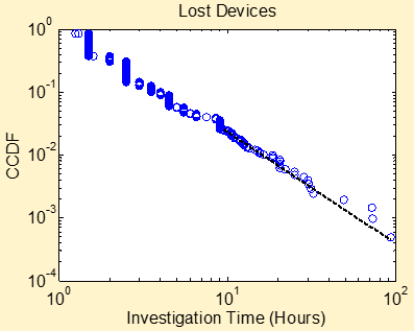
Date
Time to resolve (hours)
Incident type tag
- #Malware
- #Email
- #Intern's website

Analyze data





Embrace uncertainty



Large events are NOT outliers

Largest incident can be more impactful than all other incidents combined!

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

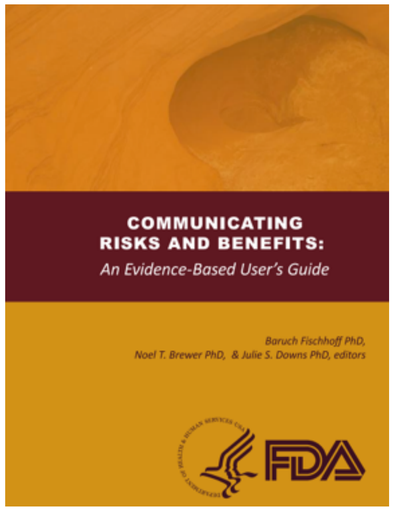
Exploring Your Data: Risk Visualization Techniques

Jay Jacobs

Sr. Data Scientist
BitSight Technologies
@jayjacobs

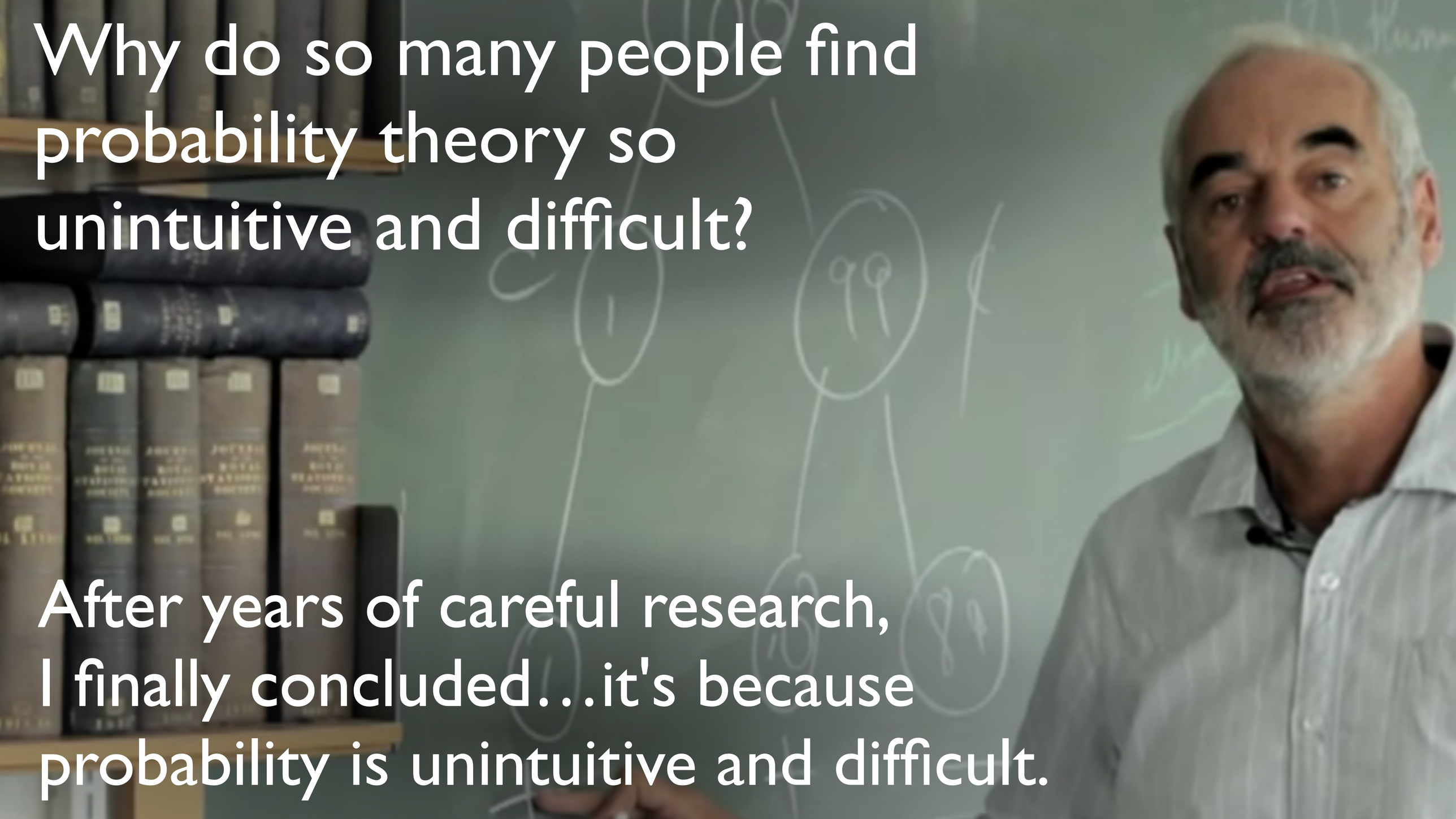
Concepts you will walk away with

- Probability
- What makes a good data visualization?
- Evolution of data maturity
- Advanced techniques

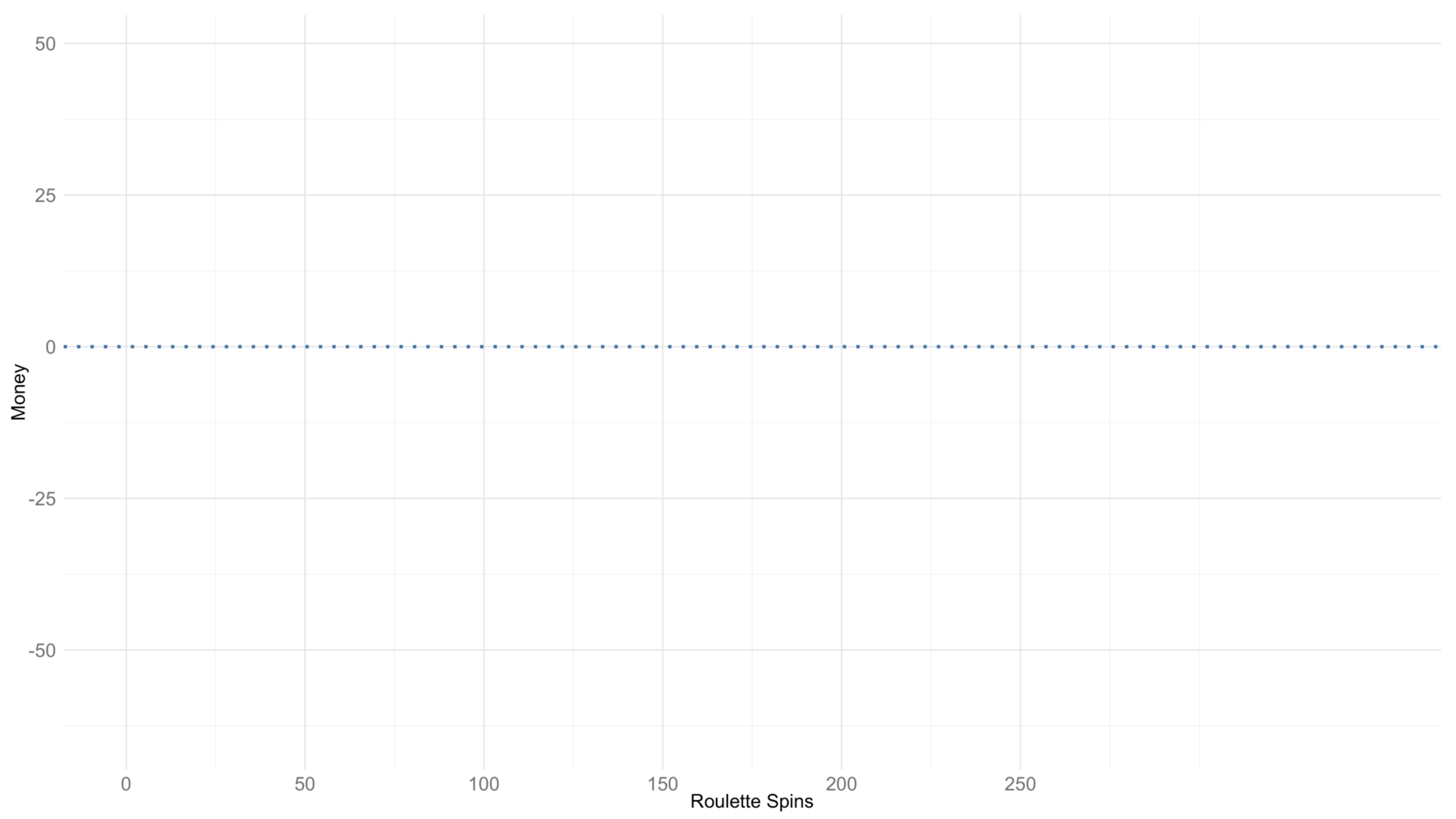


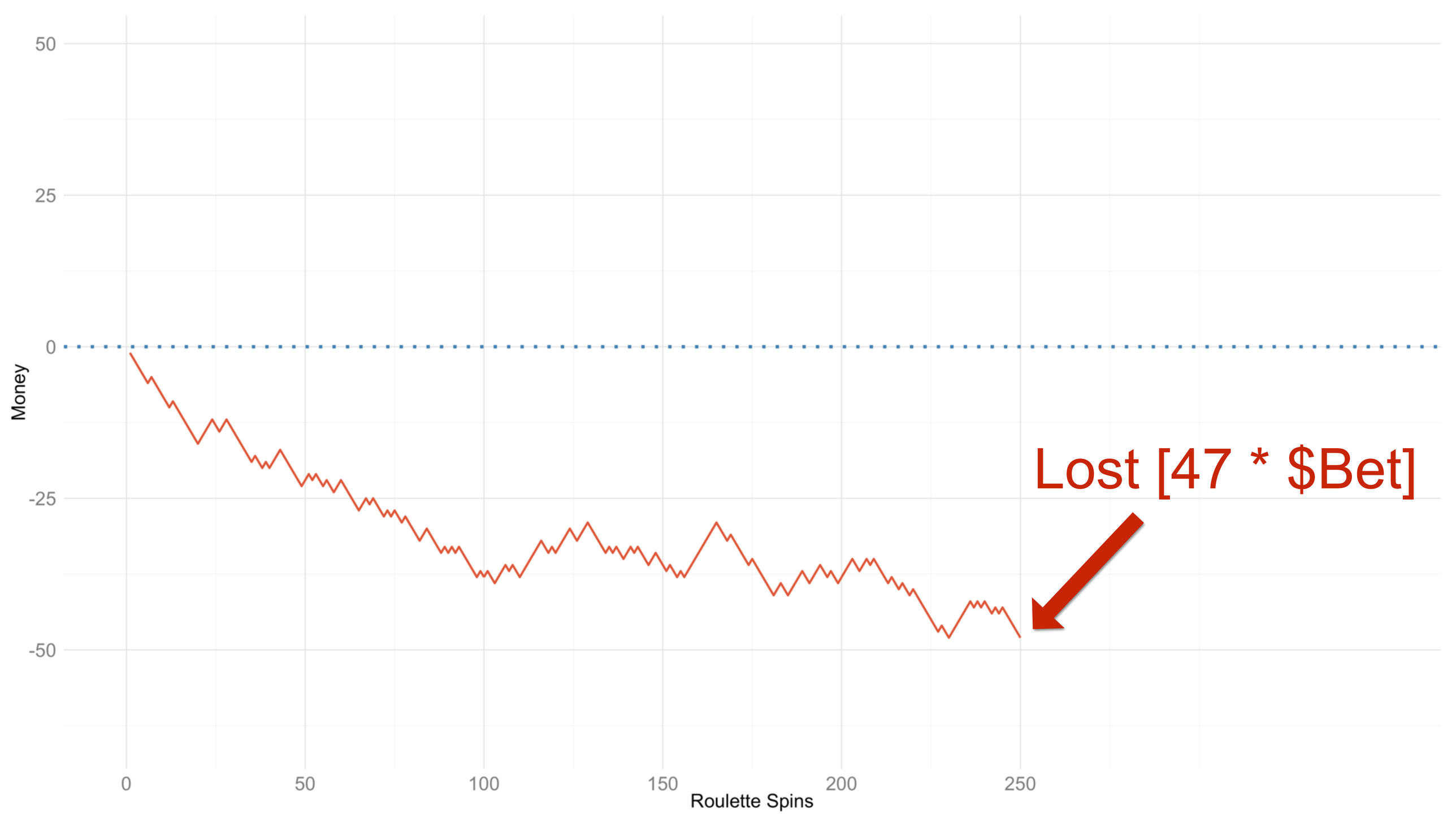
"***Risk communication*** is the term of art used for situations when people need good information to make sound choices."

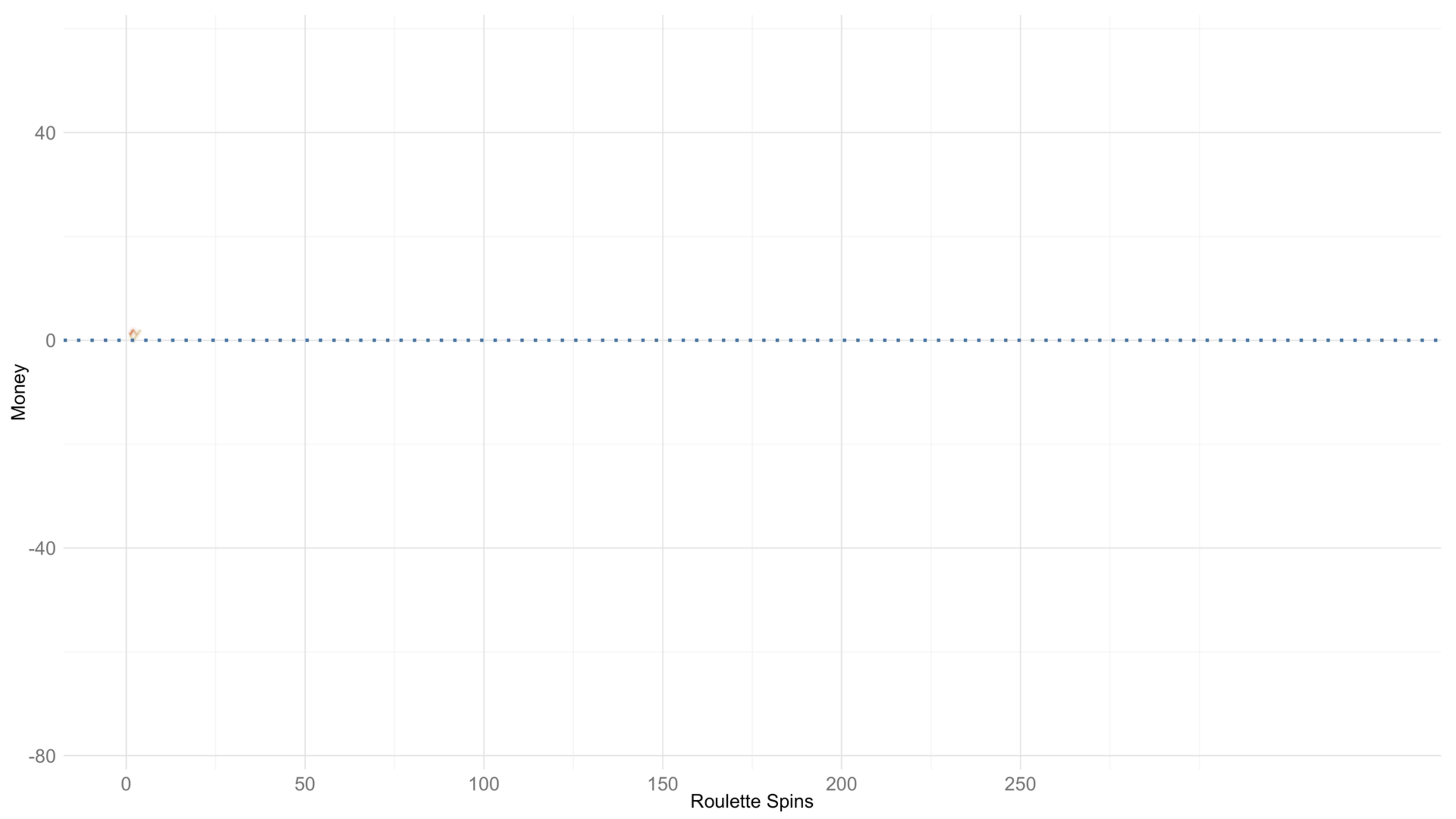
Fischhoff, B. (2012). Communicating Risks and Benefits: An Evidence Based User's Guide. Government Printing Office.


Why do so many people find probability theory so unintuitive and difficult?
After years of careful research, I finally concluded…it's because probability is unintuitive and difficult.

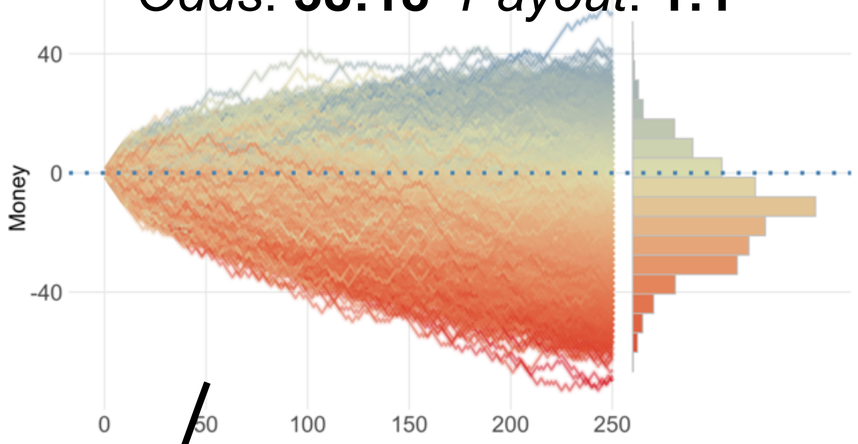
A Challenge in Risk Visualization


50
25
0
-25
-50
Money
0
50
100
150
200
250
Roulette Spins

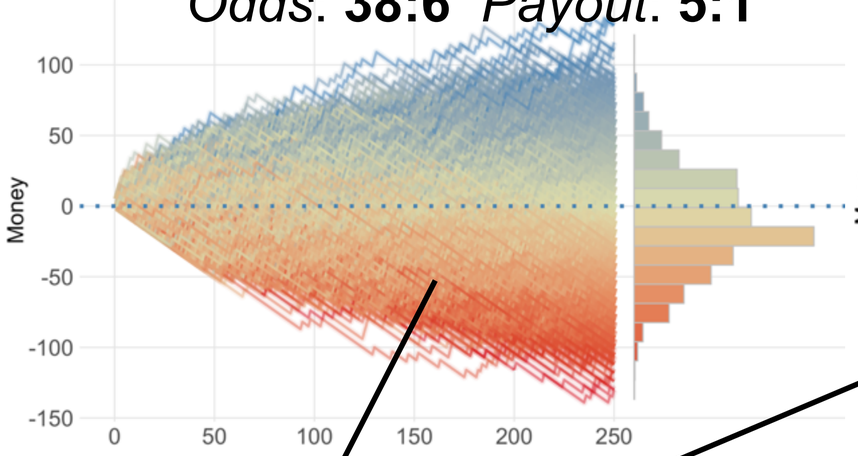

50
25
0
-25
-50
Money
0
50
100
150
200
250
Roulette Spins
Lost [47 * $Bet]


