RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: HUM-F03

The Art of Thinking Security Clearly

Augusto Barros

www.securitybalance.com
@apbarros

Cognitive bias

"A cognitive bias is a pattern of deviation in judgment, whereby inferences about other people and situations may be drawn in an illogical fashion"

Confirmation Bias

We tend to only accept information that aligns with our previous beliefs.

Best way to validate an hypothesis is trying to prove it wrong, not looking only for data that confirms it.

The “2-4-6” rule and the exercise to identify it.

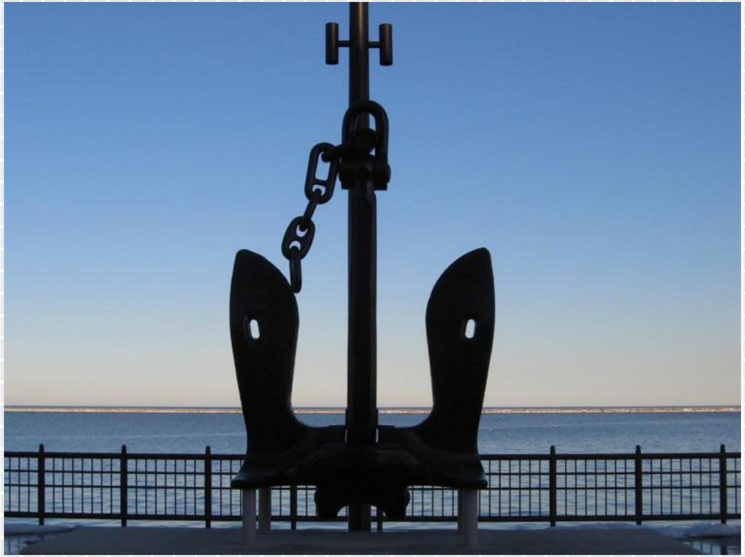
Confirmation Bias (2)

Given the following sequence:

2 4 6 ?

Provide a guess for the next number; I’ll tell you if it fits or if it doesn’t fit the rule. After that, you can guess what’s the rule being used for the sequence

Anchoring



- Numbers we absorb through multiple ways affect our estimates for quantities.
- Any number that you are asked to consider as a solution to an estimation problem will induce an anchoring effect.
- This is a special case of a 'priming‘ effect.

Do you think Gandhi was more than 114 years old when he died?

or...

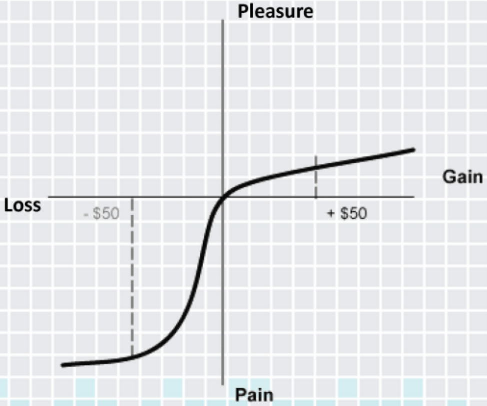
Do you think Gandhi was more than 35 years old when he died?

How old was Gandhi when he died?