40
0
-40
-80
Money
0
50
100
150
200
250
Roulette Spins

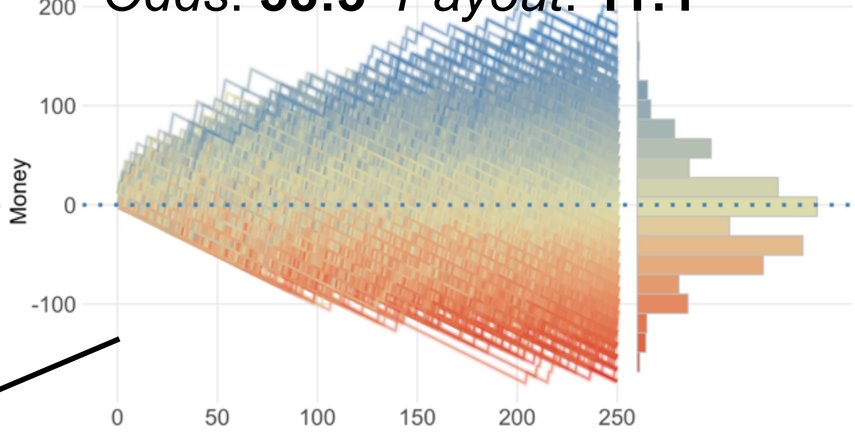
Odds: **38:18** *Payout*: **1:1**



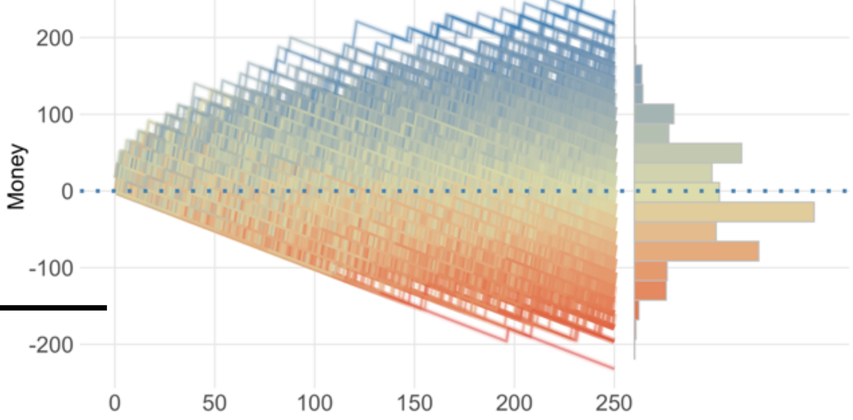
Odds: **38:6** *Payout*: **5:1**

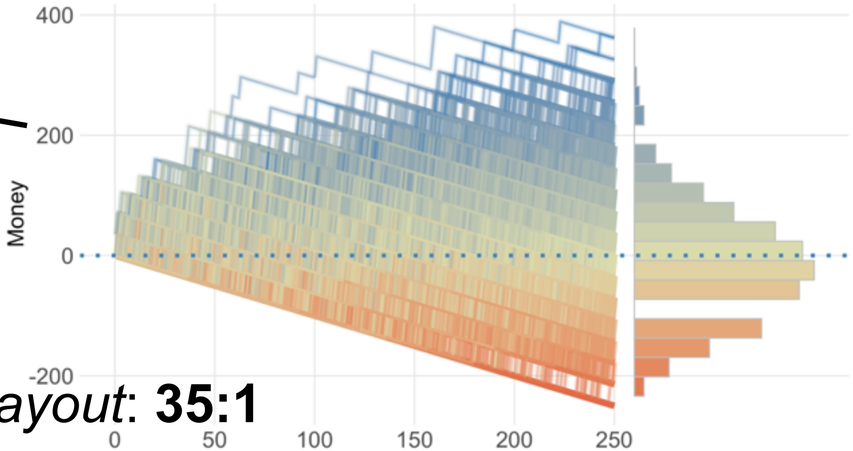


Odds: **38:3** *Payout*: **11:1**



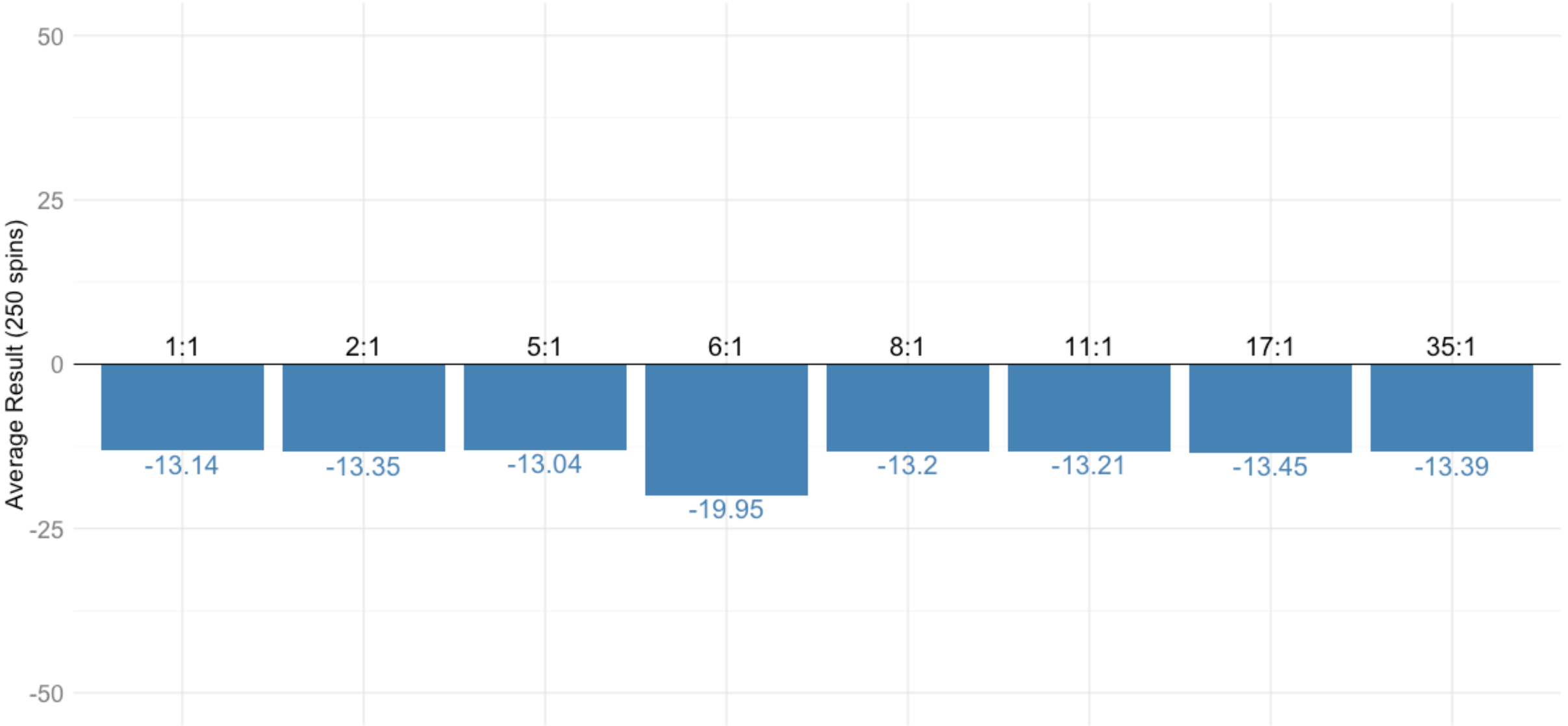
Odds: **38:2** *Payout*: **17:1**



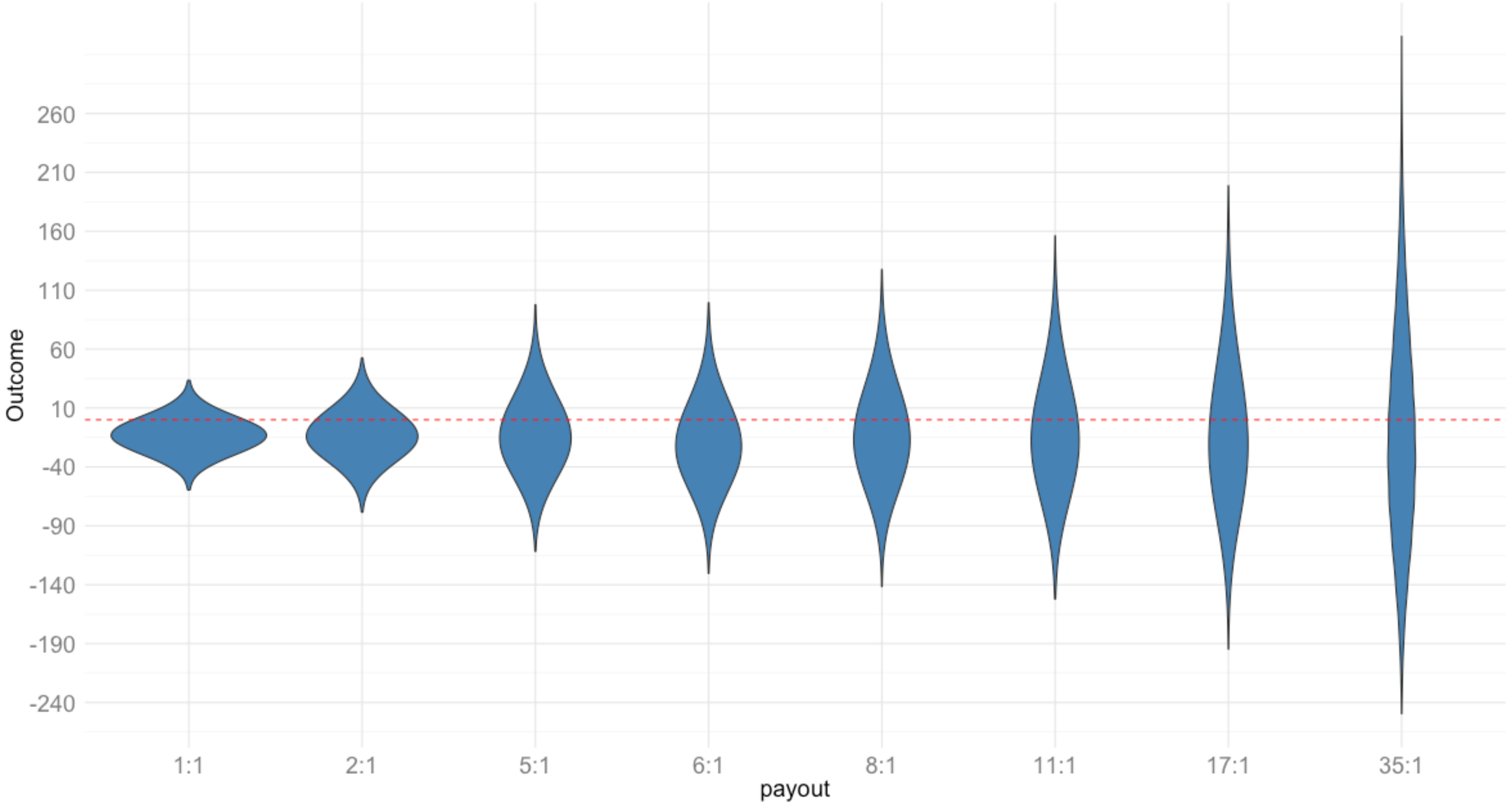


Odds: **38:1** *Payout*: **35:1**

“Average” loss after 250 rounds of Roulette



Distributions of loss after 250 rounds



Walking out of a Casino…

You would…

- leave with less money 3 out of 4 visits
- lose more than 13 * $bet around half the visits
- lose more than 34 * $bet once every ten visits*
- win more than 8 * $bet once every ten visits*

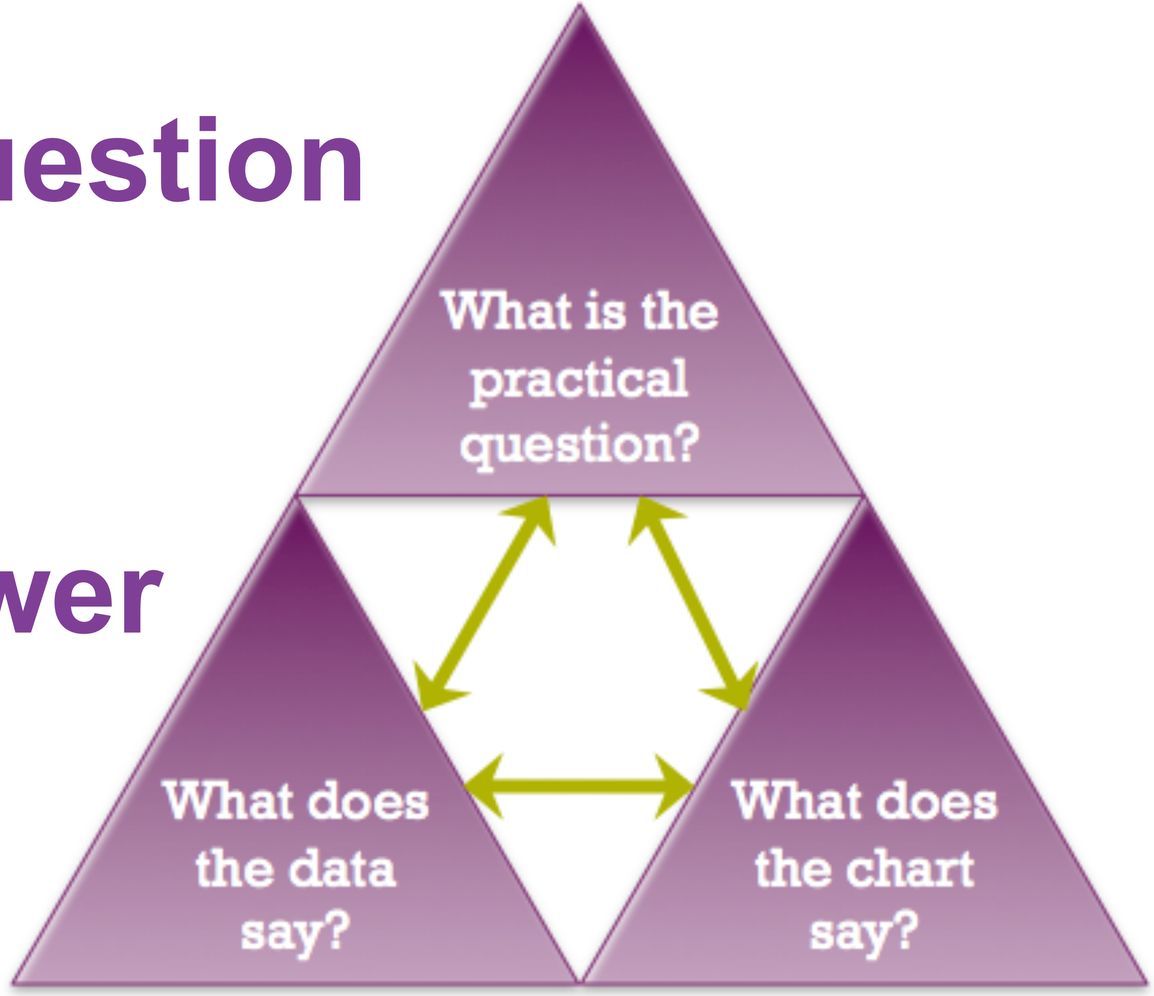
* 1:1 payout

What makes a good data visualization?

Junk Charts Trifecta Checkup

Question

Answer



Message

http://junkcharts.typepad.com/

Asking a Question

Asking a Question

"My job was to find questions about baseball that have objective answers, that's all that I do, that's all that I've done."

-- Bill James, Sabremetrician

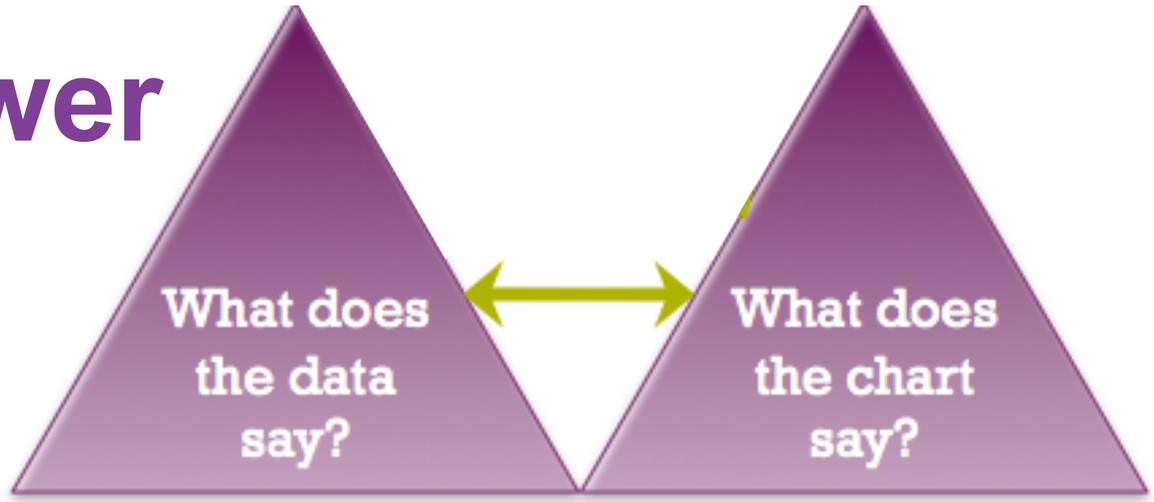
Asking a Question

A good question…

- …has an objective and measurable answer.
- …isn't too expensive to answer.
- …has someone who wants to know the answer.

A Common Pitfall

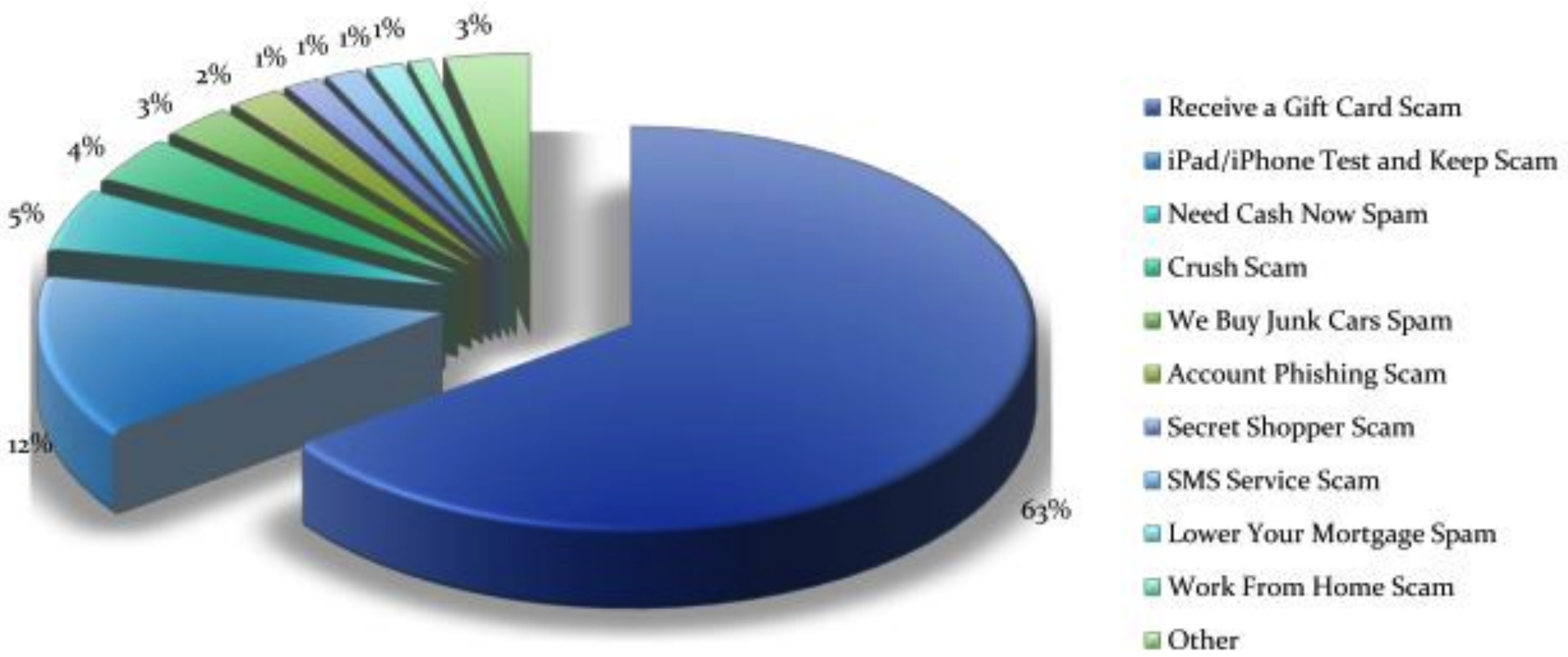
Answer



Message

http://junkcharts.typepad.com/

A Common Pitfall



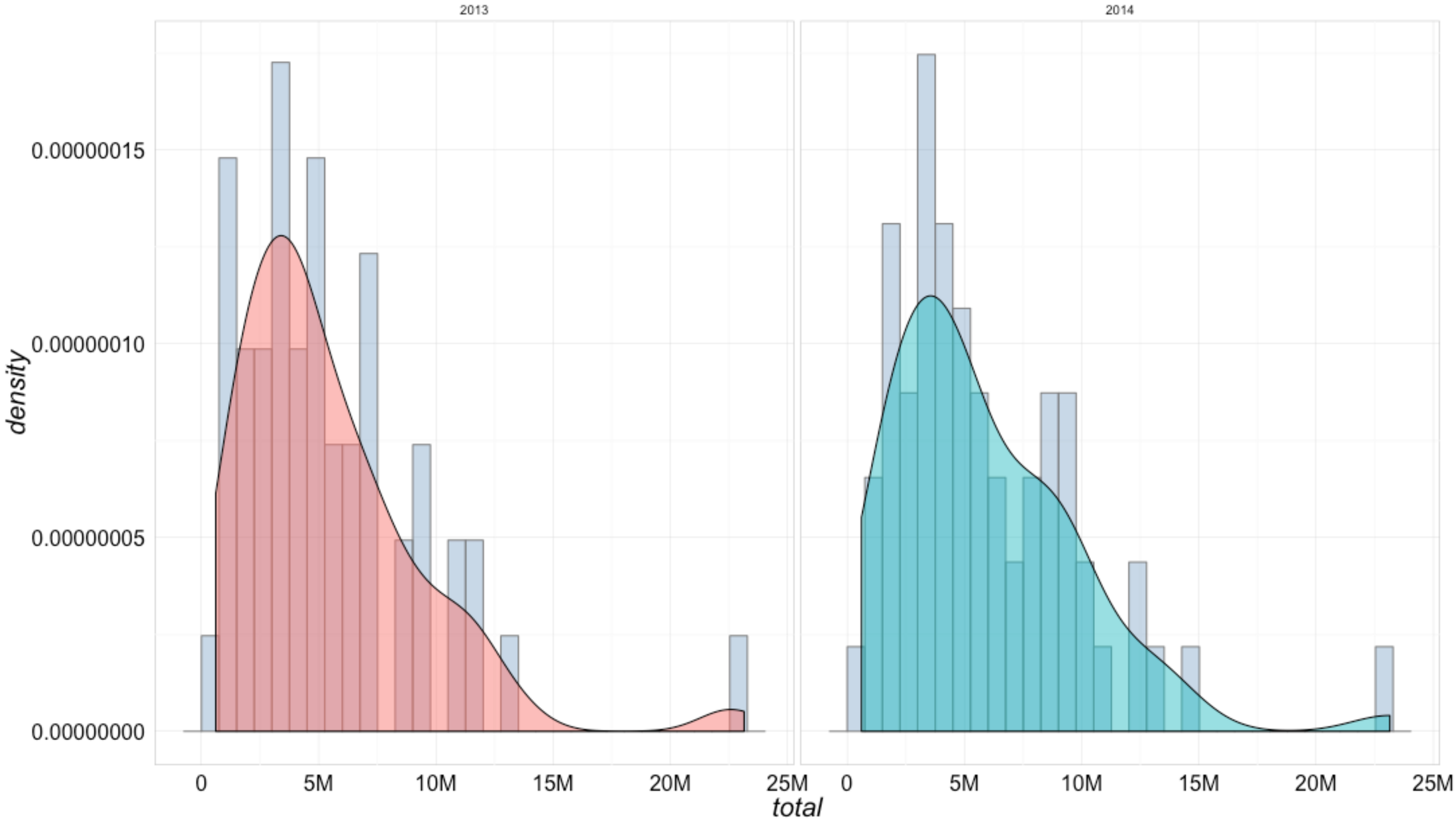
United States: Top Categories of SMS Spam
https://www.cloudmark.com/en/s/resources/whitepapers/sms-spam-overview

Using Data

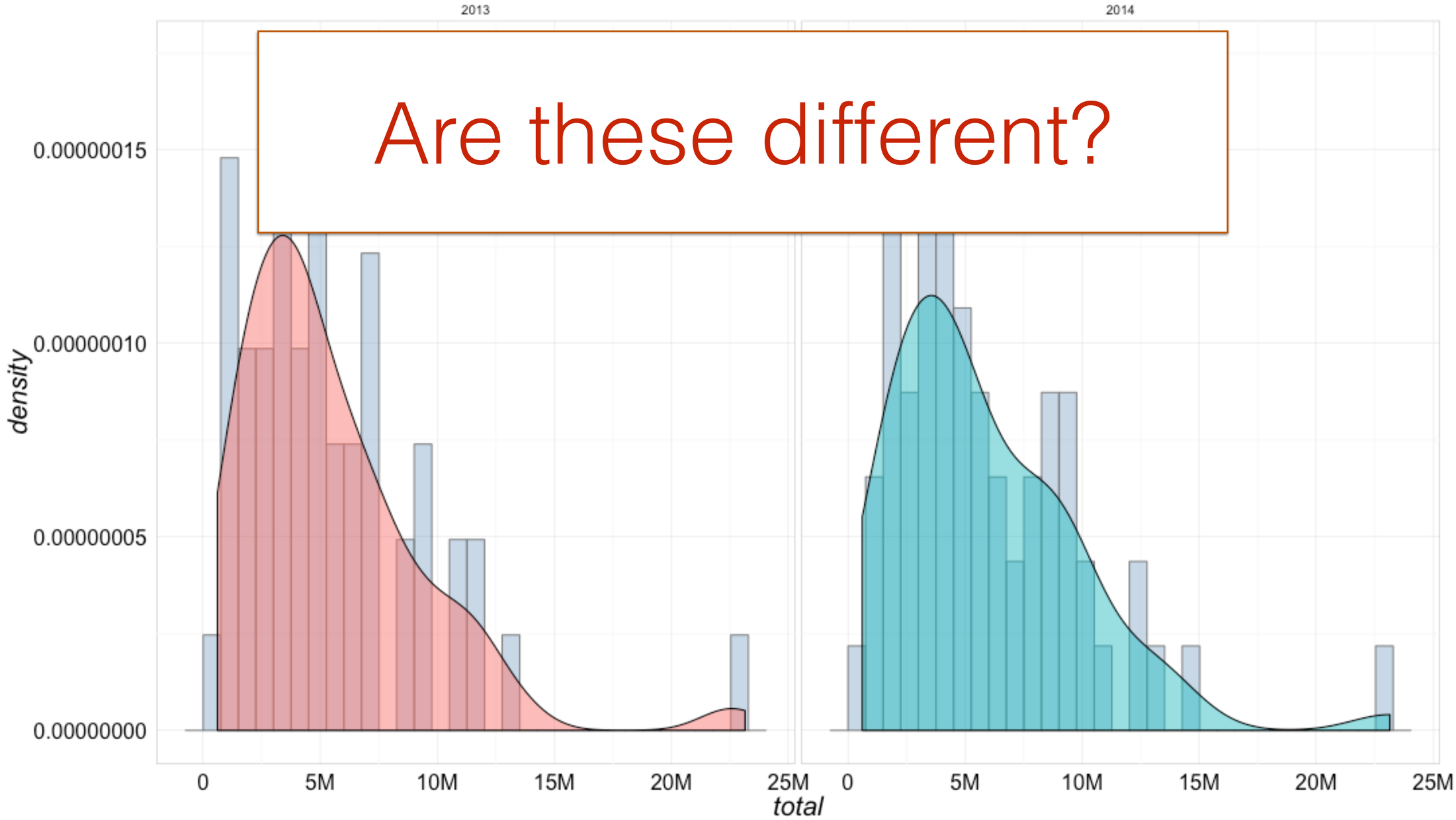
Evolution of Data Maturity

1. Count
2. Compare (careful for language barrier)
3. Infer and estimate
4. Model
    a. forecasting
    b. insight and inference