Behavioral Economics

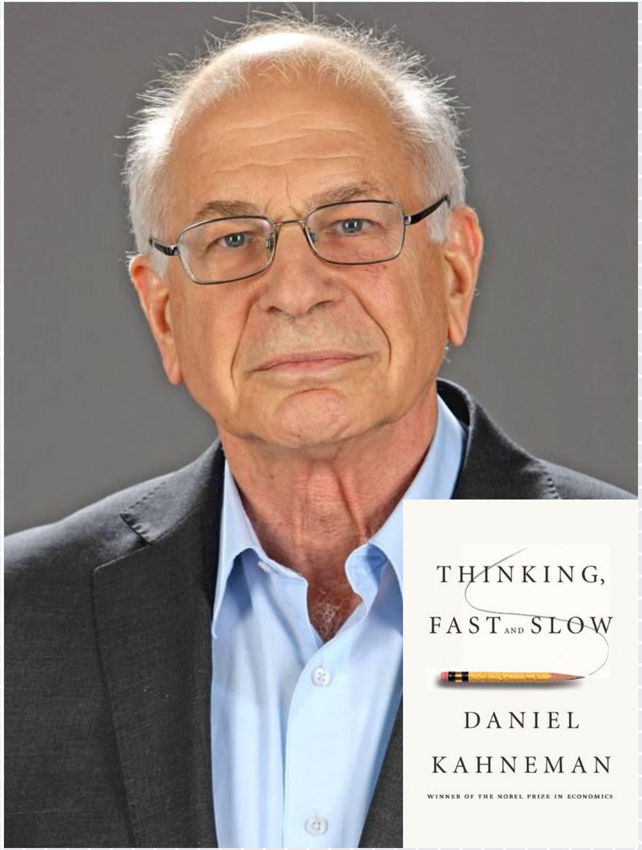
"The psychology underlying economic decision making"

Influence of psychologists on economics, showing that 'Econs' and 'Humans' are different animals



1978: Kahneman and Tversky publish Prospect Theory, where Utility theory is revised to include normal human behavior (no 'Econ'), including loss aversion and the asymmetry between loss/gain expectations.

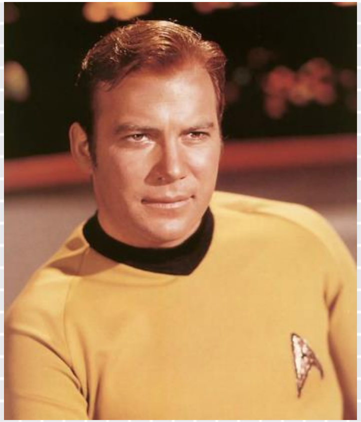
Kahneman got his Nobel for that work.



Behavioral Economics

- Many experiments and actual science documenting non-rational behavior.
- Current theory explains that by referring to two thinking processes that coexist in our minds (Keith Stanovich and Richard West):

System 1 operates automatically and quickly, with little or no effort and no sense of voluntary control