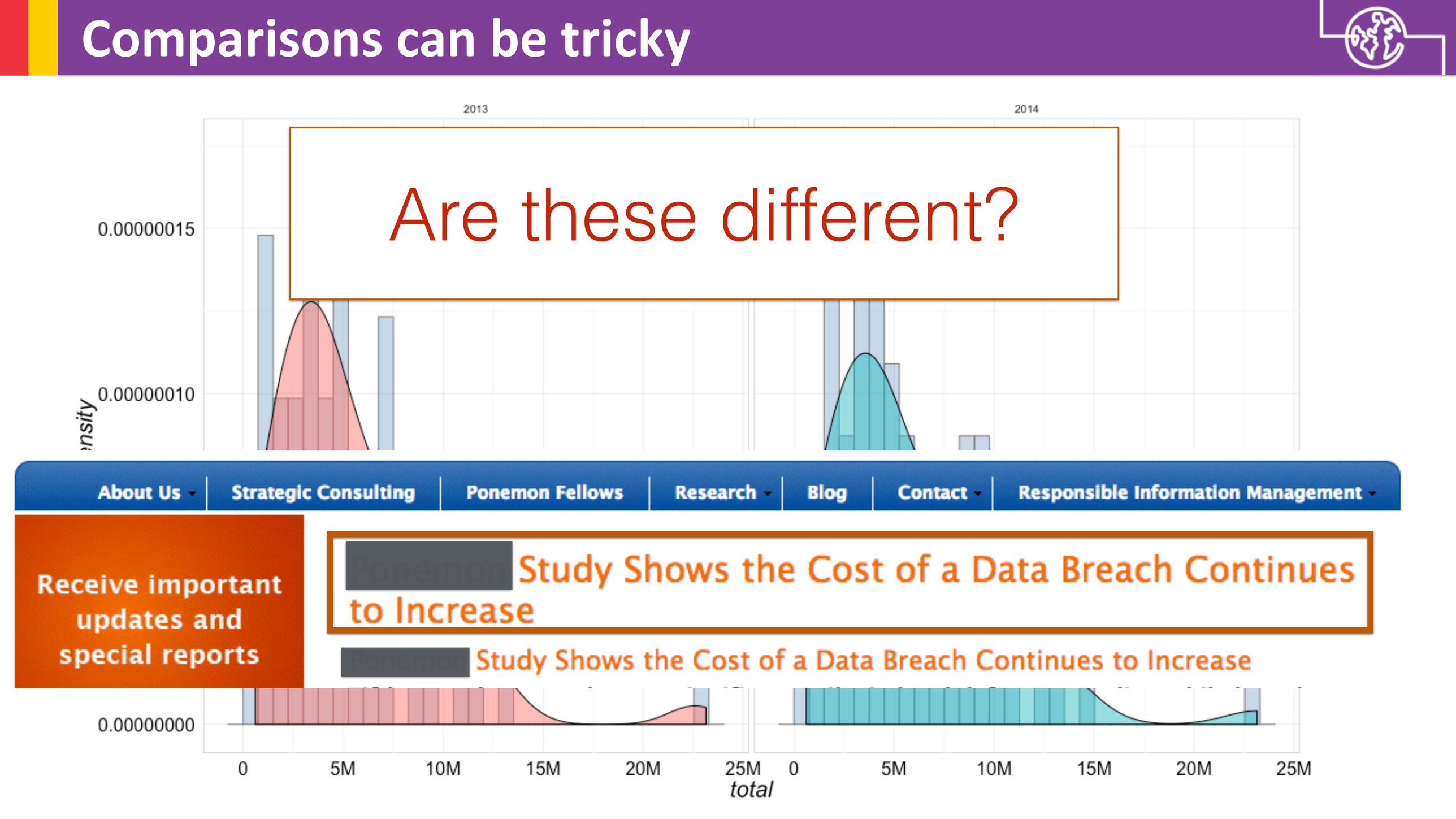
Comparisons can be tricky



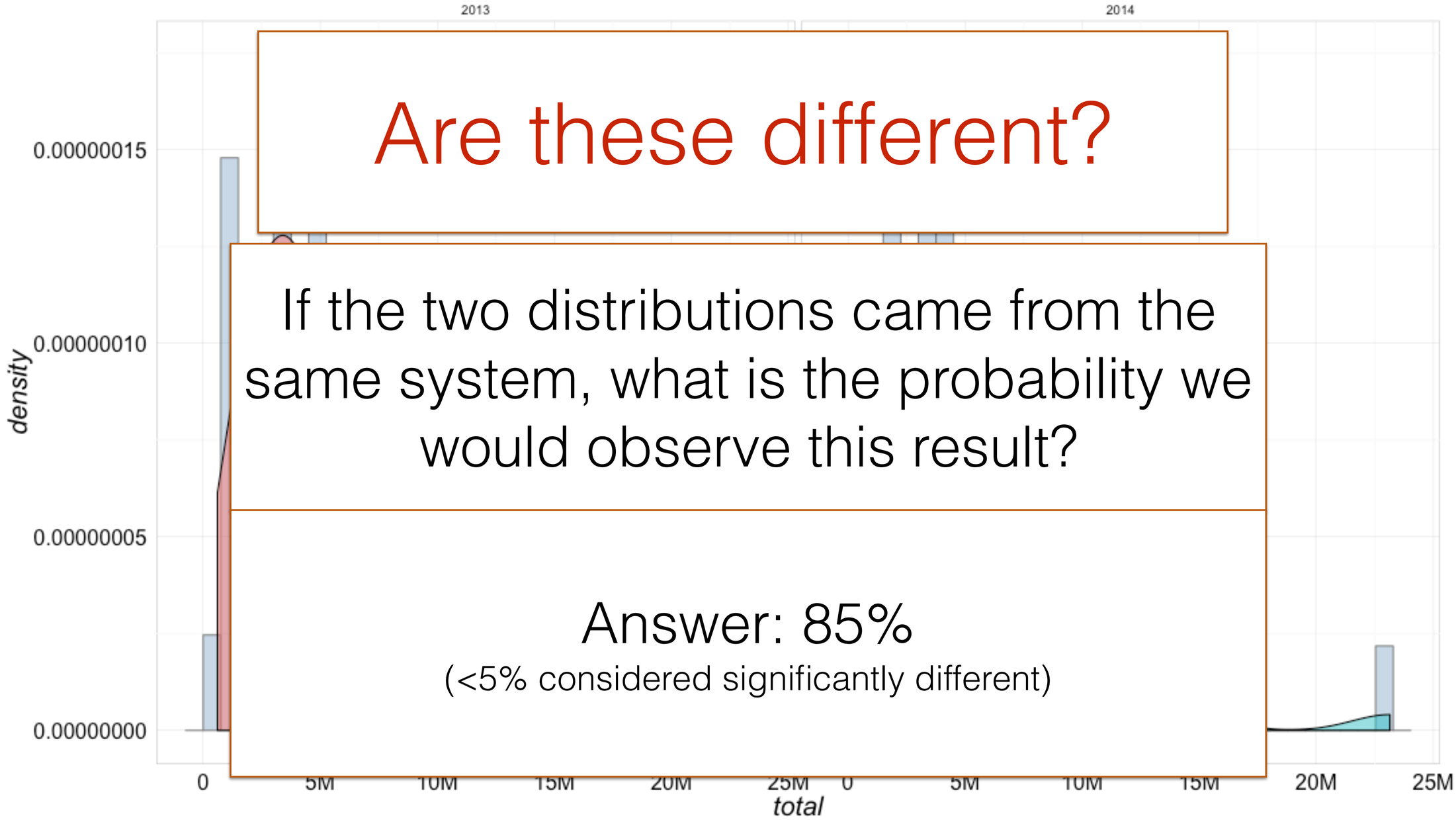
Comparisons can be tricky



Comparisons can be tricky



Comparisons can be tricky



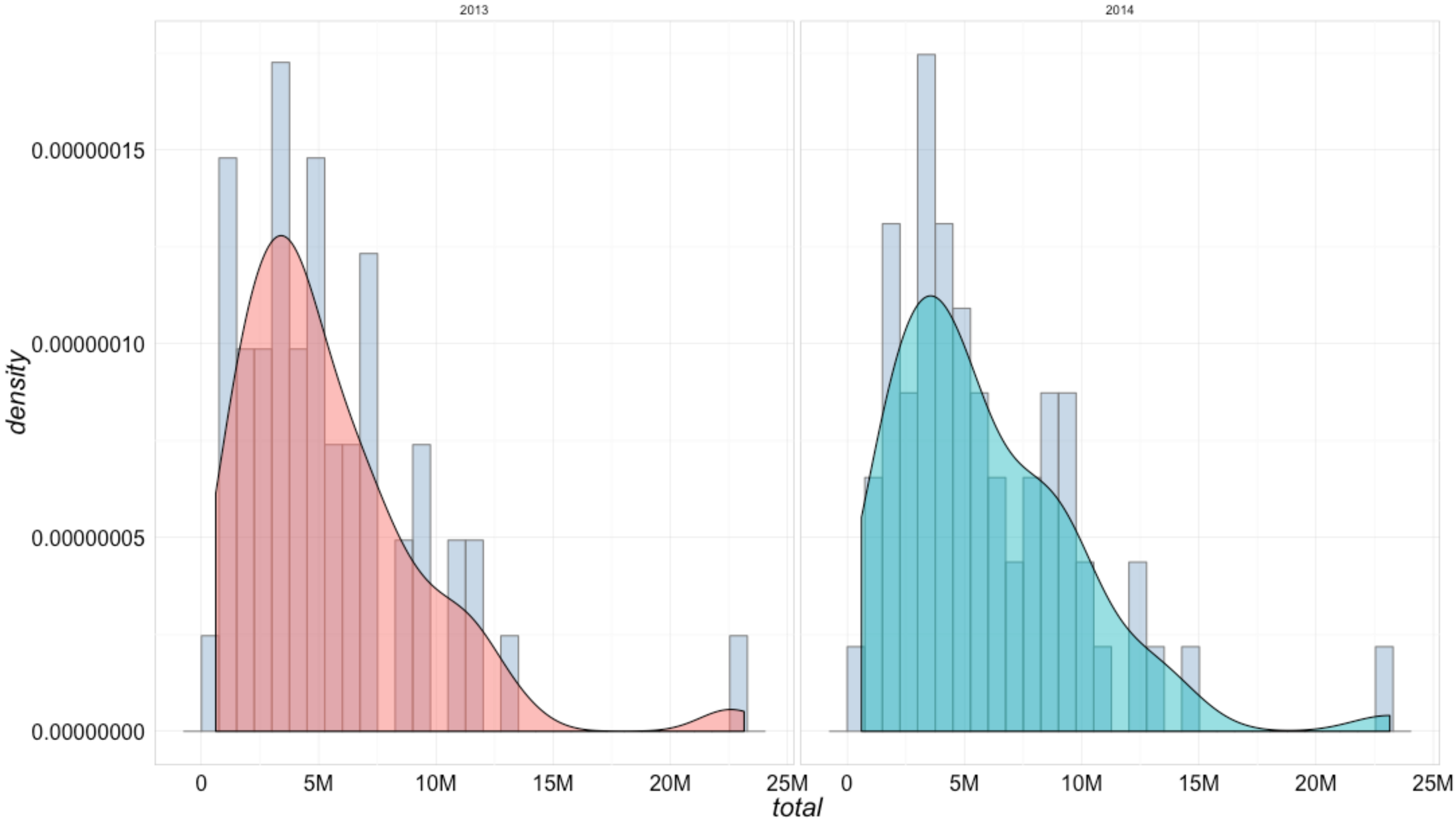
Are these different?

If the two distributions came from the same system, what is the probability we would observe this result?

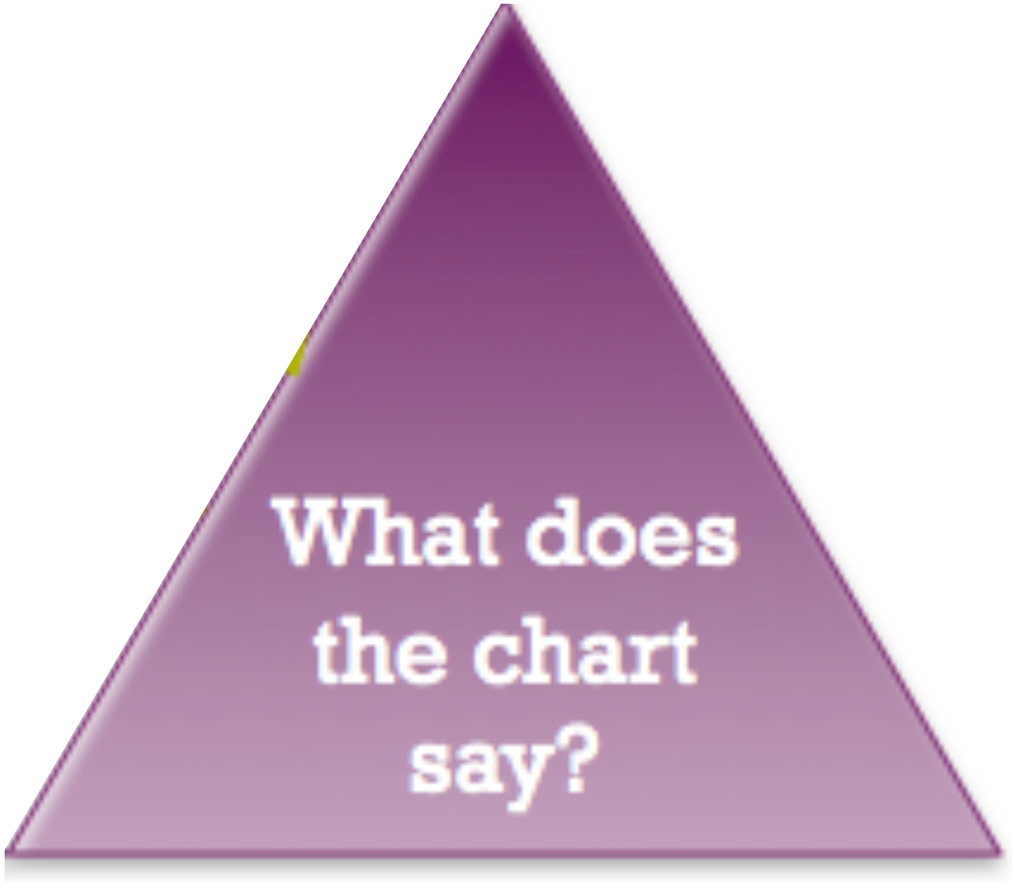
Answer: 85%

(<5% considered significantly different)

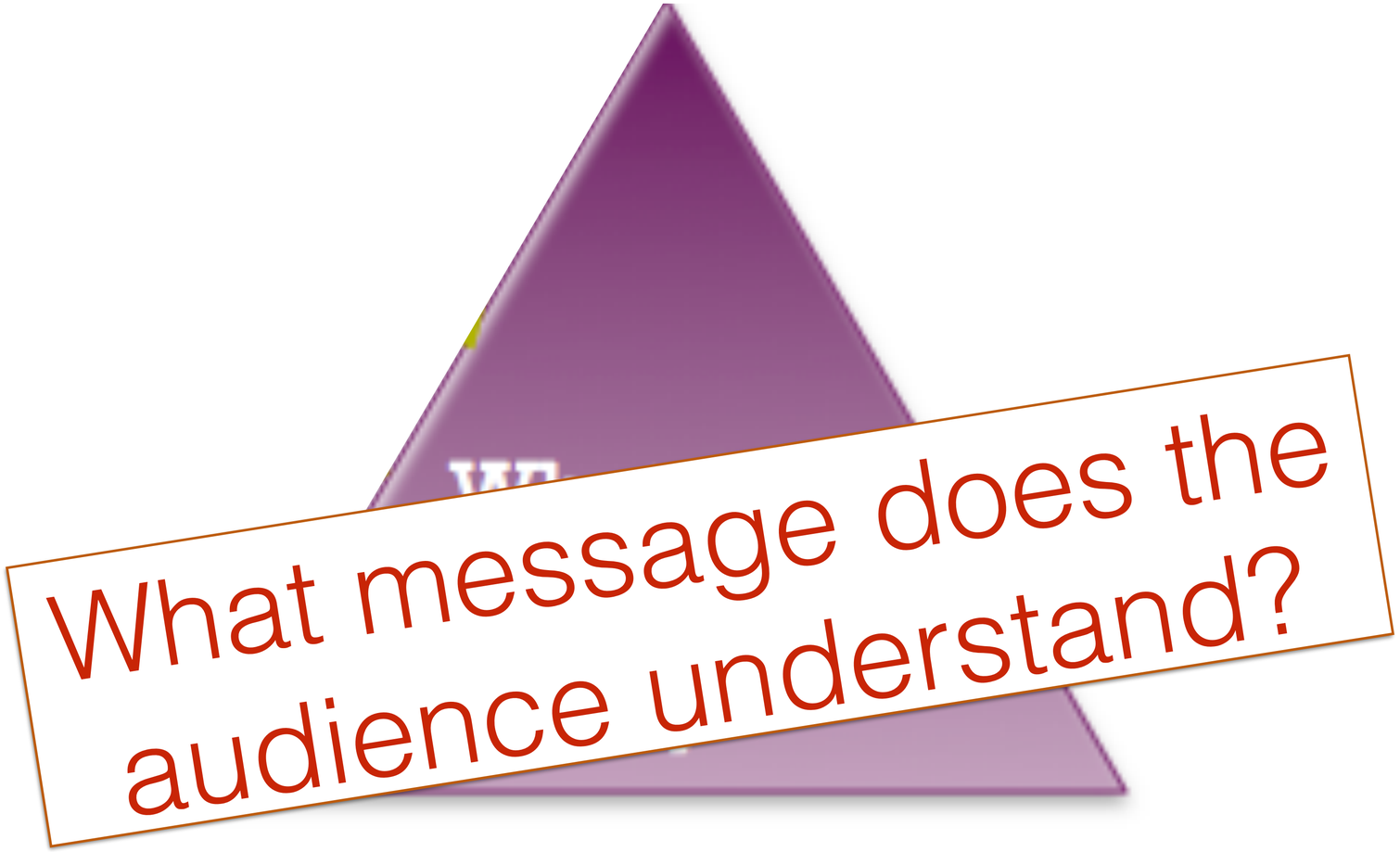
Comparisons can be tricky



Encoding the Message



Encoding the Message



Communication

Sender
Encodes

Channel/Medium

Receiver
Decodes

words

semaphores

data visualization

What are we encoding?

Encoding one or more data variables

- Quantitative or Categorical

with relationships

- Proportional, spatial, temporal

using visual cues

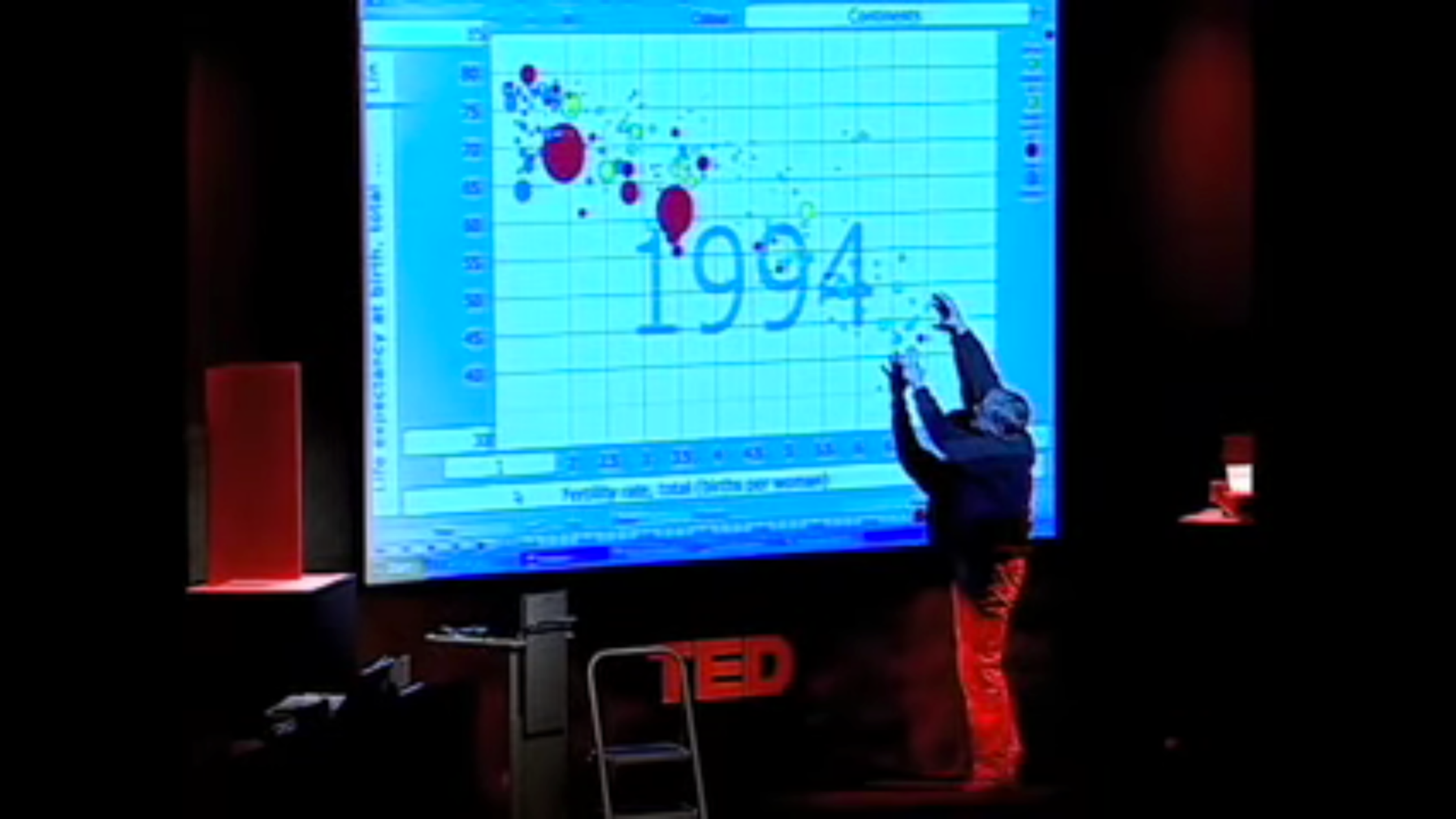
- shape, size, color and position
- length, angle, slope and area

Communication (Quantities)

Easier Decoding

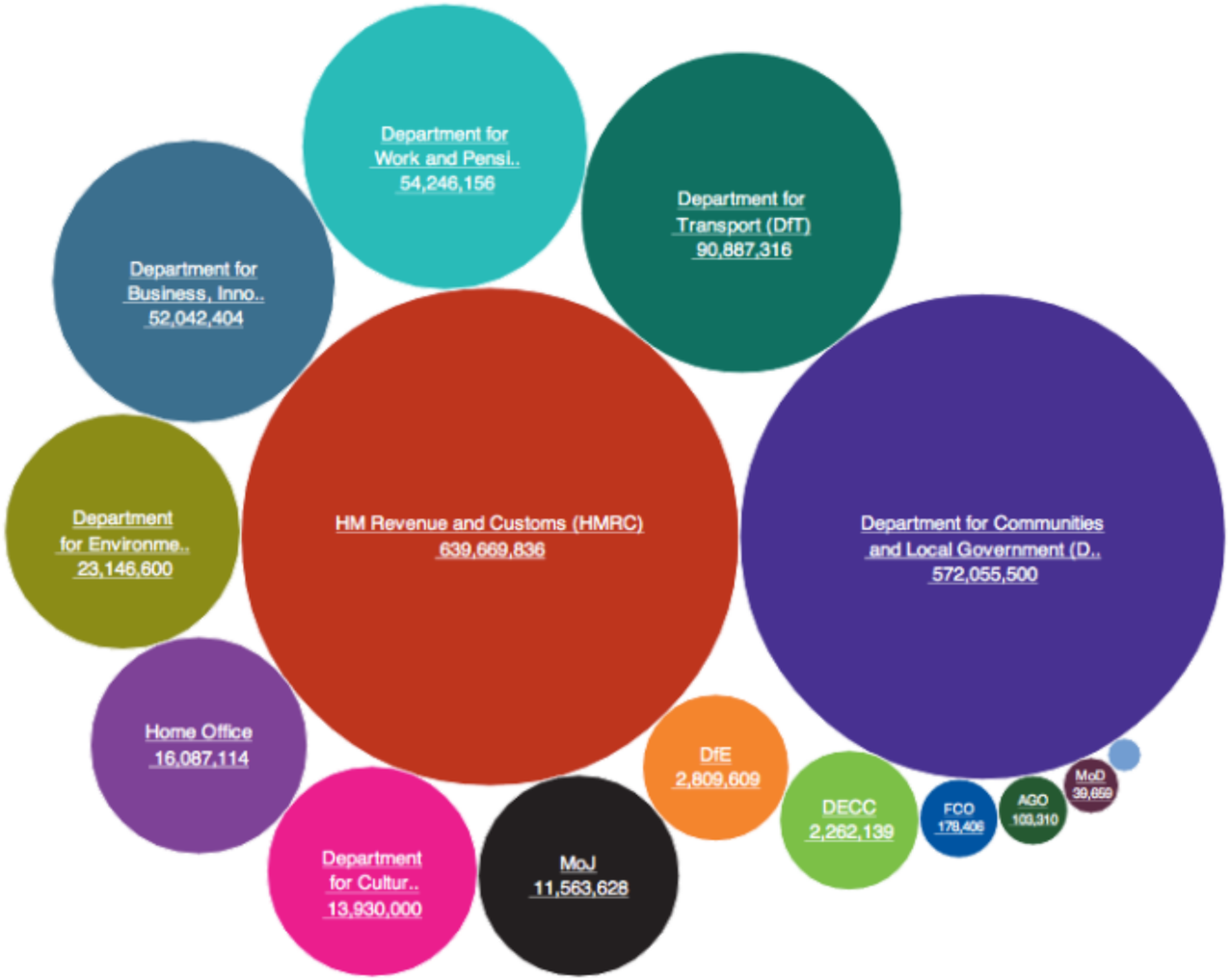
1. Position along a common scale
2. Position on unaligned scales
3. Length
4. Angle / Slope
5. Area
6. Volume / Density / Saturation
7. Hue