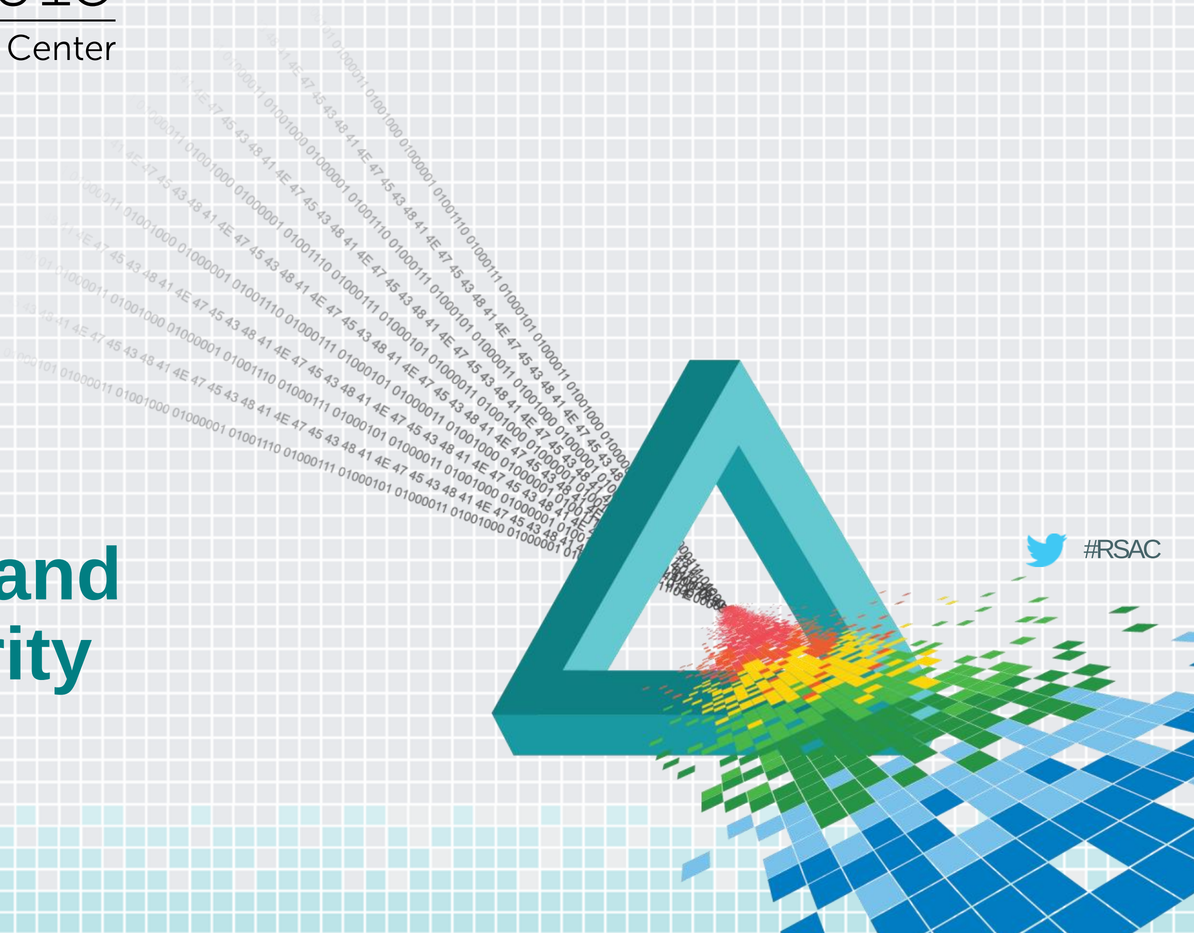
System 2 allocates attention to the effortful mental activities that demand it, including complex computations.

The operations of System 2 are often associated with the subjective experience of agency, choice, and concentration.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

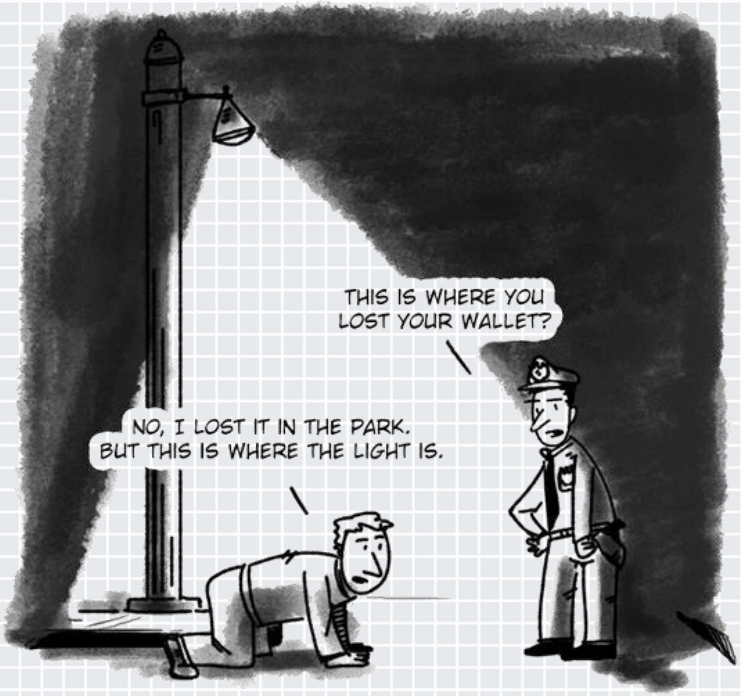
Cognitive Biases and Information Security



#RSAC

Confirmation Bias

- Vulnerability assessments and penetration testing
  - "streetlight effect"
- Attack attribution


THIS IS WHERE YOU LOST YOUR WALLET?
NO, I LOST IT IN THE PARK. BUT THIS IS WHERE THE LIGHT IS.

Anchoring

- Risk assessments
  - Impact estimates
  - Cost of breach studies (Ponemon)

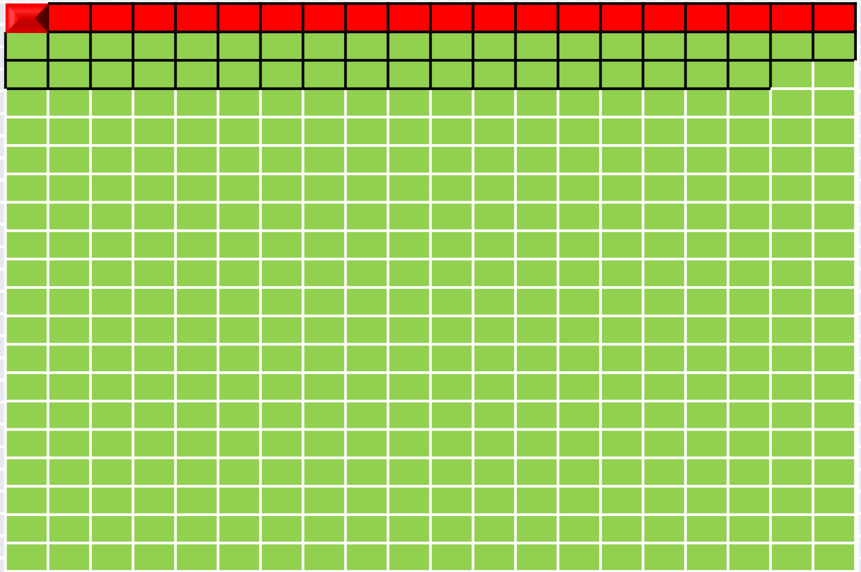
Herd Thinking

- Attribution (again ☺)
- This week’s security technology
- “Calibration sessions” for risk assessments

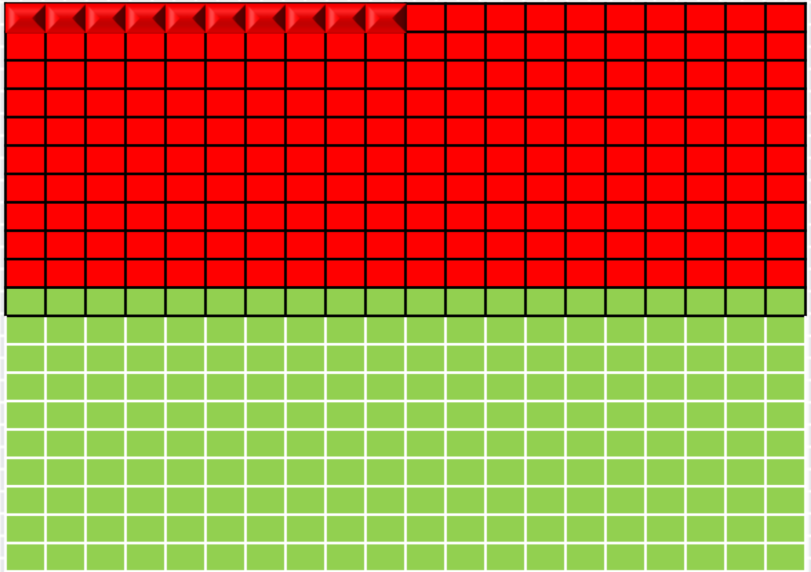
Base Rate Neglect

- Detection rates
  - False positive rate vs. Base rate
- 95% detection, 10% false positives
  - Is it good? Is it bad?
  - Key is to know (or estimate) the prevalence

Base Rate Neglect (2)