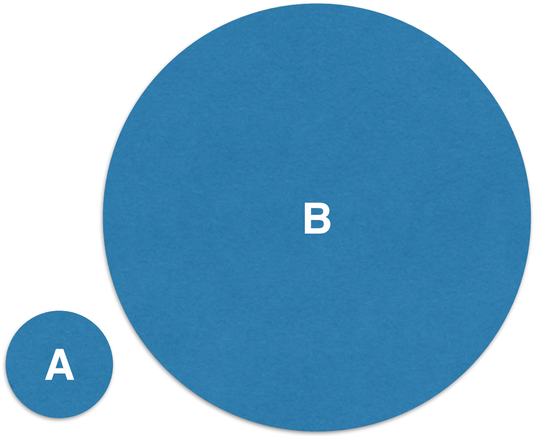
Tougher Decoding


1994
TED

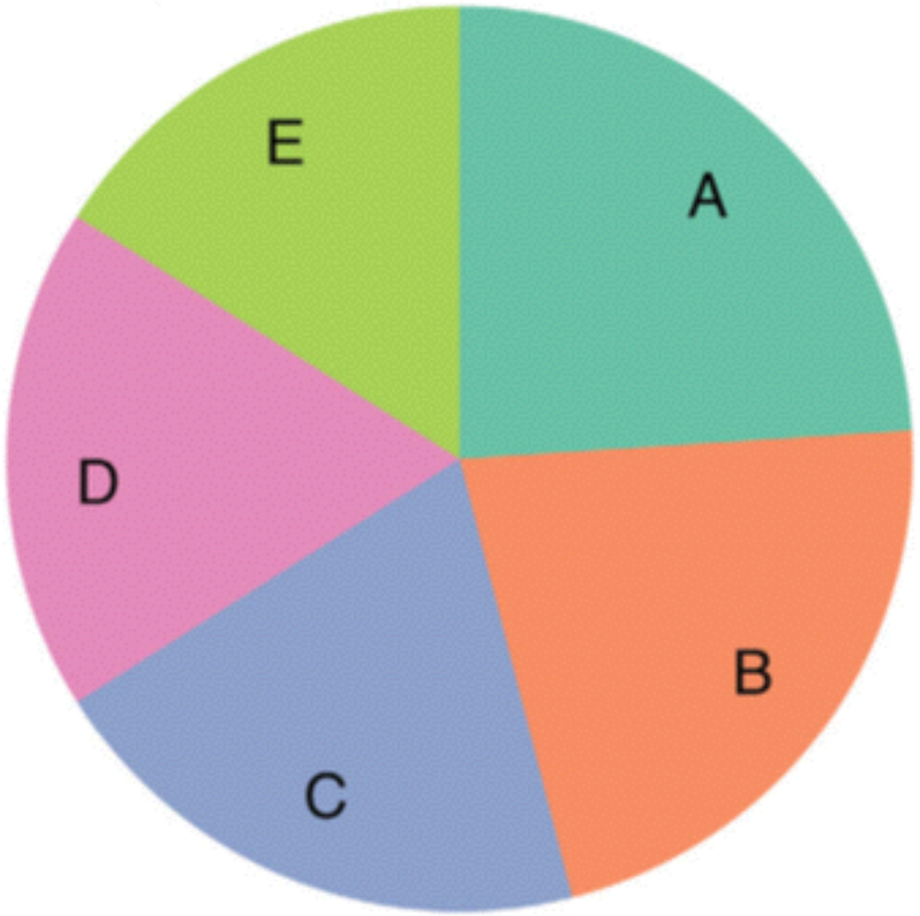
Area

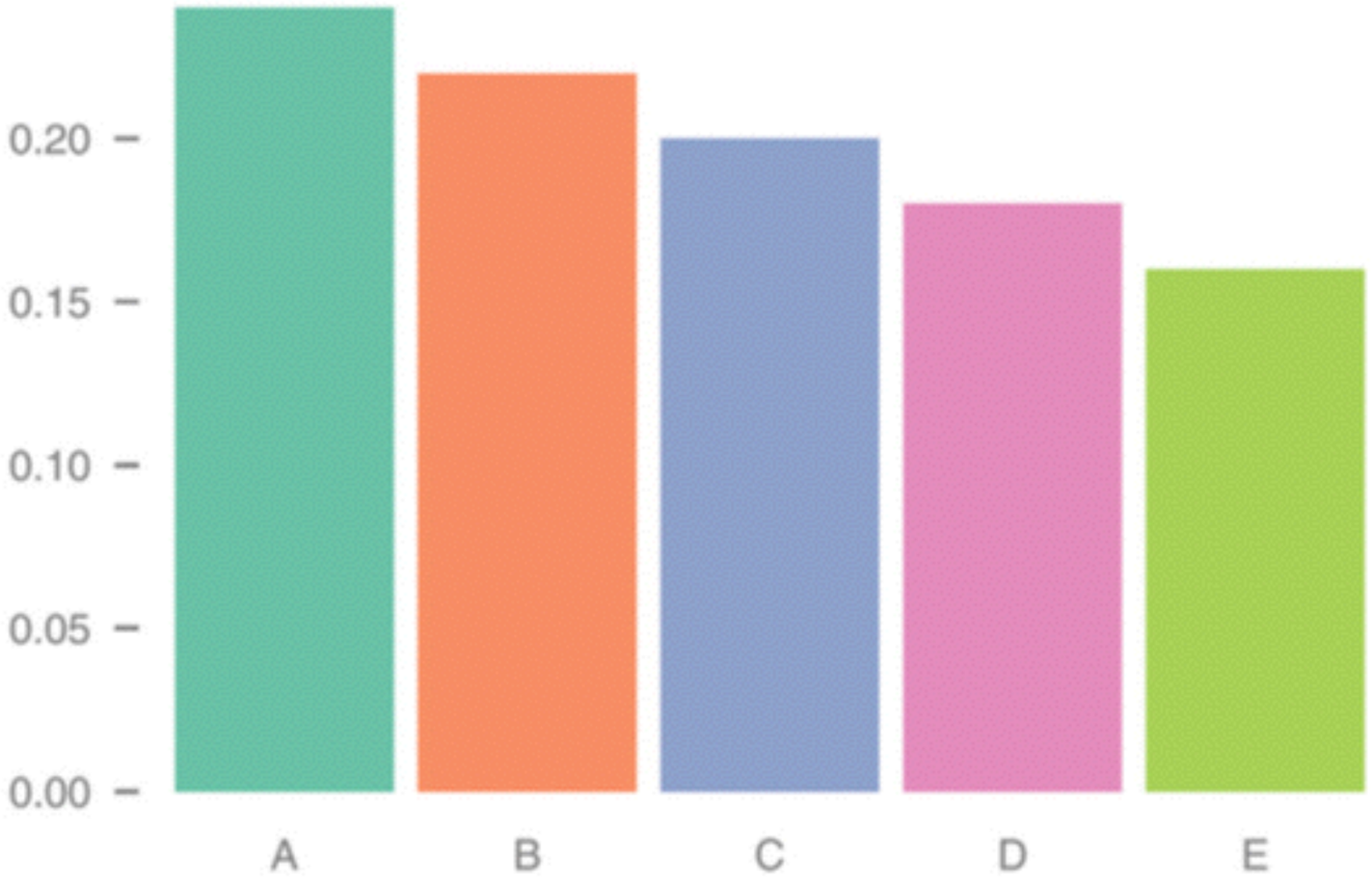
Government transactional services (by volume)



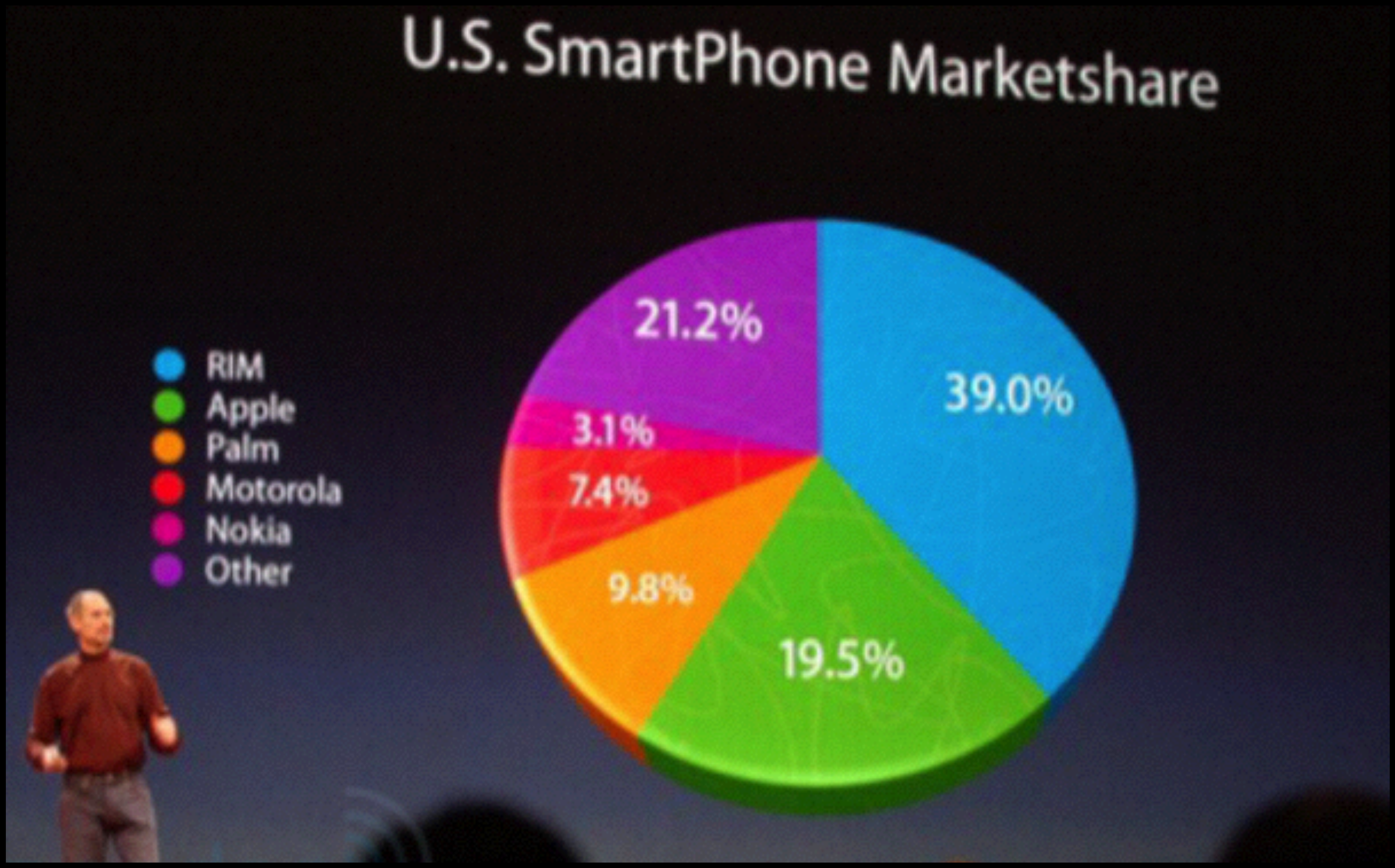


Pie Charts (Area and Angle)





U.S. SmartPhone Marketshare



Trifecta Checkup

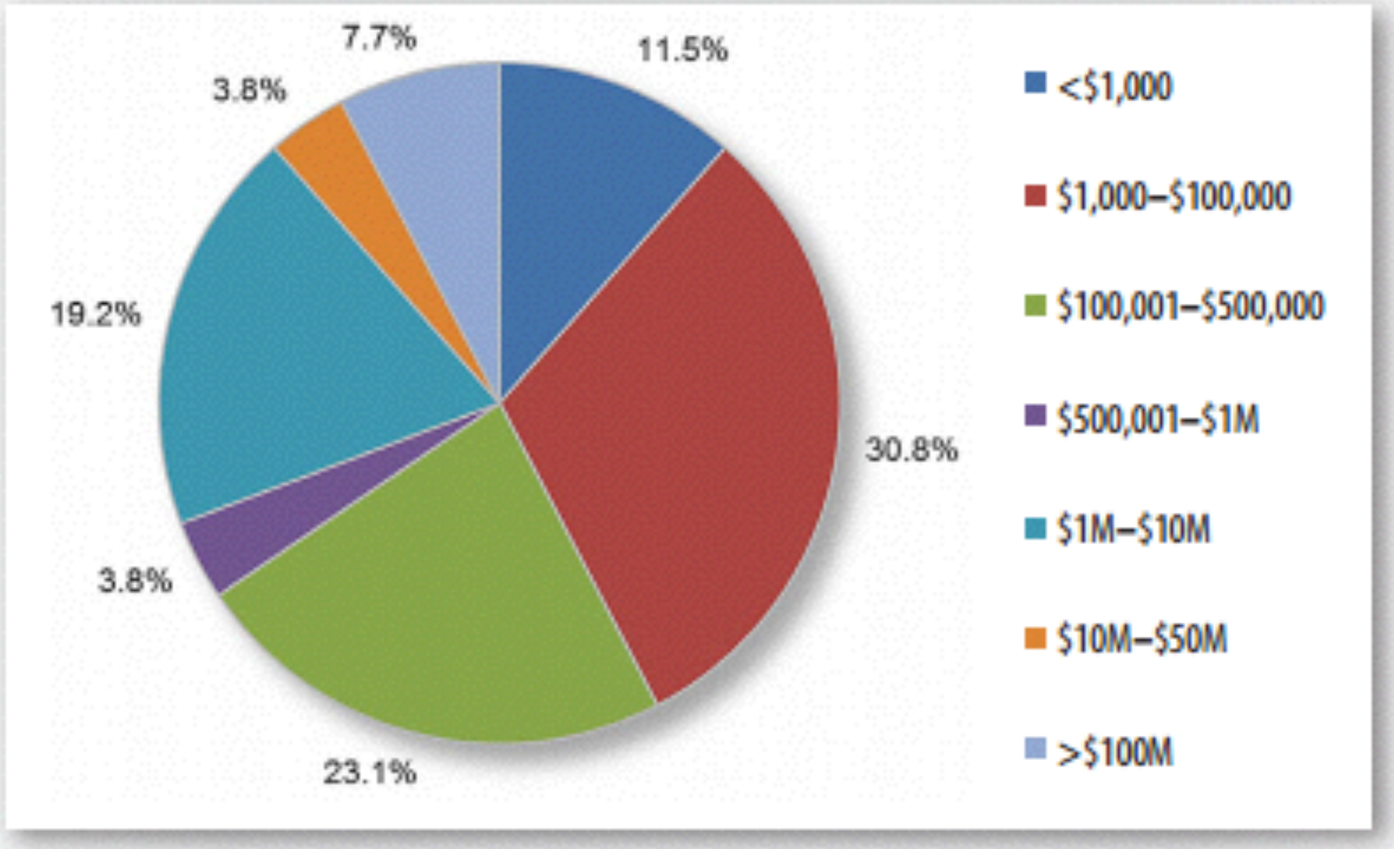
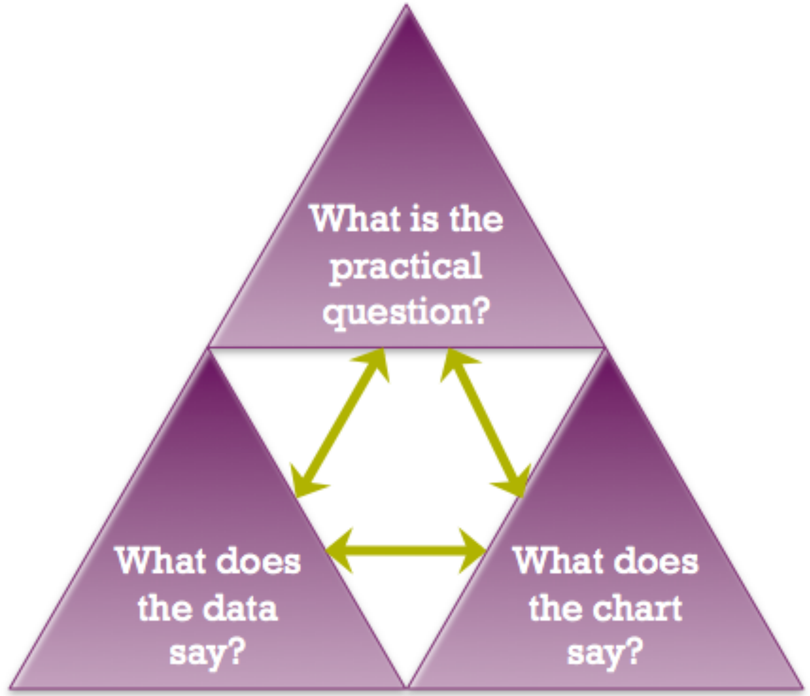
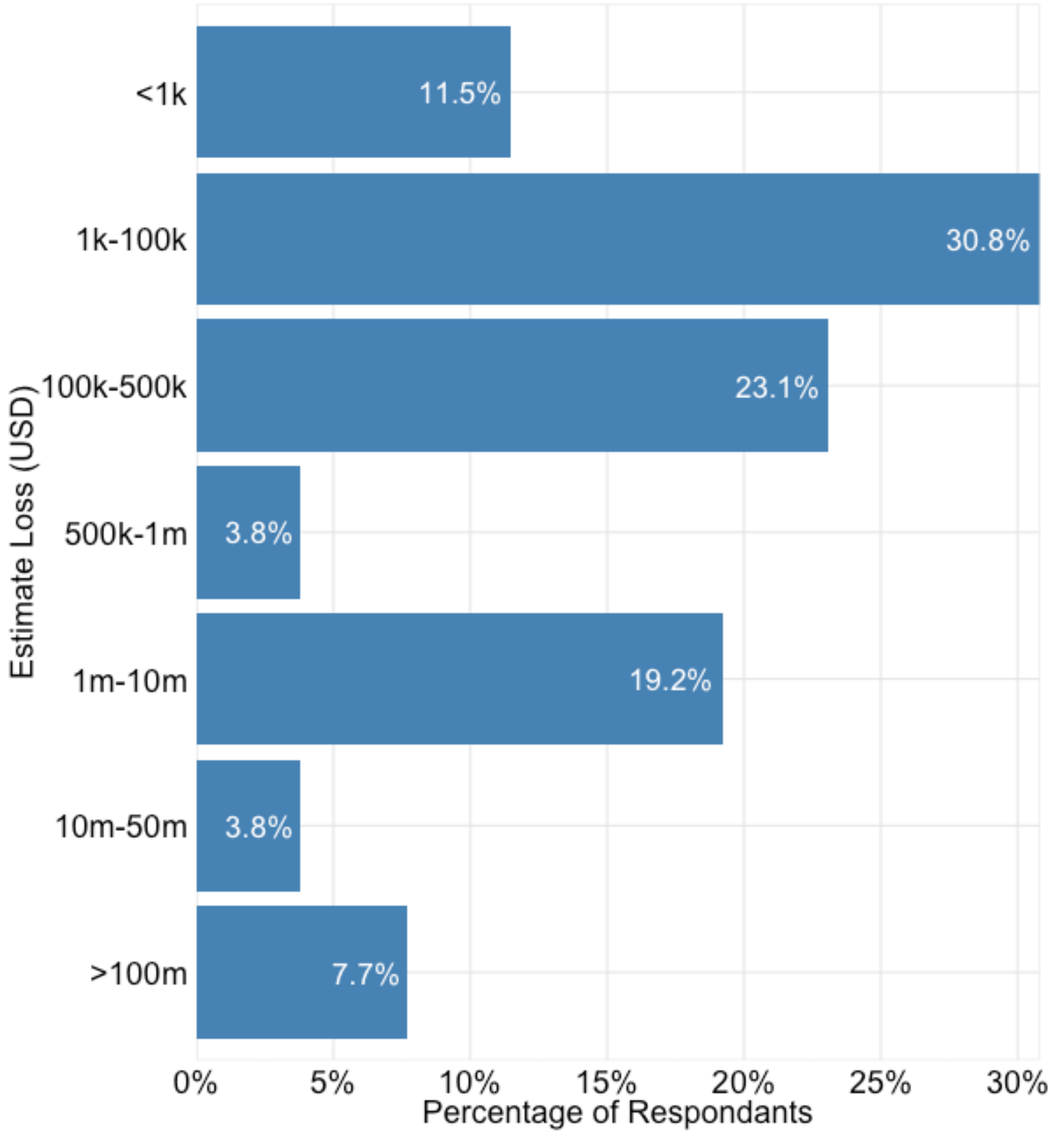


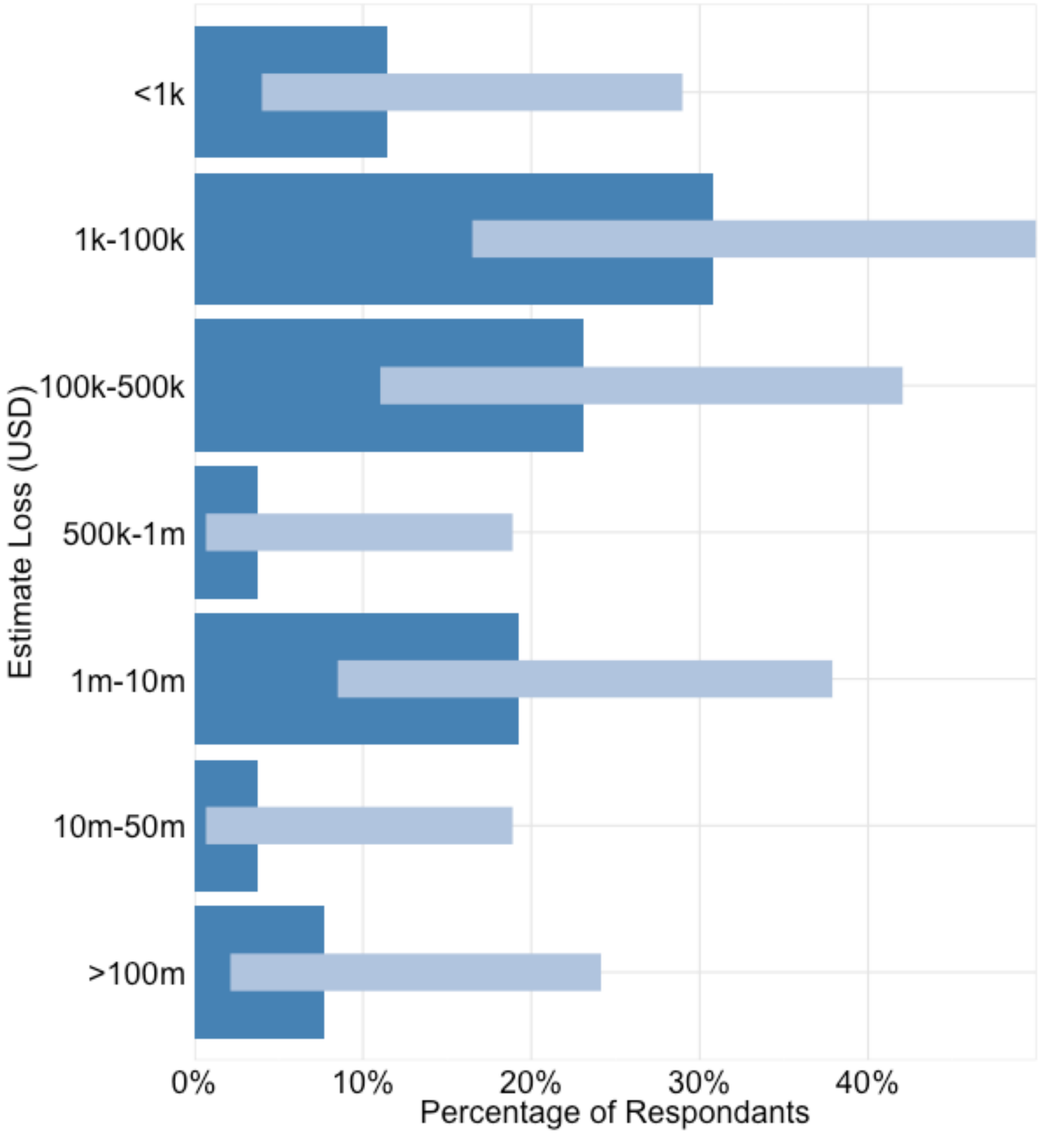
Figure 3. Estimated Financial Losses Experienced[2]



https://www.sans.org/reading-room/whitepapers/analyst/cleaning-breach-post-breach-impact-cost-compendium-36517