57 events detected
38 false positives



210 events detected
20 false positives

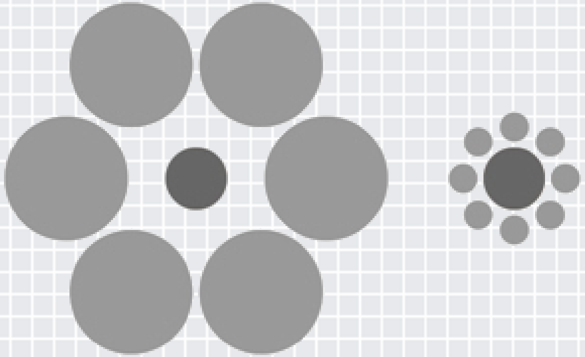
Overconfidence Effect

- In a survey, 93% of the U.S. students asked estimated themselves to be ‘above average’ drivers.
- Estimates of the efficiency of security measures and controls are often subject to the overconfidence effect.
  - *‘Unbreakable’* software ☺

Framing

- How information is presented matters – a lot
- Kahneman & Tversky experiment:

In a small town with 600 people, which epidemy control option is better?



Option A saves 200 people

Option A’: 400 people die

Option B, 33% chance that all 600 people will survive, and a 66% chance that no one will survive

Option B’, 33% chance that no one will die, and a 66% chance that everyone die

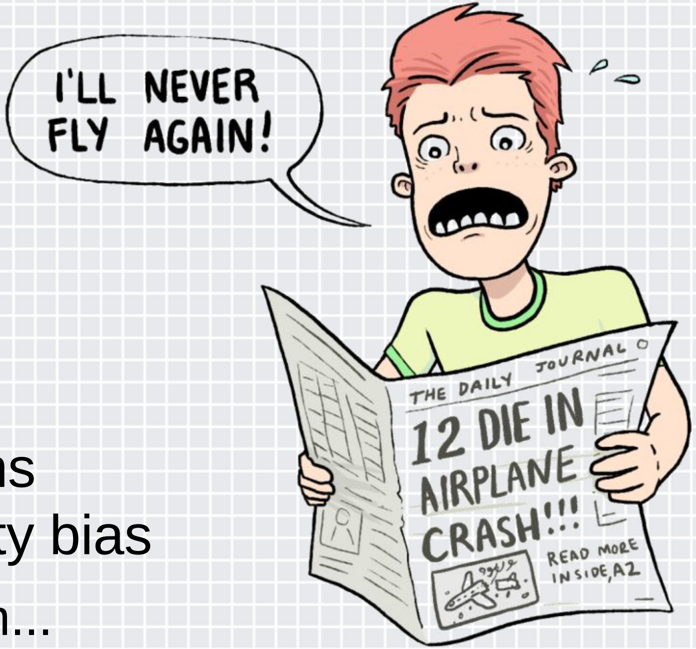
- Keep this in mind when trying to justify security investments

Ambiguity Aversion

- Ellsberg Paradox
- People generally prefer known risks over unknown risks
  - Unknown risks are not necessarily higher!

Availability Bias

- The giving of preference by decision makers to information and events that are more recent, that were observed personally, and were more memorable.
- Risk assessment and security decisions are directly influenced by the Availability bias
  - Breaches: Target, Home Depot, Anthem...



Social Engineering and Cognitive Biases

- Cognitive biases are extensively exploited in social engineering, phishing attacks
  - Authority bias
  - Reciprocity bias
  - Social proof
  - ...
- The copy machine experiment