Remaking the chart…





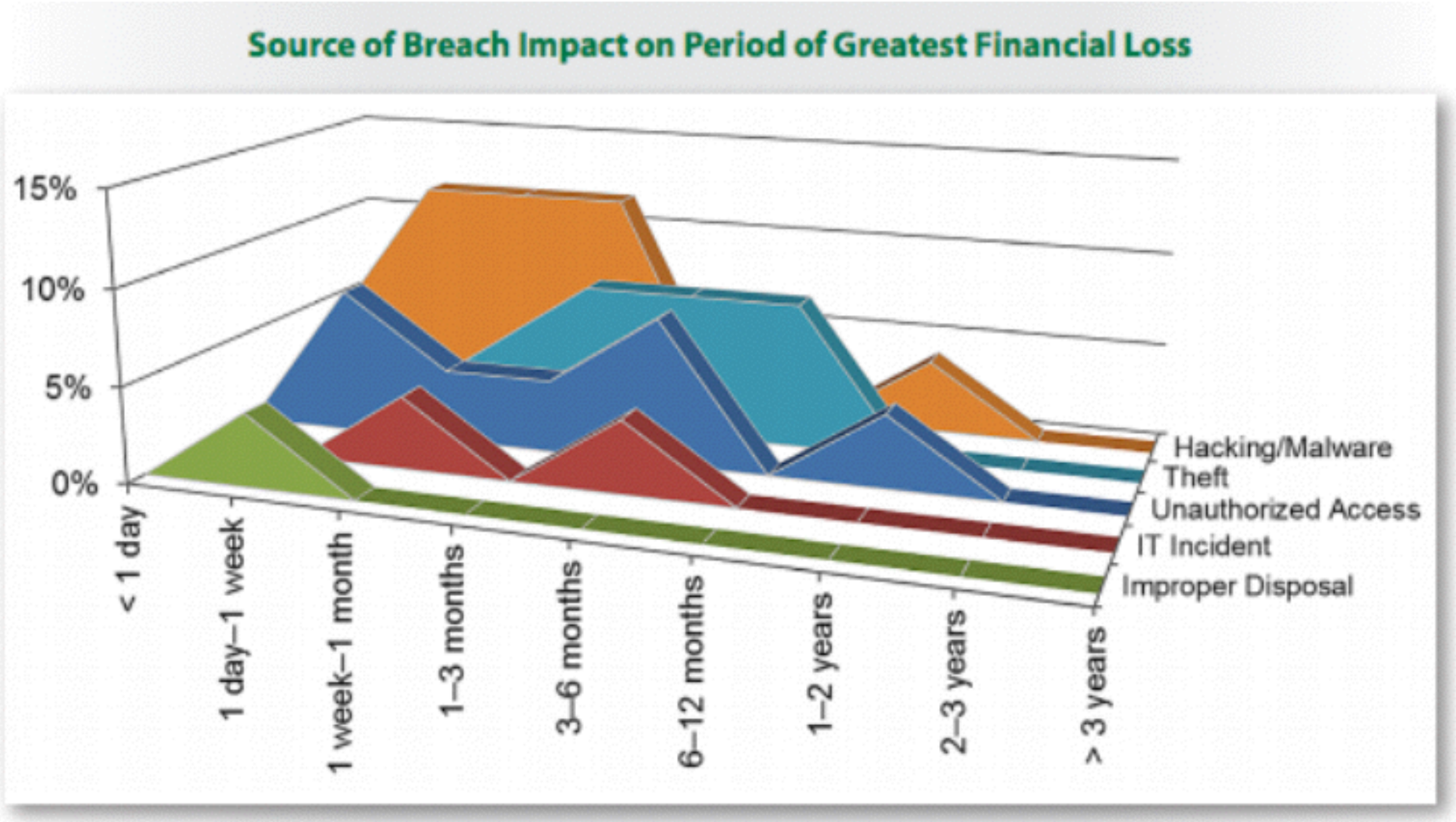


Figure 8. Source of Breach Effect on Period of Greatest Financial Loss

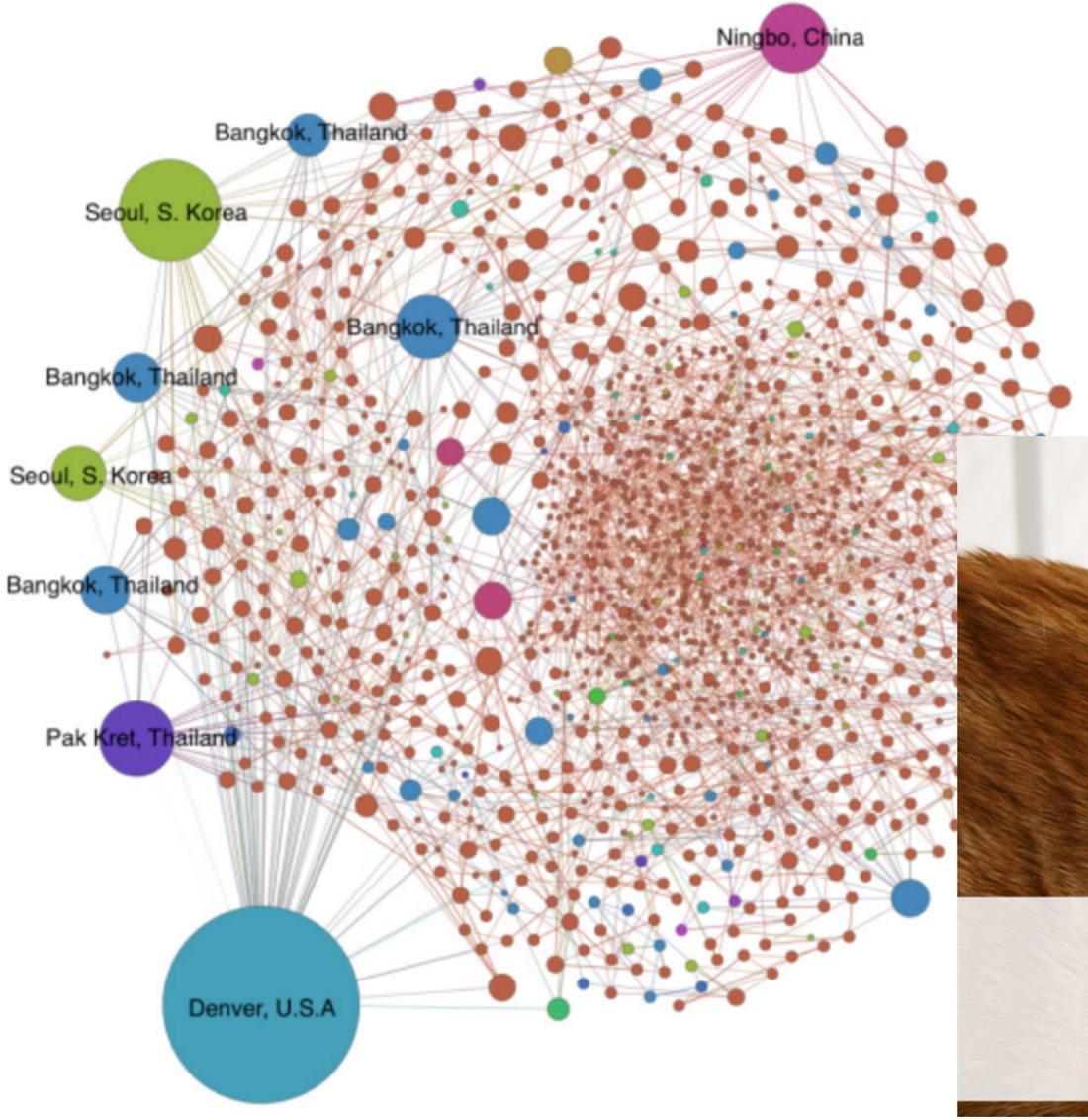
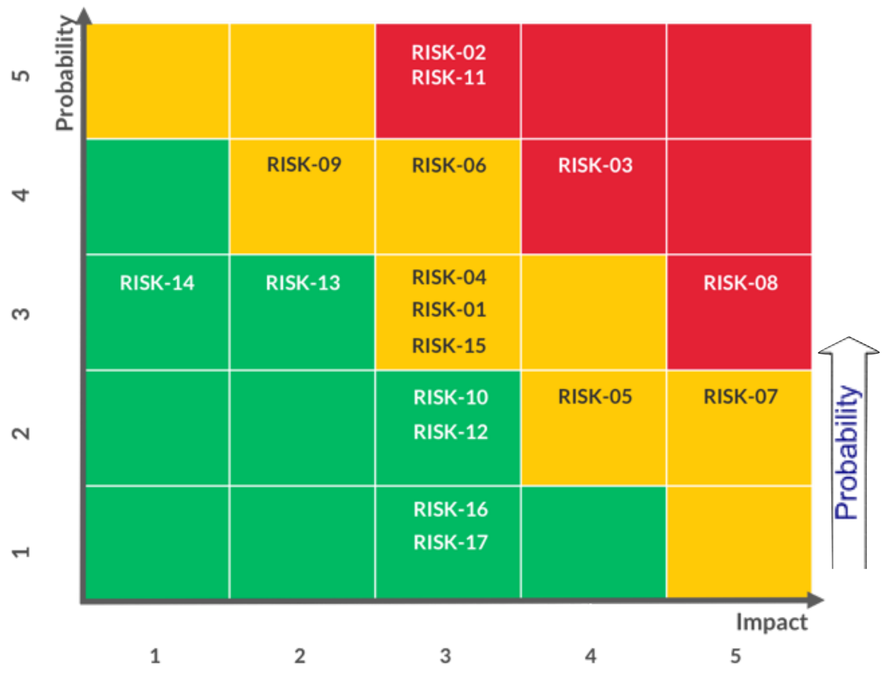
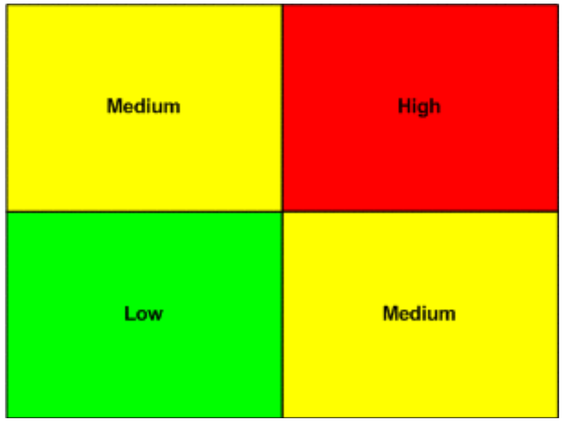
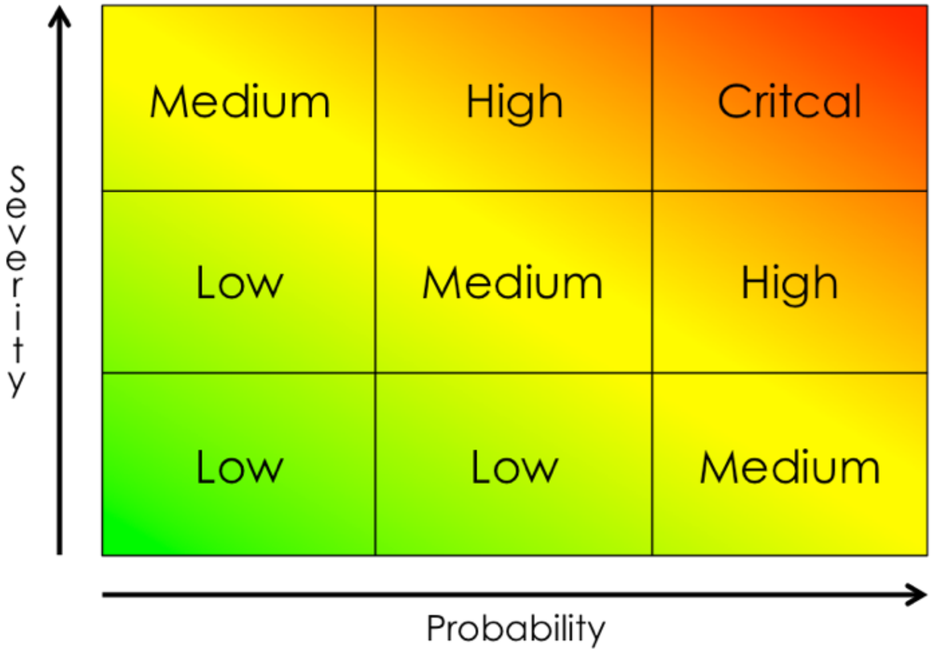


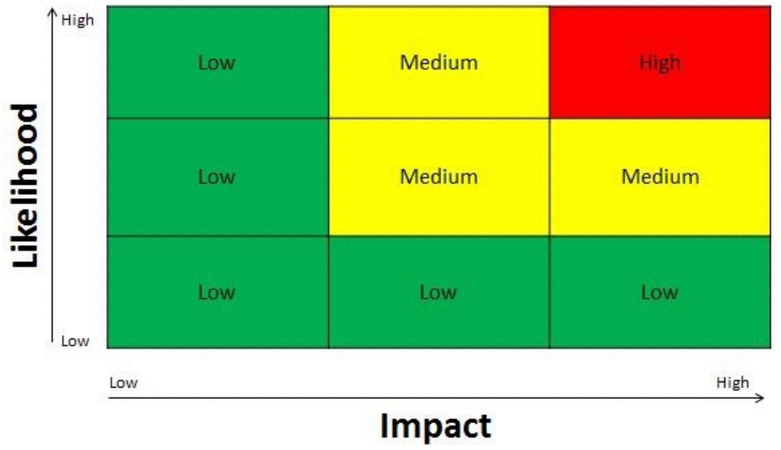
Figure 15: Network graph of all IP addresses associated with greensky27.vicp.net.

Communicating Risk





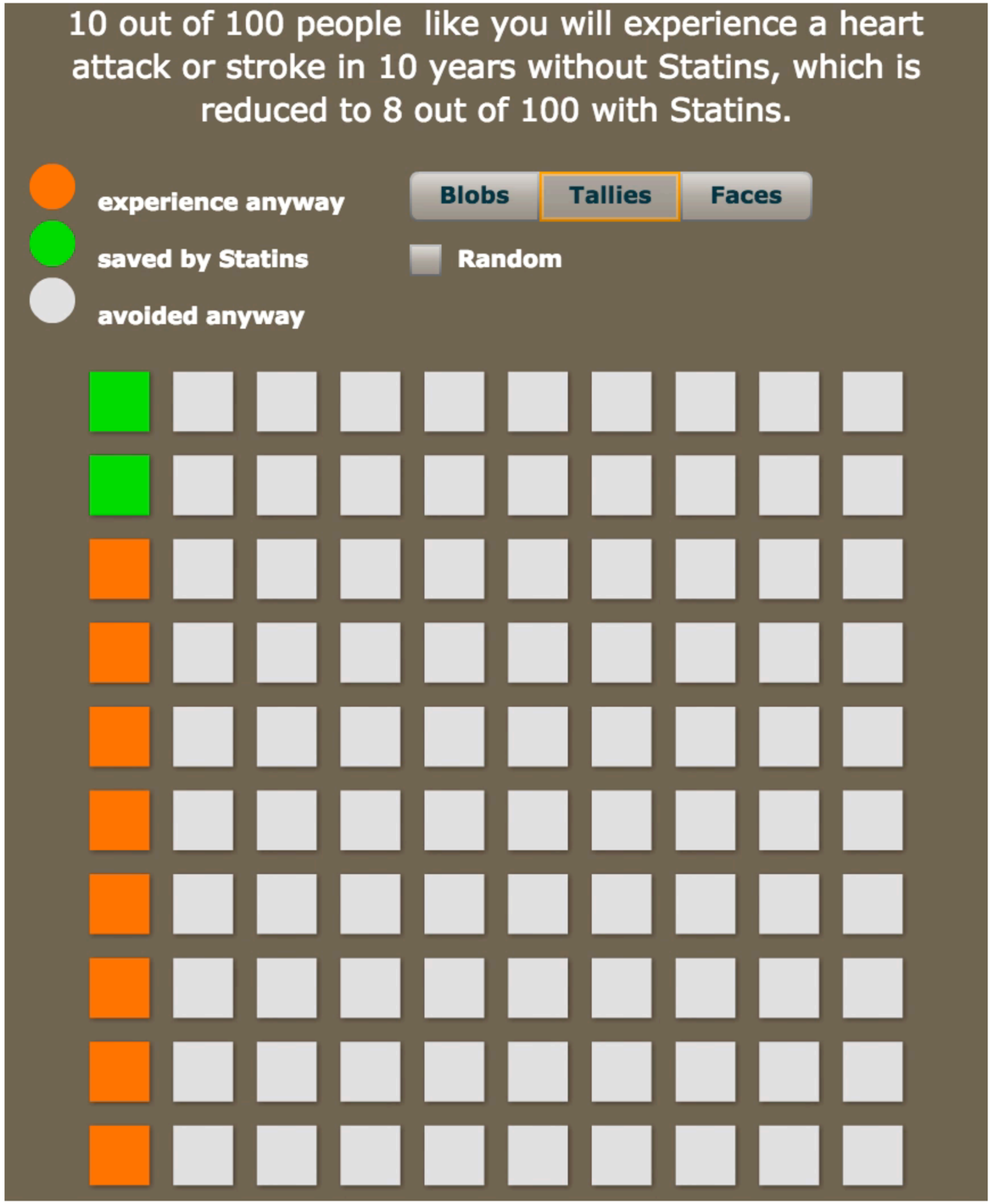




Impact

LIKELIHOOD				
Likely	Medium Risk	High Risk	Extreme Risk	
Unlikely	Low Risk	Medium Risk	High Risk	
Highly Unlikely	Insignificant Risk	Low Risk	Medium Risk	
	Slightly Harmful	Harmful	Extremely Harmful	