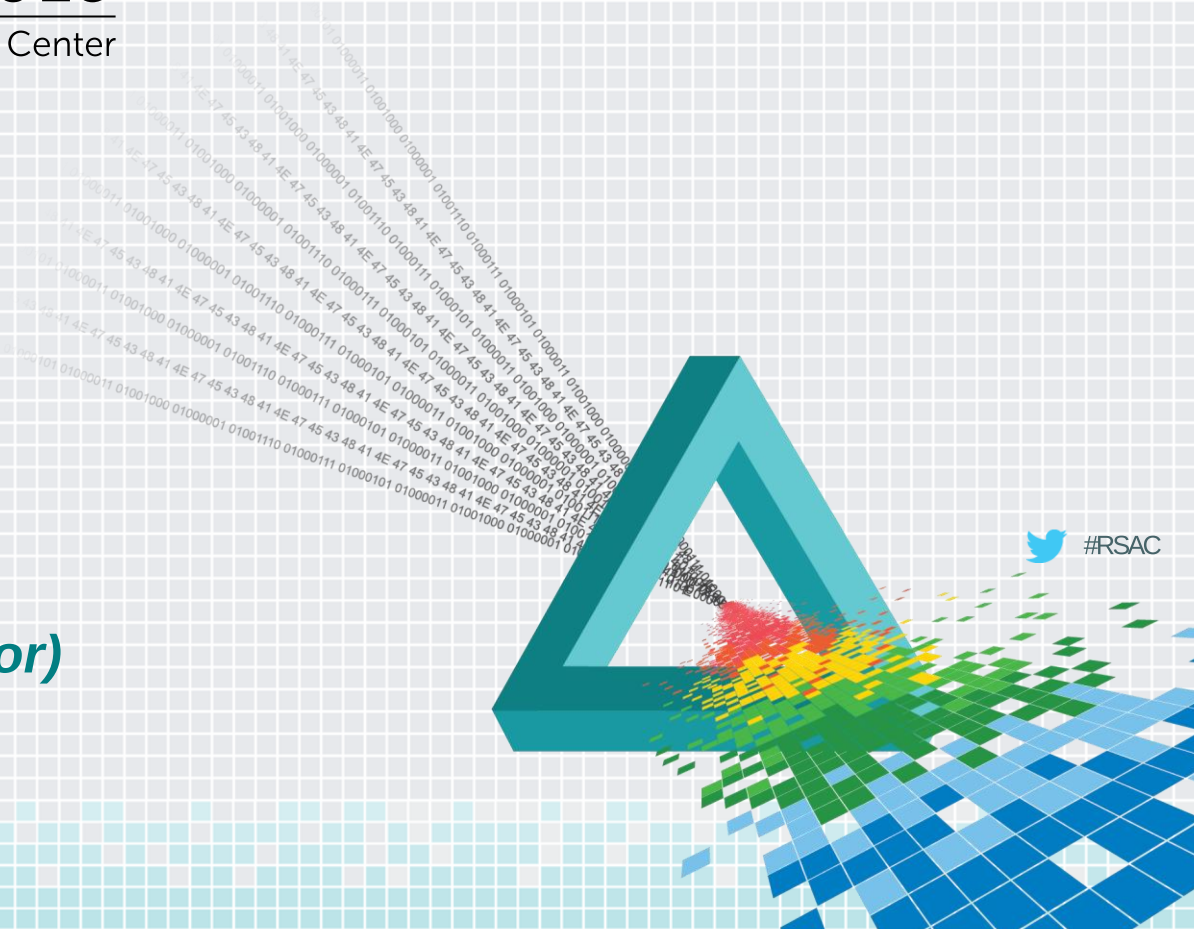
The Attacker and Cognitive Biases

- Attackers are (mostly) human
  - Also subject to biases
- Scarcity Error
- Halo Effect
- Neglect of probability

And of course...the availability bias.

Other Biases

Confirmation Bias	Planning fallacy	Clustering illusion
Anchoring Bias	Halo effect	Insensitivity to sample size
Availability Bias	Ingroup Bias	Illusion of validity
Survival Bias	Hyperbolic discounting	Scope Neglect
Framing effect	Illusion of control	Neglect of probability
Base rate neglect	Herd thinking	Gambler’s fallacy
Alternative Blindness	Ambiguity Aversion	Sunk cost effect
Hindsight Bias	Story Bias	Overconfidence effect