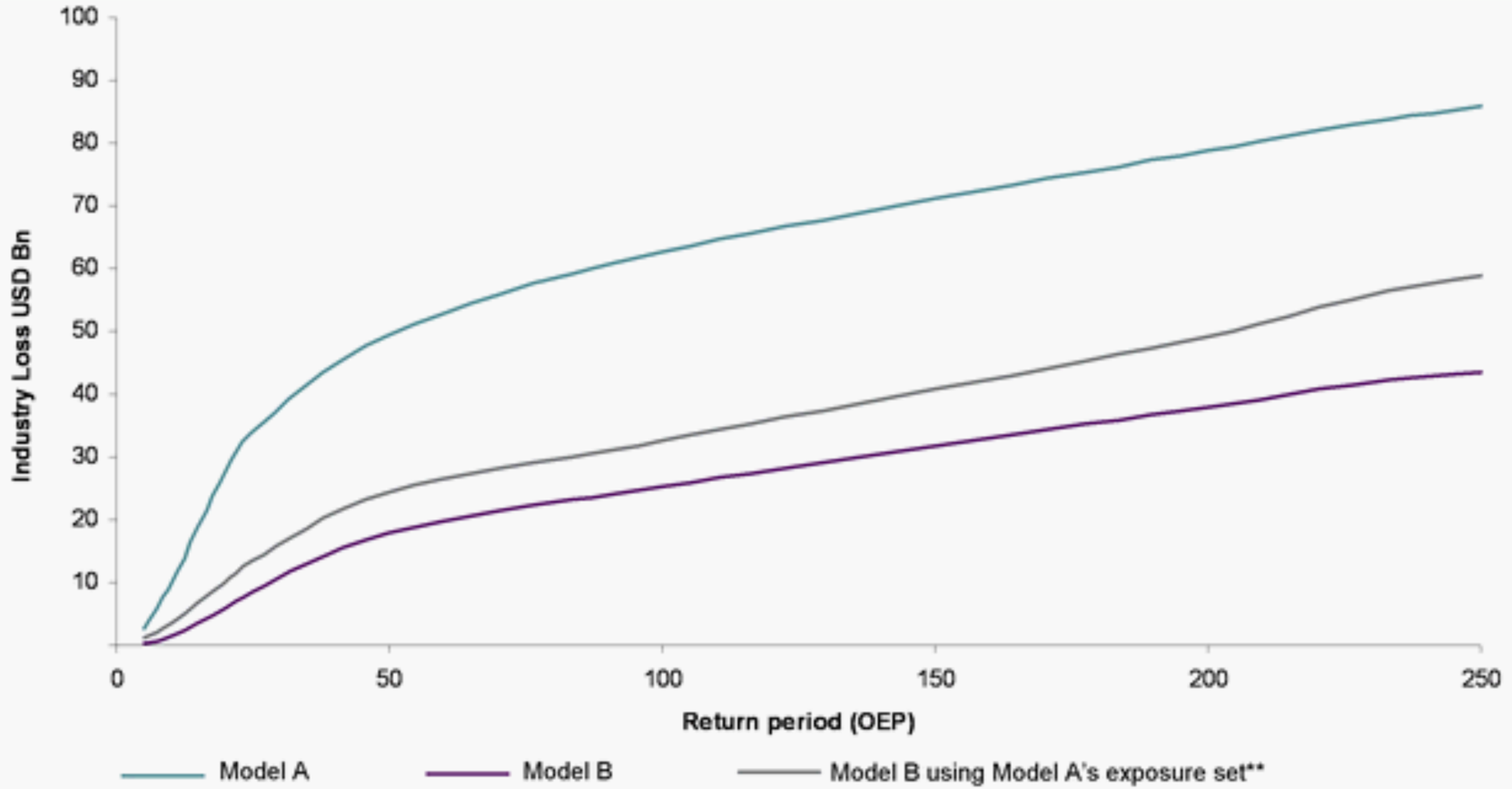
CONSEQUENCES



http://understandinguncertainty.org/node/233

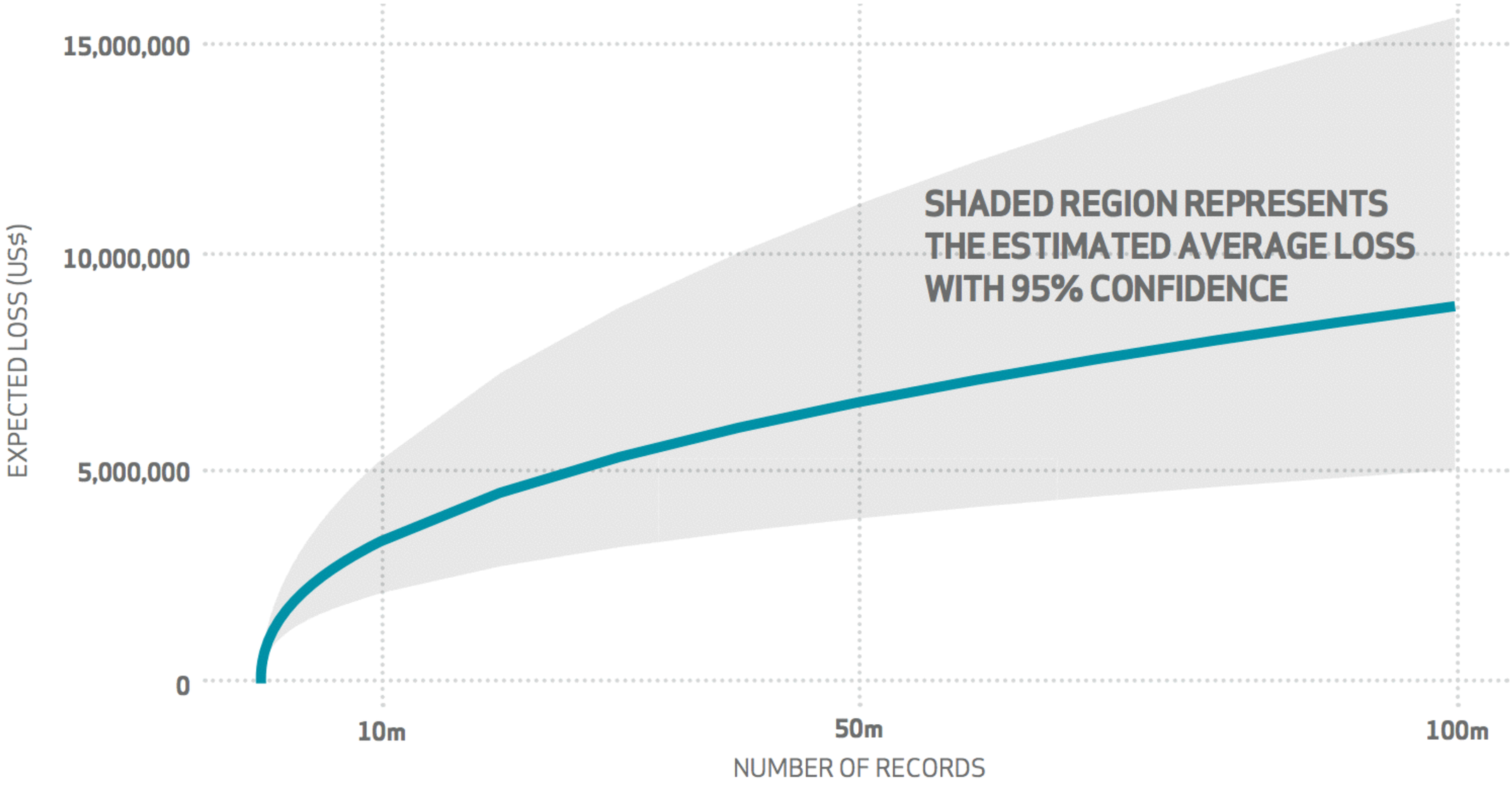
Q1 Cat Events

Japan Earthquake – Modelled Industry Loss

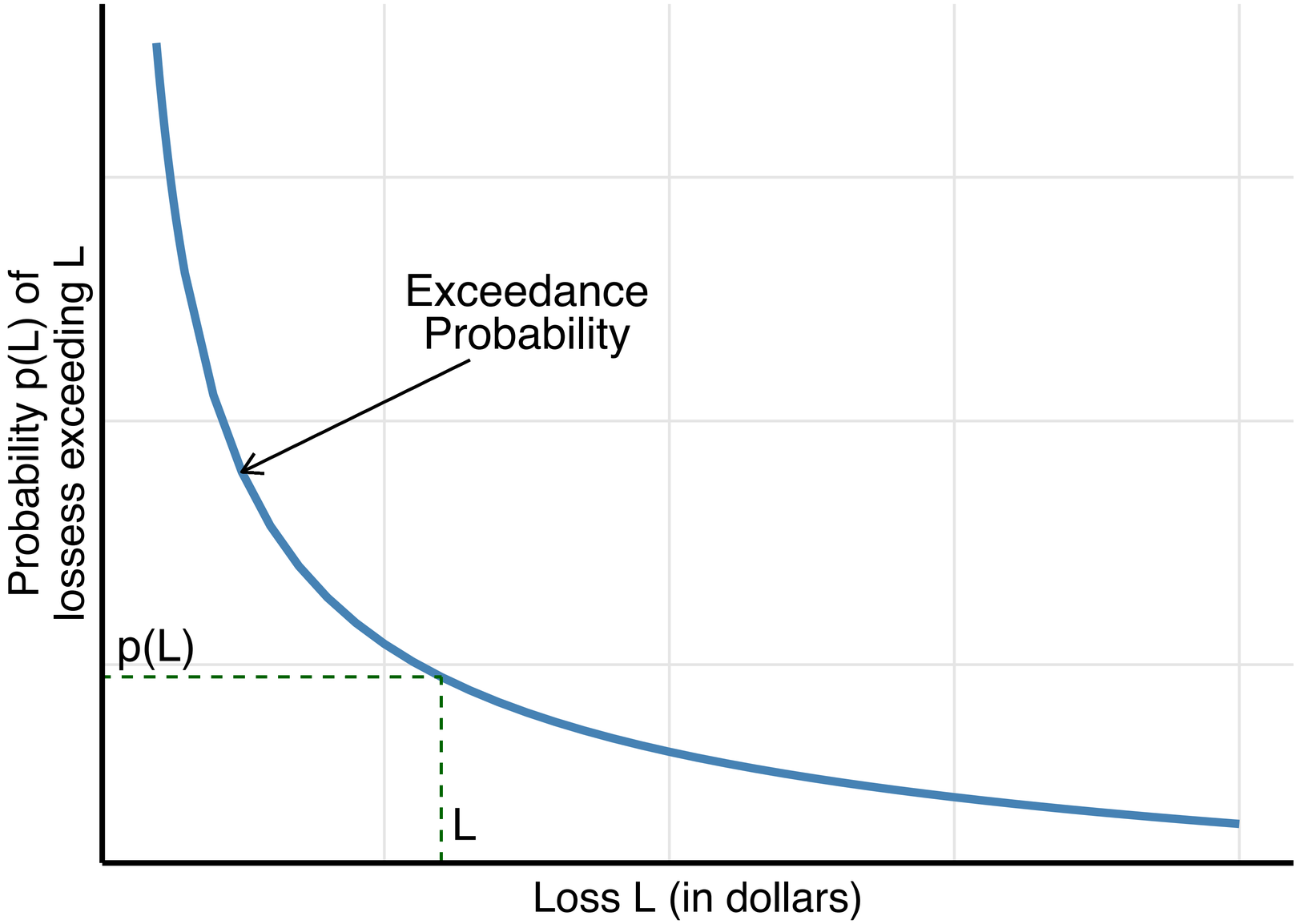


Wide Variation in Modelled Outputs for Industry Loss Exposure in Japan Even When Like for Like Assumptions Deployed

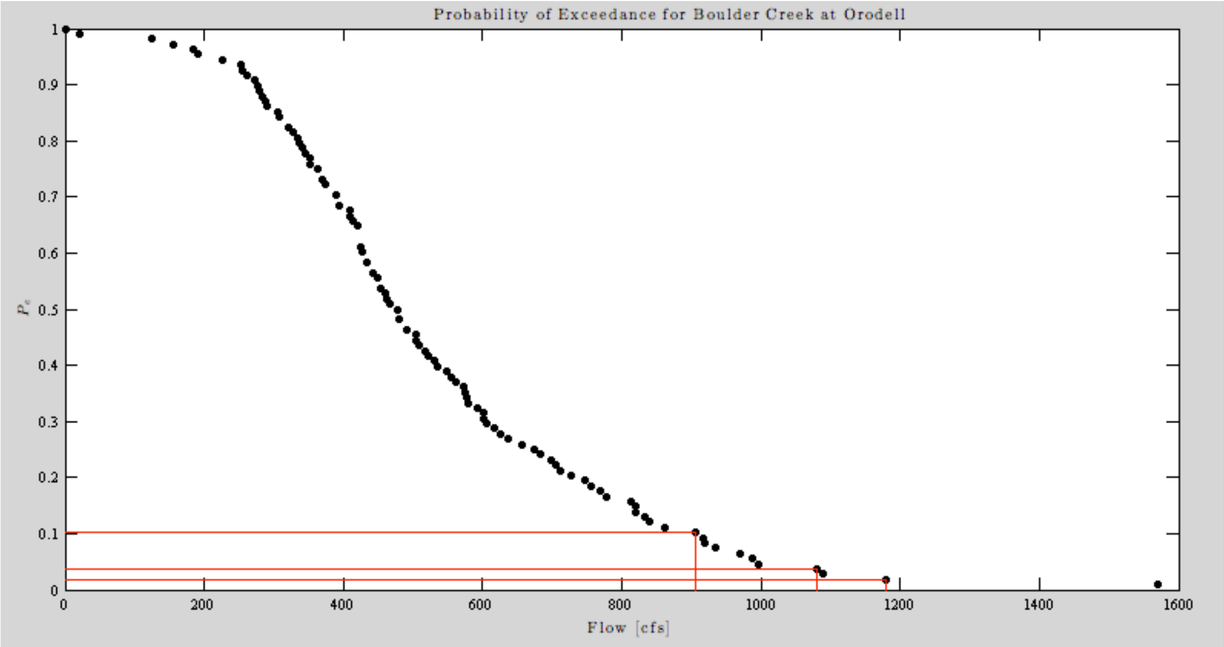
Records and Expected Loss

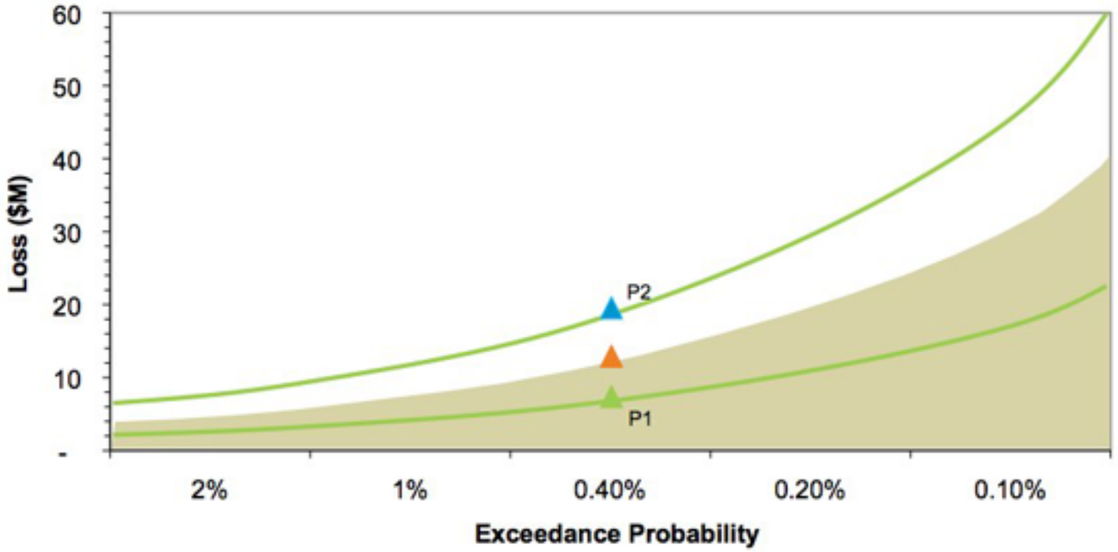


Loss Exceedance Curves



Exceedence Probability

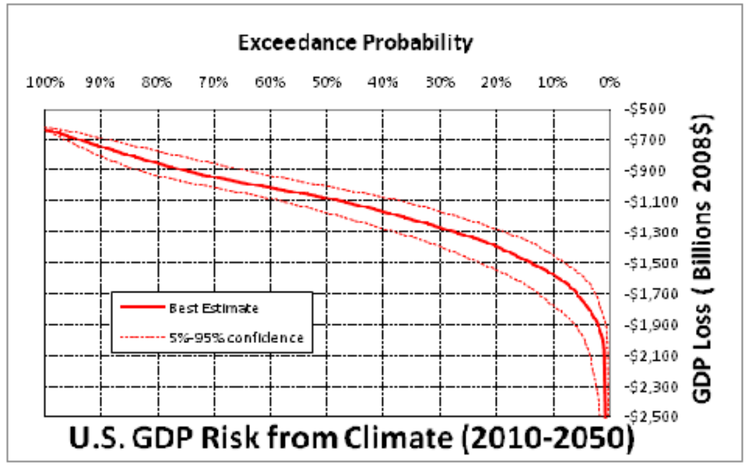


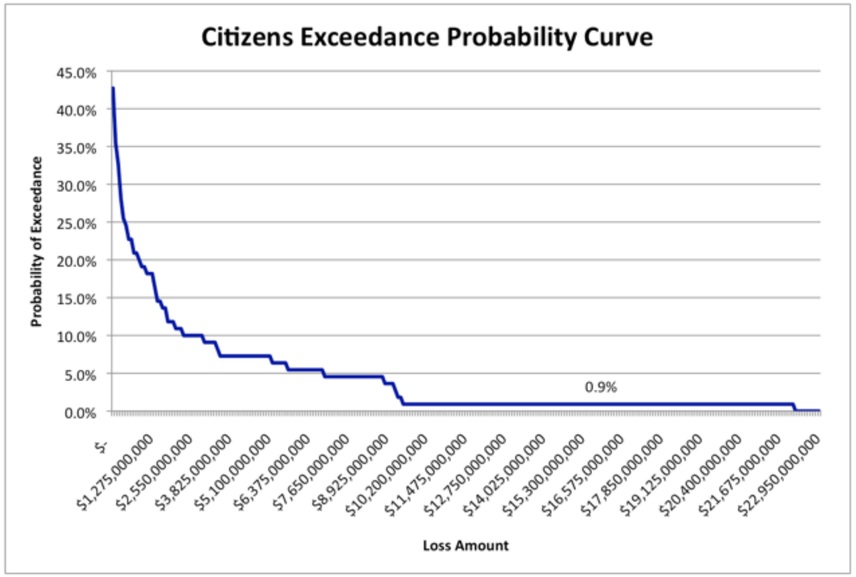


Relationship Between Return Period and Annual Exceedance and Non-exceedance Probability

Return period (years)	p (Annual exceedance probability) (1/return period)	1 - p (Annual non-exceedance probability)
2	0.50 (50%)	0.50
5	0.20 (20%)	0.80
10	0.10 (10%)	0.90
25	0.04 (4%)	0.96
50	0.02 (2%)	0.98
100	0.01 (1%)	0.99

USGS / The COMET Program





Key Takeawars

- **Probability** is unintuitive, difficult and **critical**
- Trifecta Checkup:
  - What is the practical **question**?
  - What does the **data** say?
  - What does the **chart** say?
- Count, compare, predict and infer
- Goal: probability of exceeding loss

Jay Jacobs
Sr. Data Scientist
BitSight Technologies
@jayjacobs

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

Third Party Risk Assessment: Death by 800 Questions

Jack Jones

EVP R&D
RiskLens, Inc.
@jonesFAIRiq

What's the purpose?

Ensure 3rd parties have good security?

Exercise "due diligence?"

Mitigate 3rd party risk?

Help the organization make well-informed decisions about 3rd party risk?

What we'll cover…

- Challenges with the current state
- Alternatives
- Q&A

Challenges with the current state?

So…Darn…Many…Of…Them (3rd parties)

Not…Enough…Resources

Questionnaire length

One, two, three…

…five hundred and ninety one, five hundred and ninety two…

Common types of questions

- Policies & standards
- Processes
- Architecture

But are they the right questions at the right level of detail?

Questionnaires (often) lie

- Okay, perhaps “misinform” is more appropriate
- Why?
  - Ambiguous questions
  - Weasel words
    - “Adequate”
    - “Periodic”
    - “Implement”
    - “Risk assessment”
  - Yes/No answers
  - Sheer volume vs. resources

No such thing as a stupid question…?

- Are there controls in place to limit access from/to the roof?
- How often is the contact information reviewed for accuracy?
- Does your company provide or manufacture products reliant on the forestry/wood or pulp/paper industry?
- Are you using PERL's "system ()" call to run any external programs and NOT using backticks (‘ ‘)?

Interpretation challenges

- For the 3rd party respondent
  - What does this question mean?
  - What qualifies in order to answer “yes”?
  - Time constraints
- For the 1st party reviewer
  - Requires interpretation by individual SME’s
    - All elements treated equally?
    - Introduces bias, inaccuracy, inconsistency, etc.
    - Time constraints

Things change

- One, two, three…
- Crap.
- One, two, three, four…
- Dang it!
- One, two…

Answers reflect a point-in-time state (at best)

Are we achieving any of them?

Ensure 3rd parties have good security?

Exercise “due diligence?”

Mitigate 3rd party risk?

Help the organization make well-informed decisions about 3rd party risk?

Alternatives

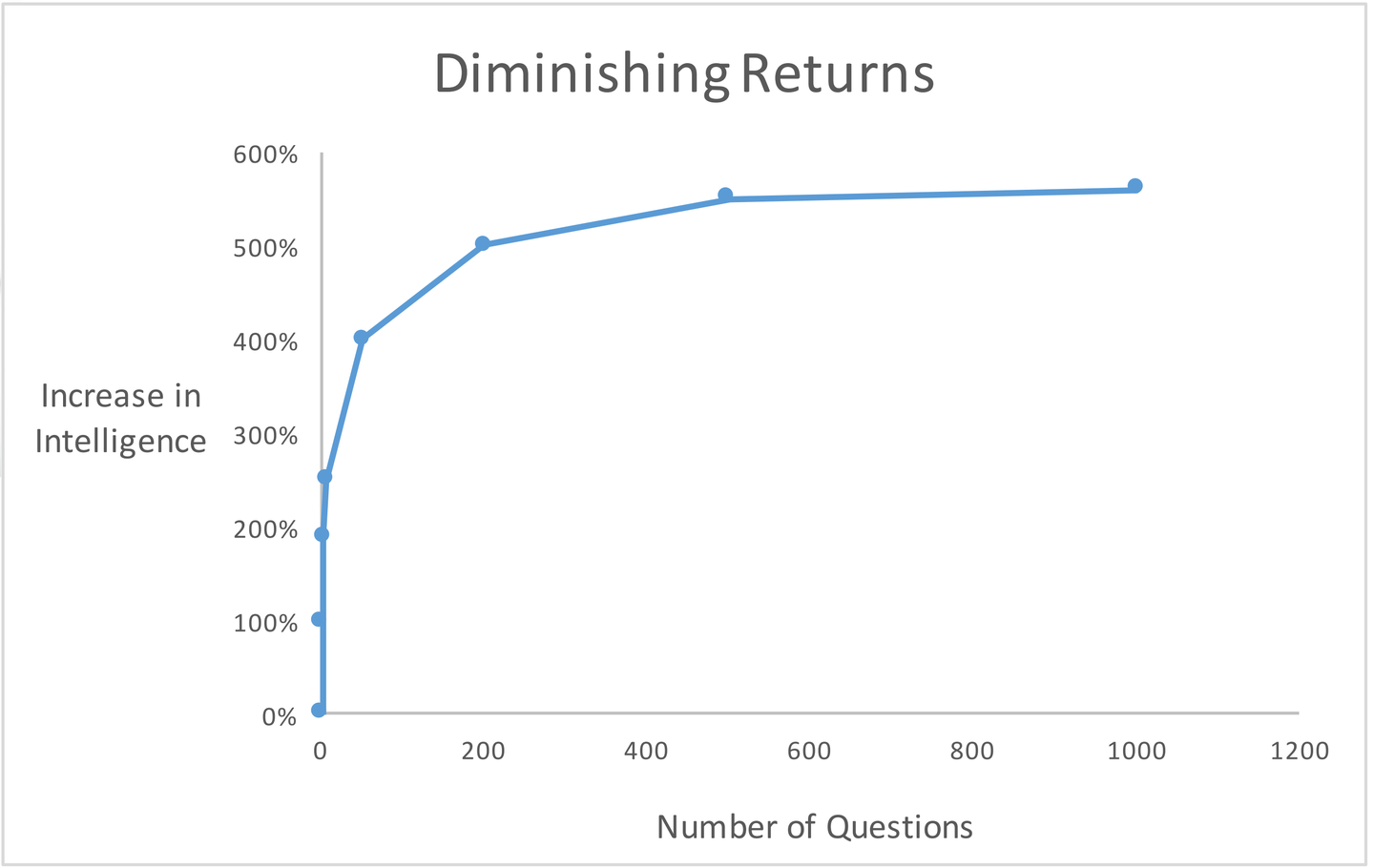
Refined objective

Cost-effectively understand which 3rd parties we need to worry about most.

How much do we need to know, really?

- How much more do you learn, really, from 1600 questions versus 160, or 16?

There are diminishing returns



Start with impact triage

- Three dimensions:
  - Access to sensitive information
    - What kind?
    - How much?
  - Critical operations dependency
  - Network connectivity (what can they get to?)

Step 2: Look for symptoms of weakness…

- Limping
- Erratic behavior

Step 2: Look for symptoms of weakness…

- Vulnerable conditions
- Immature risk management

Look for symptoms of weakness…

- Discrete vulnerable conditions
  - Poor security test results (e.g., from scanning)

Discrete Vulnerability Evaluation

- Advantages
  - Can be a good indicator of risk level and risk management efficacy
    - …but need some additional information to be sure
  - Can be more data driven
  - Some degree of automation may be leveraged
- Disadvantages
  - Lagging indicator
  - Scope dependent
  - May be difficult to get approvals to perform testing or see test results

Look for symptoms of weakness…

- General control conditions
  - Patching efficacy
  - Access privilege management
  - Detection capabilities
  - Etc.

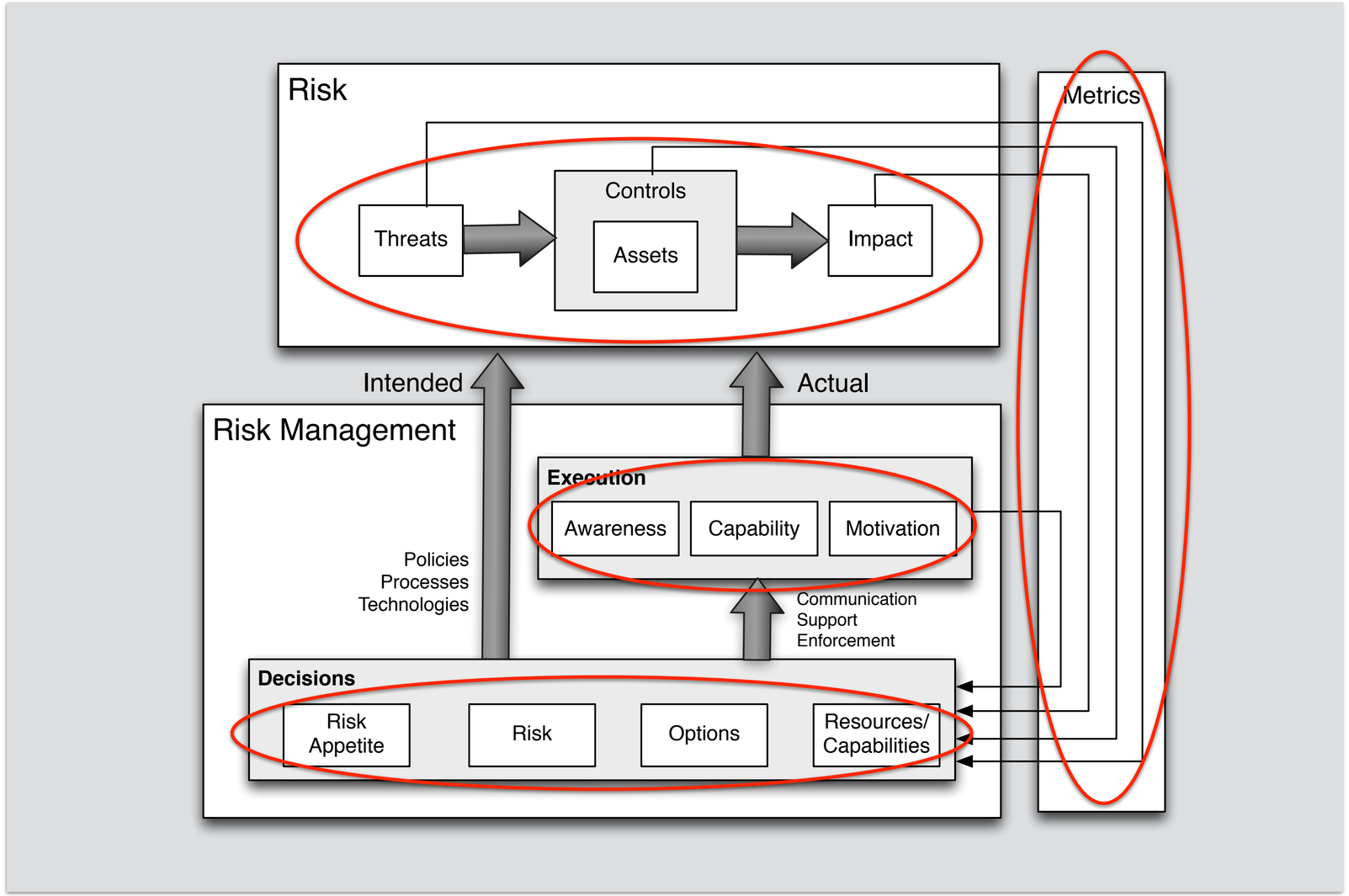
General Vulnerability Evaluation

- Advantages
  - Can be a good indicator of risk management efficacy
  - Can be a good indicator of overall control conditions
  - Easy information to get (if you ask the right questions in the right way)
- Disadvantages
  - Lagging indicator
  - General in nature

Look for symptoms of weakness…

- Immature risk management
  - Poor decision-making capability
  - Poor execution

The role of risk management…



Evaluating risk management

- Decision-making
  - Visibility into:
    - Assets
    - Threat landscape
    - Controls
    - Deficiency root causes
  - Analytics
    - Ability to prioritize effectively

Evaluating risk management

- Execution
  - Awareness
  - Capabilities
  - Motivation

Risk Management Maturity Evaluation

- Advantages
  - Can be a good indicator of undetected vulnerability
  - Leading indicator (root causes)
  - Easy information to get (if you ask the right questions in the right way)
- Disadvantage
  - Less data driven
  - Many (most?) organizations are immature

Ask questions differently

General Controls Example

Threat Event Visibility	Which of the following best describes your organization's ability to capture data regarding threat events (e.g., failed login attempts, unsuccessful attempts to access files, network protocol violations, etc.)?	○ Few if any meaningful capabilities exist (e.g., logs, etc.)to capture potential threat activity. ○ Capabilities exist to capture threat activity on some of the key assets and points of attack, but important gaps in coverage remain. ○ Most if not all potentially threatening activity is captured on critical assets, the internal network, and external points of attack. No important gaps in coverage exist.

RiskLens™

Risk Management Example

Asset Visibility	Which of the following best describes your organization's visibility into its system and information assets? The purpose is to gauge the organization's ability to know where its assets are and what their value is.	○ An inventory of information, applications, and system assets does not exist or is severely out of date (i.e., cannot be relied on to support decision-making). Processes for maintaining the inventory either do not exist or are not practiced. ○ An inventory of information, applications, and system assets exists but is not consistently maintained. Processes for maintaining the inventory are immature or are exercised unreliably. Audits of the inventory regularly find more than 5% of the entries are inaccurate. ○ An inventory of information, applications, and systems assets exists and is kept up-to-date through well-defined and consistently practiced

Keys to effective questions…

- Be descriptive
- Add guidance to reduce ambiguity
- Use quantitative parameters where feasible
- Use simple language

Applying What You Have Learned

- Next week you should:
  - Evaluate your 3rd party assessments for:
    - The number of questions. (Diminishing returns?)
    - Yes/No answers?
- In the first three months following this presentation you should:
  - Introduce impact-related triage to identify 3rd parties that represent the greatest potential impact
  - Reduce the number of questions. Focus on higher-level elements that suggest vulnerability and/or risk management weakness.
  - Weed out or refine ambiguous questions.

Applying What You Have Learned

- Within six months you should:
  - If you're using yes/no answers, change them to multiple choice (e.g., Strong, Partial, Weak).
  - …or, better yet, change to questions/answers that are descriptive in nature.

Summary

- The current approach to 3rd party risk assessments usually don’t help us meet our objectives — at least cost-effectively
  - Information inaccuracy
  - Diminishing returns
- An improved approach is possible using better triage and looking for higher level information that helps us to identify symptoms of weakness
  - Vulnerability (specific and/or general)
  - Risk management immaturity
- Descriptive questions and answers can be more informative than those that seek a yes/no or strong/partial/weak answer

Questions

Please fill out your session evaluation form!

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

The Marriage of Threat Intelligence and Risk Assessment

Wade Baker

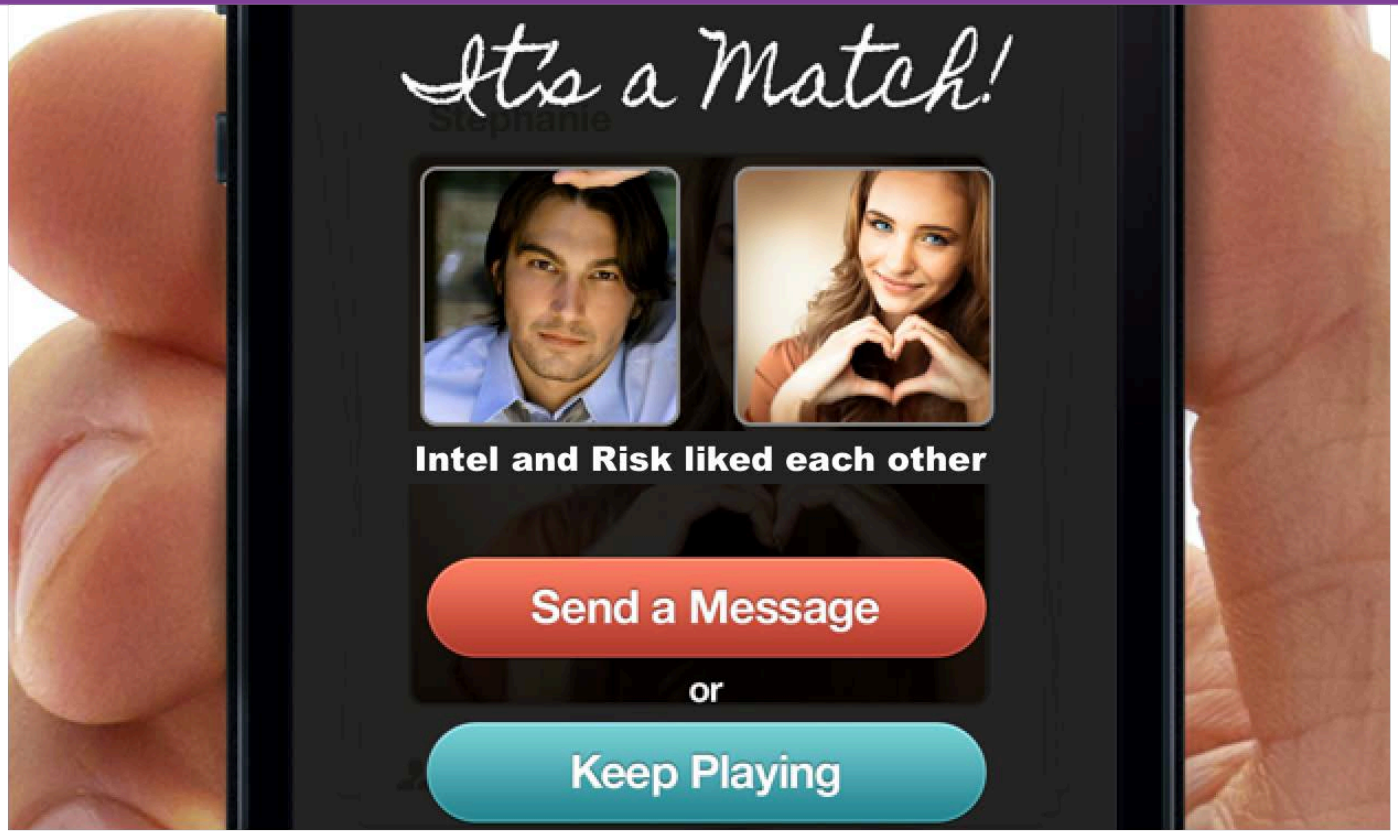
VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker

#RSAC

Underlying assumption

Good **intelligence** makes smarter **models**;
Smarter models inform **decisions**;
Informed decisions drive better **practice**;
Better practice improves risk **posture**;
which, done efficiently,
Makes a successful security **program**.

Intel & Risk: Those two should hook up…



…but they haven't quite hit it off…

Threat Intelligence

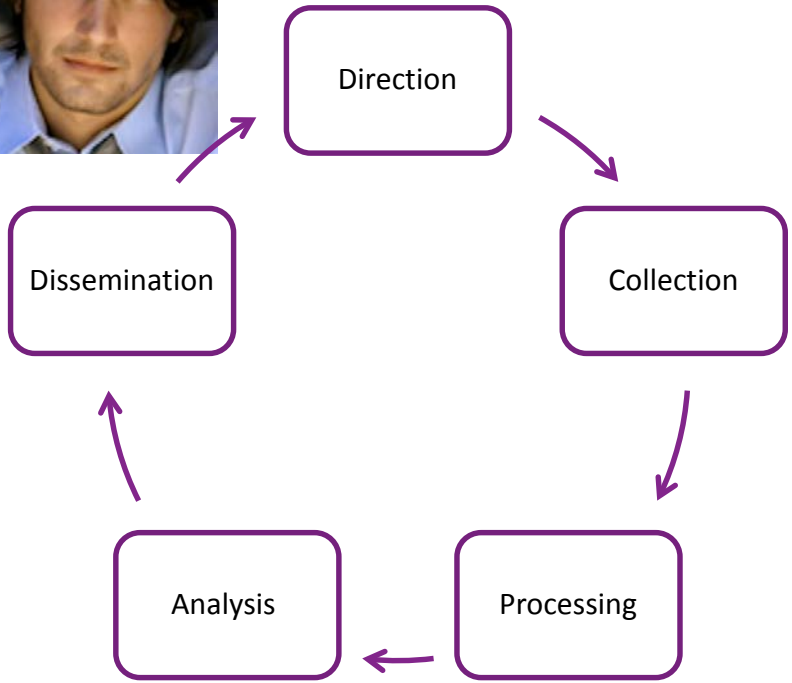
- "There's way too much uncertainty in her life. I need something predictable."
- "I'm a simple guy from the STIX and drive a TAXII; she's a one-percenter by nature."
- "Everything's an assessment with her; I don't want to be managed!"
- "Sure, she's a great model now, but I worry about overfitting as she gets older."

Risk Management

- "I feel like I'm under constant surveillance; he tries to control my private domain."
- "I don't like the way he treats me; he needs to just accept me as I am."
- "He won't open up and never shares. I swear, if he TLP-Red's me one more time…"
- "What's his deal with China, anyway? It's uncomfortable around my Asian friends."

...& they run in such different circles

Threat Intelligence



Risk Management

Let’s help this young couple find love

Agenda

- Marriage of Risk & IR in Verizon's DBIR.
- *Dating*: Let's get to know each other.
- *Love*: There's something special here.
- *Marriage*: How does this actually work?

The Marriage of Risk and IR in Verizon's DBIR

Risk + IR = Love

Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%

Dating:

Let's get to know each other

What is threat intelligence?

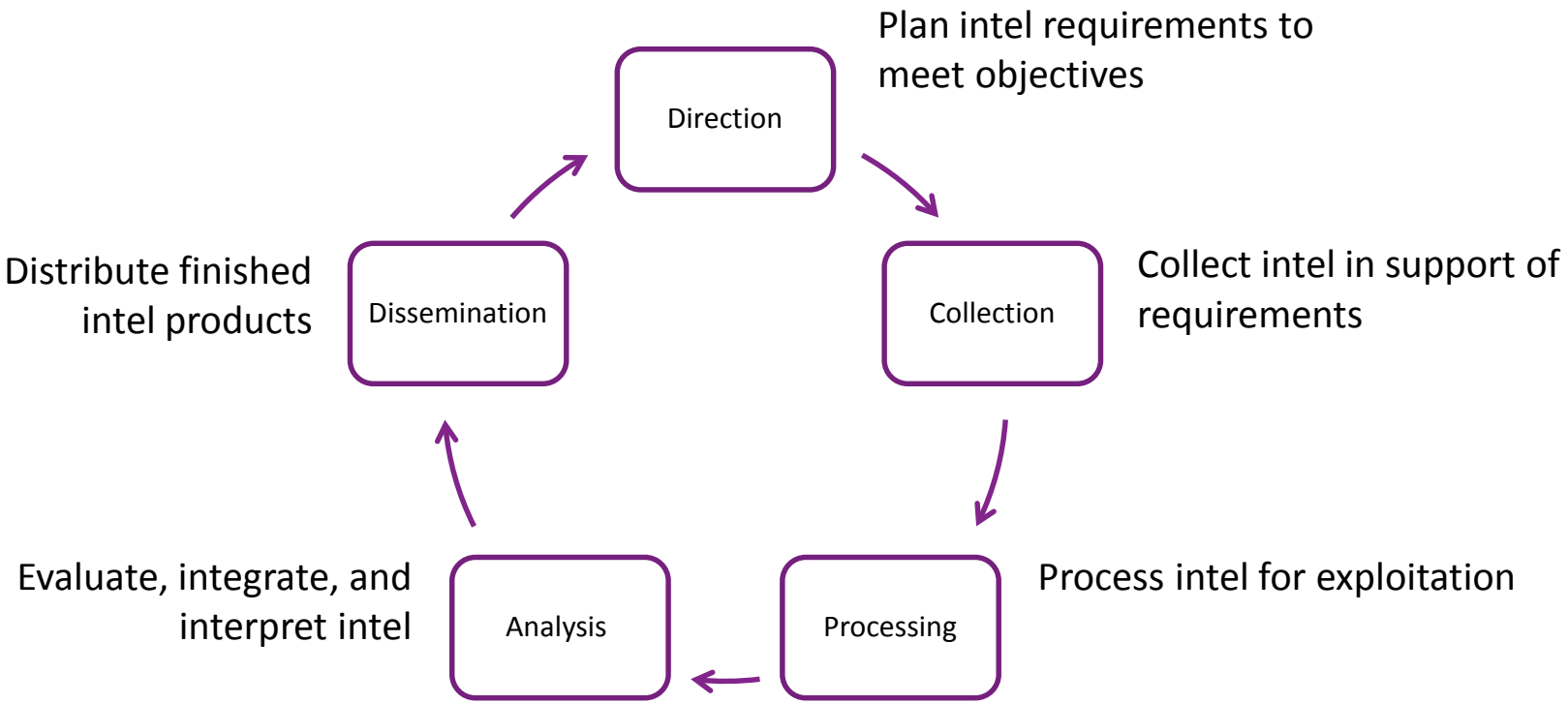
"Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

Gartner

"The details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats."

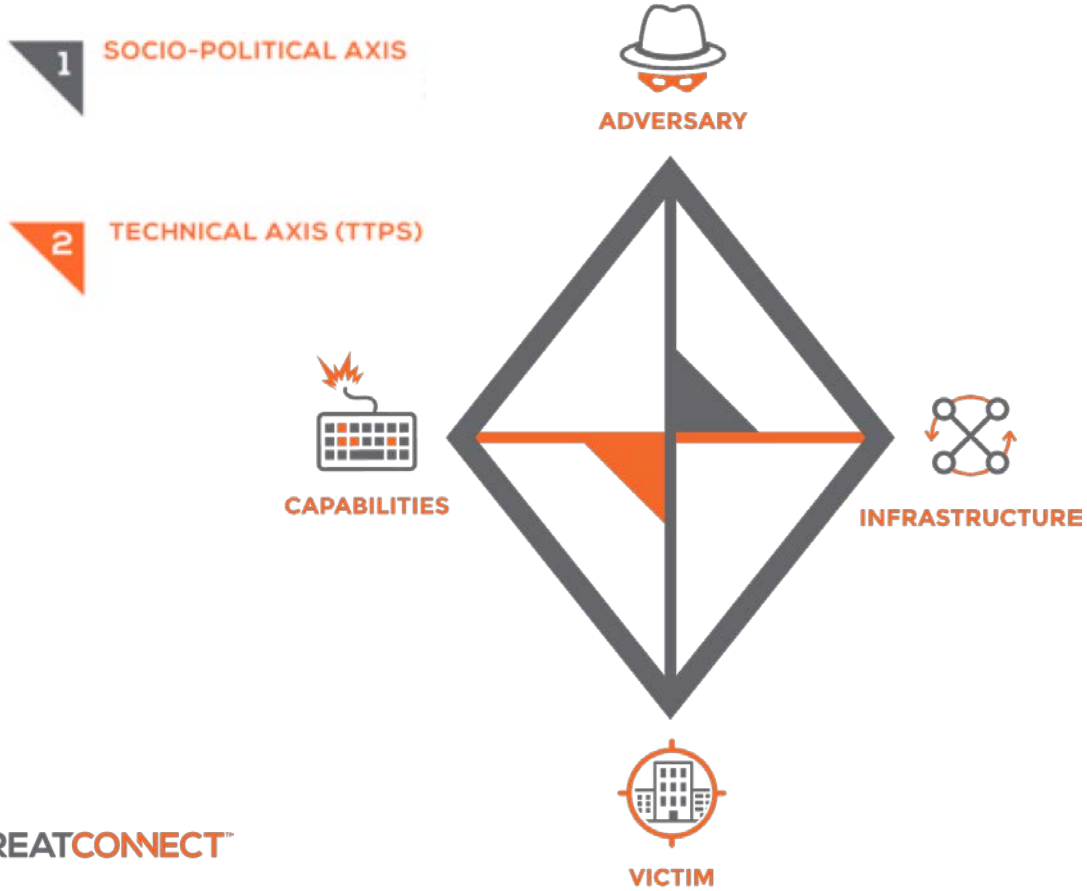
FORRESTER®

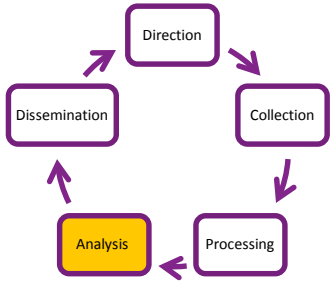
Classic intelligence cycle



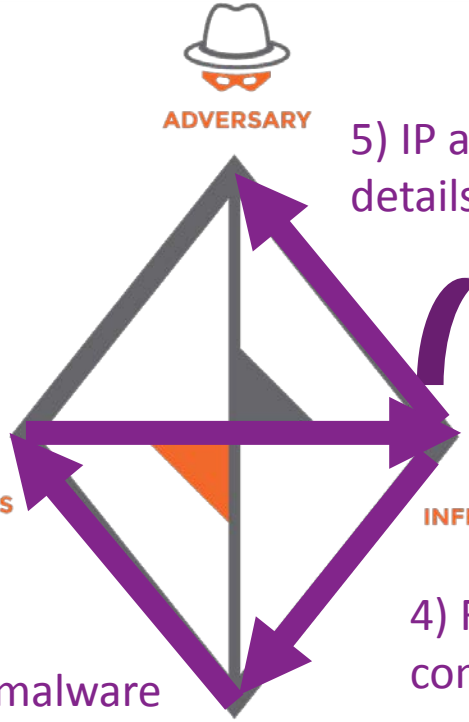
Threat intelligence process

The Diamond Model of Intrusion Analysis





Threat intelligence process



5) IP address ownership details reveal adversary

2) Malware contains C2 domain

3) C2 domain resolves to IP address

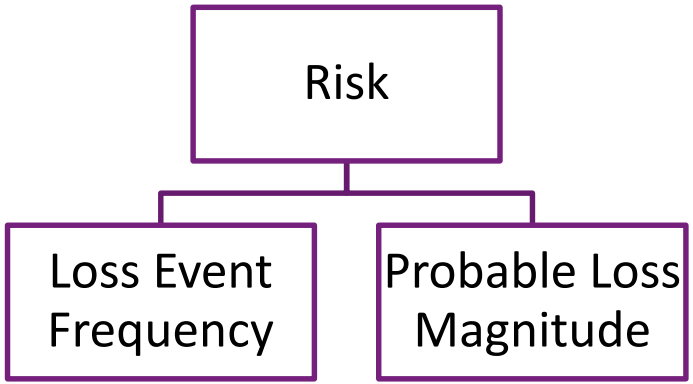
4) Firewall logs reveal more comms to C2 IP

1) Victim discovers malware

What is risk?

"The probable frequency and probable magnitude of future loss"

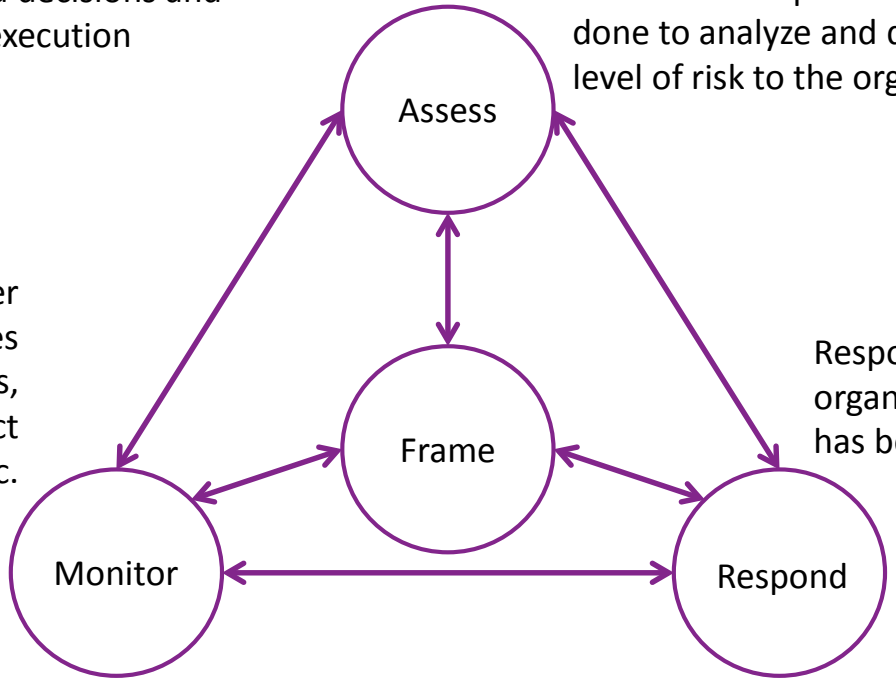
- Factor Analysis of Information Risk (FAIR)



Risk management process (NIST 800-39)

Frame: establishes the context for risk-based decisions and strategy for execution

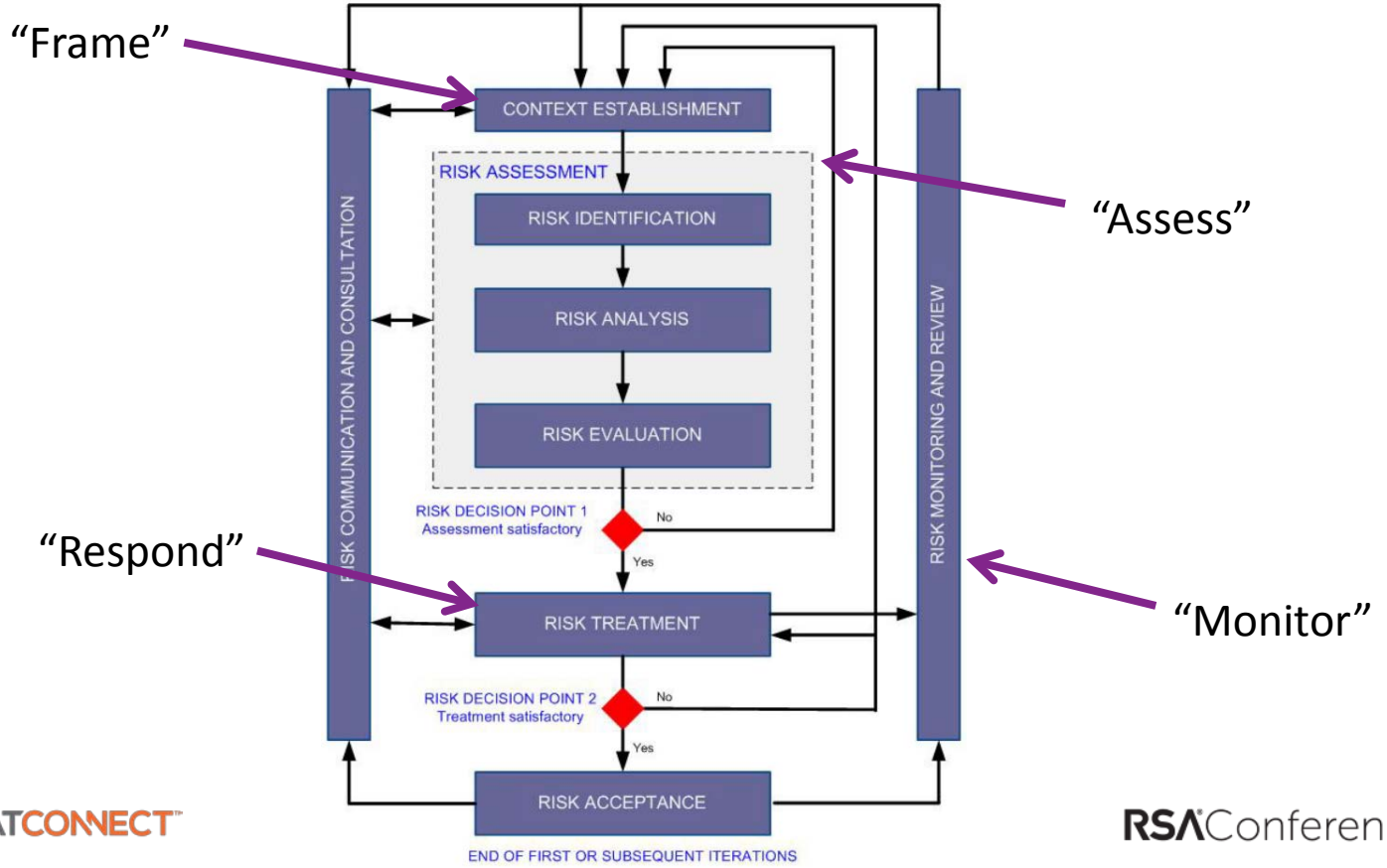
Assess: encompasses everything done to analyze and determine the level of risk to the organization.