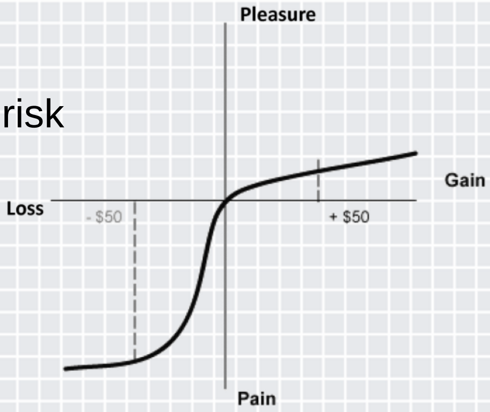
#RSAC

Fighting Biases

(or using them in our favor)

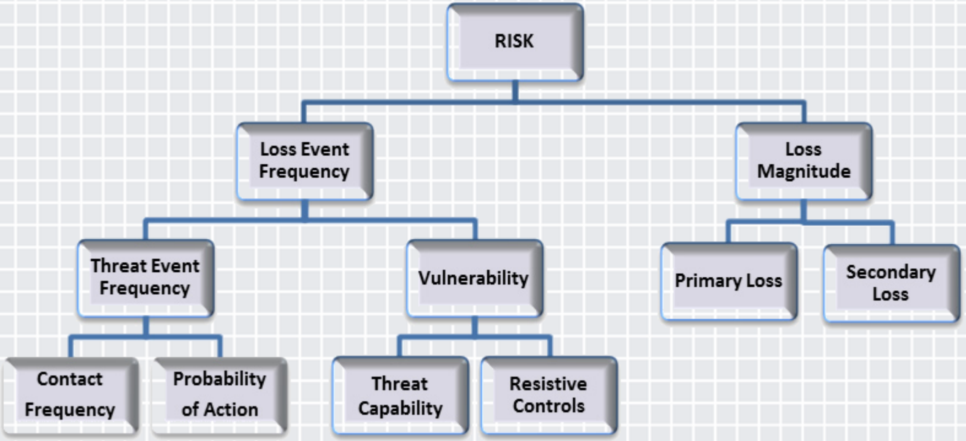
Risk Management

- Risk Assessment is an estimation exercise – perfect “target” for cognitive biases
    - Prospect Theory
    - Determining the likelihood of events
        - Availability Bias
        - Halo effect, affect heuristic: how do I feel about it vs. actual risk
        - Gambler’s fallacy (incorrect understanding of ‘regression to the mean’)
- Risk treatment strategy, control selection
    - Alternative blindness
    - Herd effect
    - Availability...



Risk Management(2)

- How to fix it?
  - Formulas
    - Simple formulas are very efficient. FAIR!
    - Formulas vs expert opinion
      - Humans are inconsistent on their opinions.
      - System 1 is too context sensitive and affects judgment.
    - Formulas are better in low validity environments.
    - Don’t use 'expert opinion' to adjust results of formula
      - Use it to estimate the factors and let model generate the result.



Risk Management(3)

What else?

  - Peering assessors based on opposite biases and averaging estimates
  - Outside view: data from other environments (Verizon DBIR)
  - Team A / B approach to assessments
  - Moving from single to joint estimates (narrow to broad scope of comparison)

- Security decision making and control selection:
  - Utilize Decision Theory techniques to minimize alternative blindness, confirmation bias.
  - When planning, use external data to mitigate planning fallacy
  - Overconfidence: ‘devil’s advocate’ exercises. Explaining failure from the future
  - Consider framing for security investments business cases