Monitor: verifies proper implementation, measures ongoing effectiveness, tracks changes that impact effectiveness or risk, etc.

Respond: addresses what organizations choose to do once risk has been assessed and determined

Risk management process (ISO 27005)



Love:

There’s something special here

Risky questions needing intelligent answers

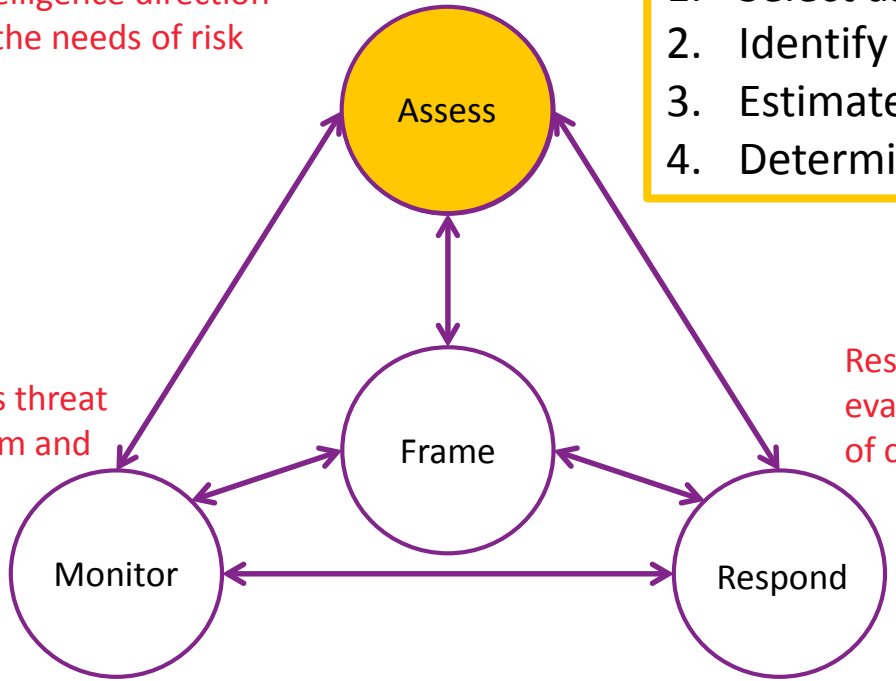
- What types of threats exist?
- Which threats have occurred?
- How often do they occur?
- How is this changing over time?
- What threats affect my peers?
- Which threats could affect us?
- Are we already a victim?
- Who's behind these attacks?
- Would/could they attack us?
- Why would they attack us?
- Are we a target of choice?
- How would they attack us?

- Could we detect those attacks?
- Are we vulnerable to those attacks?
- Do our controls mitigate that vulnerability?
- Are we sure controls are properly configured?
- What happens if controls do fail?
- Would we know if controls failed?
- How would those failures impact the business?
- Are we prepared to mitigate those impacts?
- What's the best course of action?
- Were these actions effective?
- Will these actions remain effective?

Intel in the risk management process

Frame: adjust intelligence direction and ops to meet the needs of risk management

1. Select asset(s) at risk
2. Identify risk scenarios
3. Estimate risk factors
4. Determine risk level

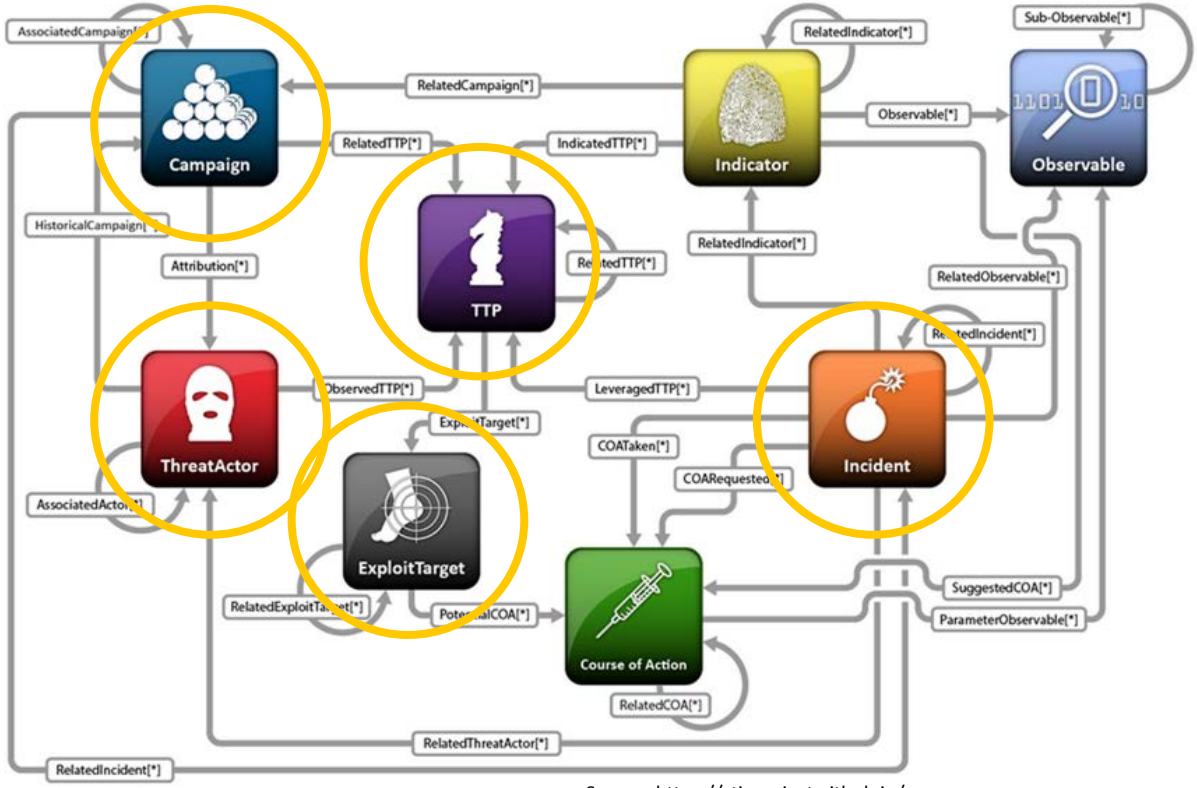


Monitor: intelligence tracks threat changes that warrant system and control changes

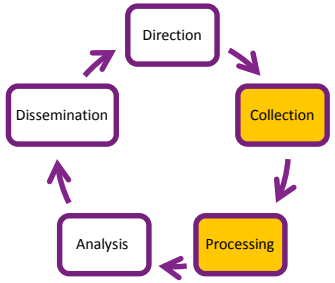
Respond: intelligence supports evaluation and implementation of courses of action

Building a model relationship

Structured Threat Information eXpression (STIX)

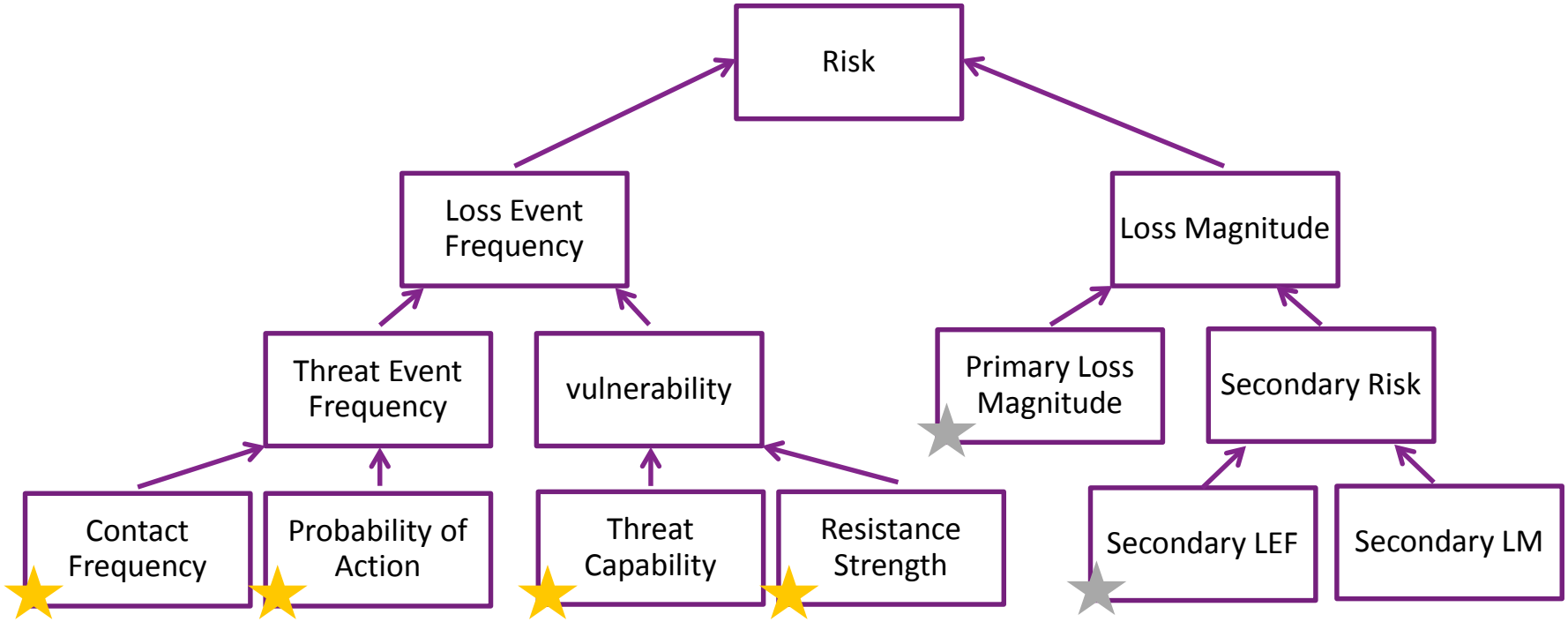


Source: https://stixproject.github.io/



Building a model relationship

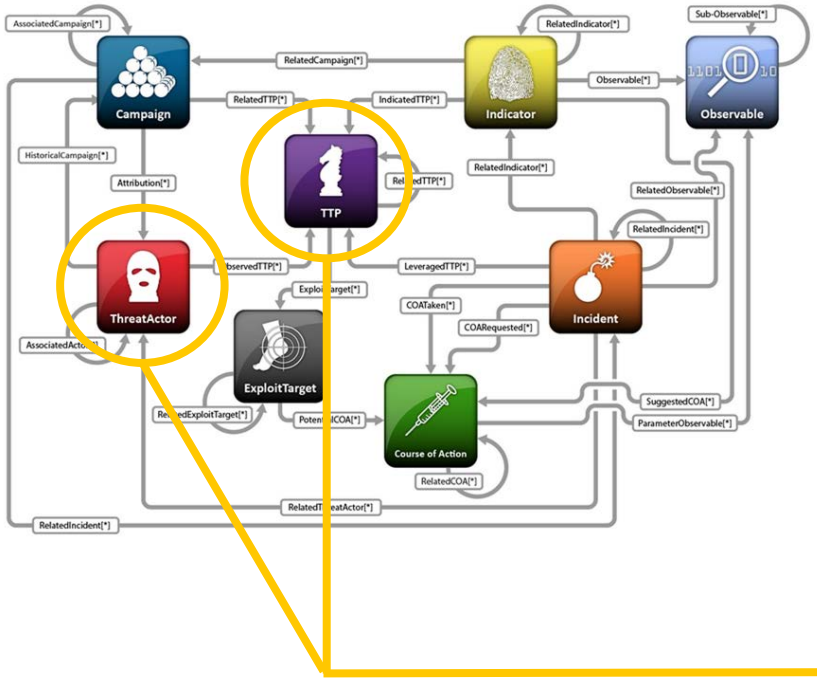
Factor Analysis of Information Risk (FAIR)



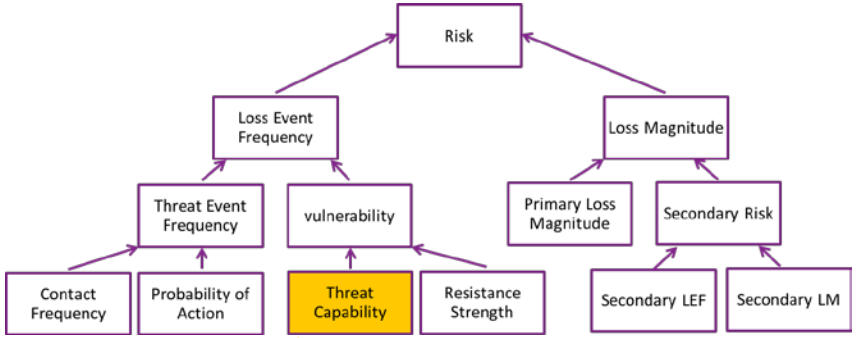
Building a model relationship

Finding mutual interests and activities

Threat Intel (STIX)



Risk Analysis (FAIR)



- *Type*
- *Behavior*
- *Sophistication*
- *Resources*
- *Kill_Chain_Phases*
- *Intended_Effect*
- *Exploit_Targets*
- *Observed_TTPs*

*Initial map: https://threatconnect.com/threat-intelligence-driven-risk-analysis/

And they lived happily ever after!

Marriage:

How does this actually work?

Example risk assessment project

"During a recent audit, it was discovered that there were active accounts in a customer service application with inappropriate access privileges. These accounts were for employees who still worked in the organization, but whose job responsibilities no longer required access to this information. Internal audit labeled this a high risk finding."

From: *Measuring and Managing Information Risk*
by Jack Freund and Jack Jones (p 123)

Example risk assessment project

FAIR analysis process flow

From: “Measuring and Managing Information Risk” by Jack Freund and Jack Jones (p 93)

Example risk assessment project

Scenarios associated with inappropriate access privileges

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality

FAIR estimations relevant to the cyber criminal scenario

TEF Min	TEF M/L	TEF Max	TCap Min	TCap M/L	TCap Max
0.5 / year	2 / year	12 / year	70	85	95

From: "Measuring and Managing Information Risk" by Jack Freund and Jack Jones (p 127)

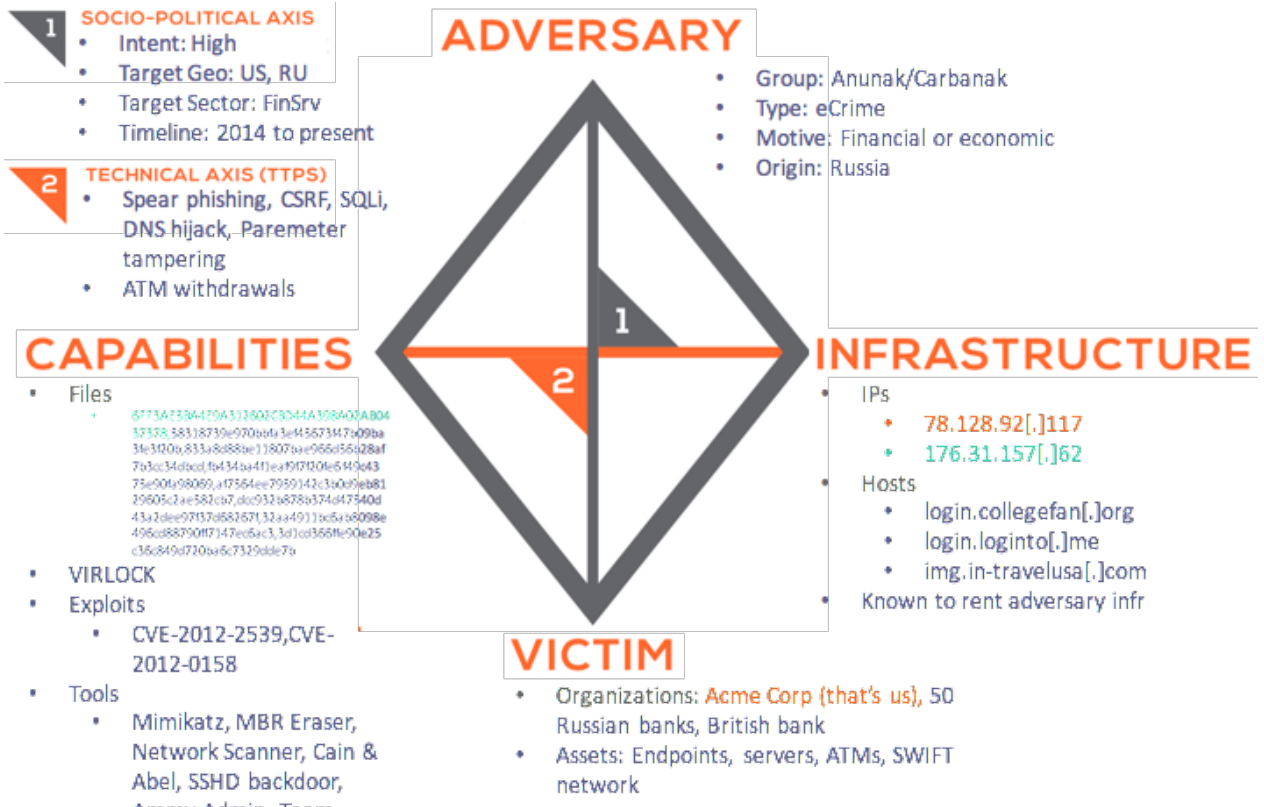
Example risk assessment project

Standard cyber criminal threat profile

Factor	Description
Motive	Financial, Intermediary
Primary intent	Engage in activities legal or illegal to maximize their profit.
Sponsorship	Non-state sponsored or recognized organizations (illegal organizations or gangs).
Targets	Financial services and retail organizations
Capability	Professional hackers. Well-funded, trained, and skilled.
Risk Tolerance	Relatively high; however, willing to abandon efforts that might expose them. Prefer to keep their identities hidden.
Methods	Malware, stealth attacks, and Botnet networks.

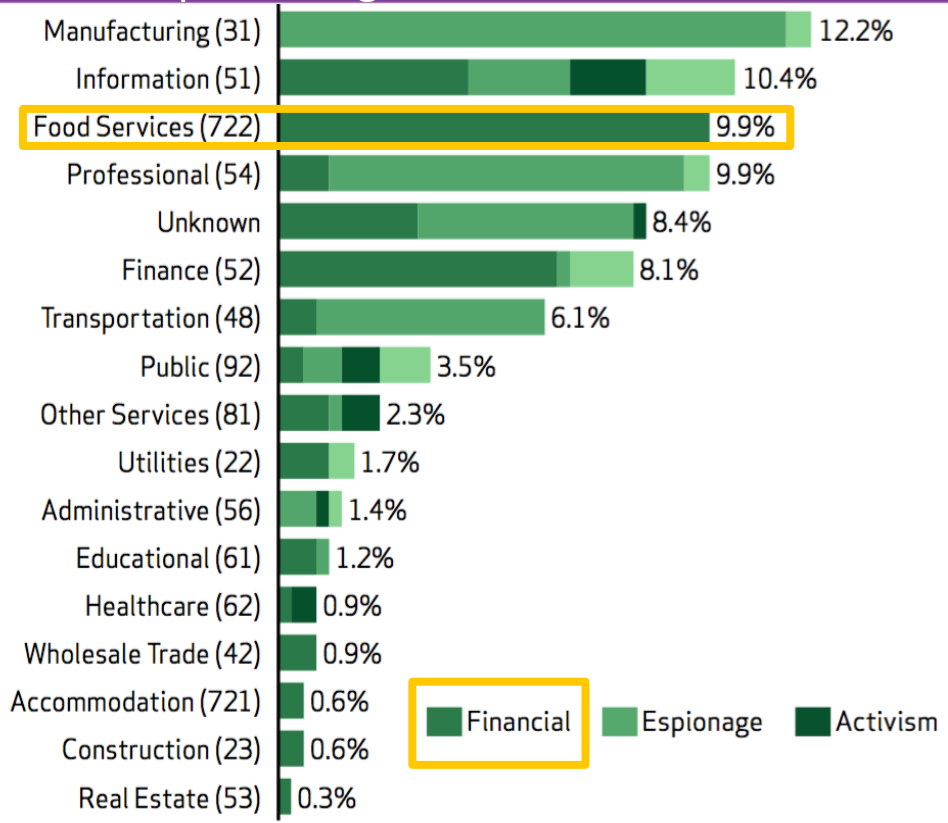
Example risk assessment project

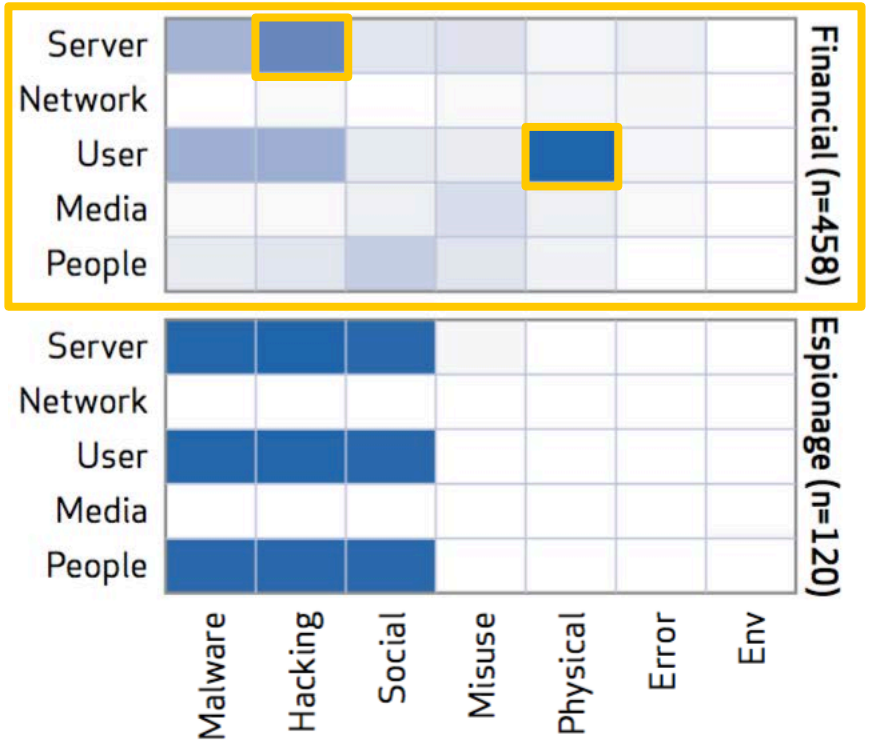
Example intelligence-driven adversary profile



Example risk assessment project

Example intelligence-driven threat community profile...OVER TIME





Making it work in your organization

1. Initiate communication between intel & risk teams
2. Orient intel processes & products around desired risk factors
3. Identify threat communities of interest and create profiles
4. Establish guidelines & procedures for risk assessment projects
5. Encourage ongoing coordination & collaboration
   - Create centralized tools/repositories

~~Underlying assumption~~
Motivating conviction

Good **intelligence** makes smarter **models**;
Smarter models inform **decisions**;
Informed decisions drive better **practice**;
Better practice improves risk **posture**;
which, done efficiently,
Makes a successful security **program**.

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

The Marriage of Threat Intelligence and Risk Assessment

THANK YOU!!

Wade Baker

VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker

#RSAC