Security Awareness and Training

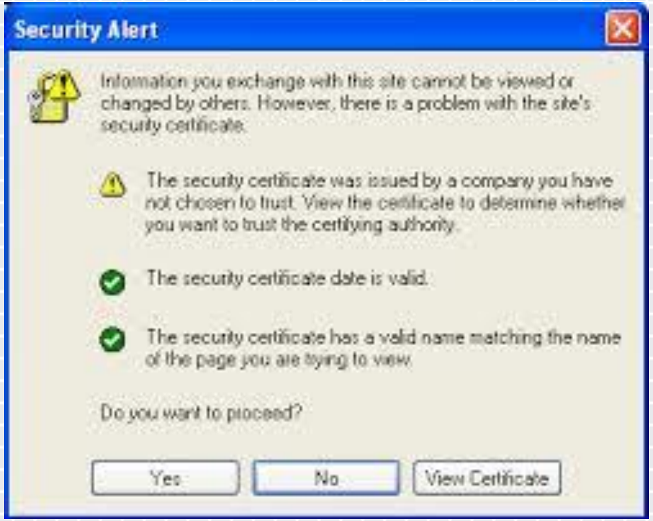
- Biases can and should be used for good too!
  - Leverage behavior science to build security training that changes/enforces behavior
    - Knowing what is right vs. Doing what is right
    - Two options:
      - Prepare System 1 to make the right decision
      - Force System 2 to engage
        - Small print and hard to read fonts may help – but this can backfire

Security Awareness and Training (2)

- Priming
  - Short security messages in the right moment
- Explore framing for the message to be delivered
  - A/B testing with feedback tests
    - phishing exercises
- Use the Story Bias

User Interfaces

- The power of defaults
- Consider “nudges”: small interventions to make people do what you want them to do
- Choice Architecture
  - Behavioral sciences applied to building choice scenarios



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

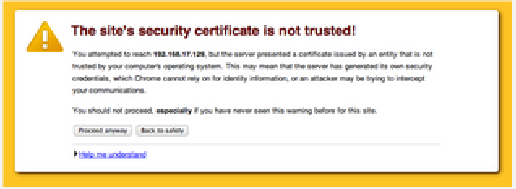
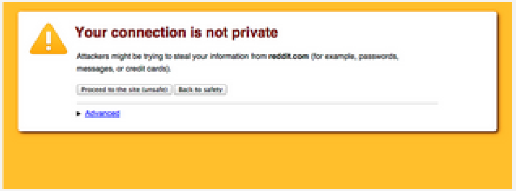
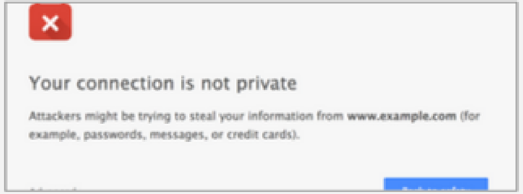
✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

User Interfaces (2)

- "Improving SSL Warnings" – Adrienne Porter Felt (Chrome security team)

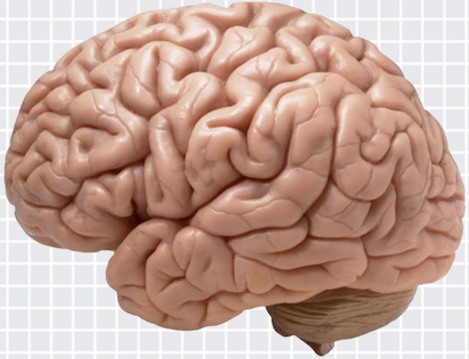
	ADHERENCE	N
 **The site's security certificate is not trusted!** You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site. Proceed anyway | Back to safety Help me understand	30.9%	4,551
 **Your connection is not private** Attackers might be trying to steal your information from **reddit.com** (for example, passwords, messages, or credit cards). Proceed to the site (unsafe) | Back to safety Advanced	32.1%	4,075
 Your connection is not private Attackers might be trying to steal your information from **www.example.com** (for example, passwords, messages, or credit cards).	**58.3%**	4,644

Security Solutions and Products

- Defaults are very important
  - Make it secure from the start, it will most likely stay that way
- Don’t forget base-rate neglect when building detective/preventive technologies
  - Even a very low false positive rate is useless when prevalence is too low
  - Adding log sources to SIEM and base rate expansion
- “Threat Intelligence” – Be careful to not automate the availability bias

Summary

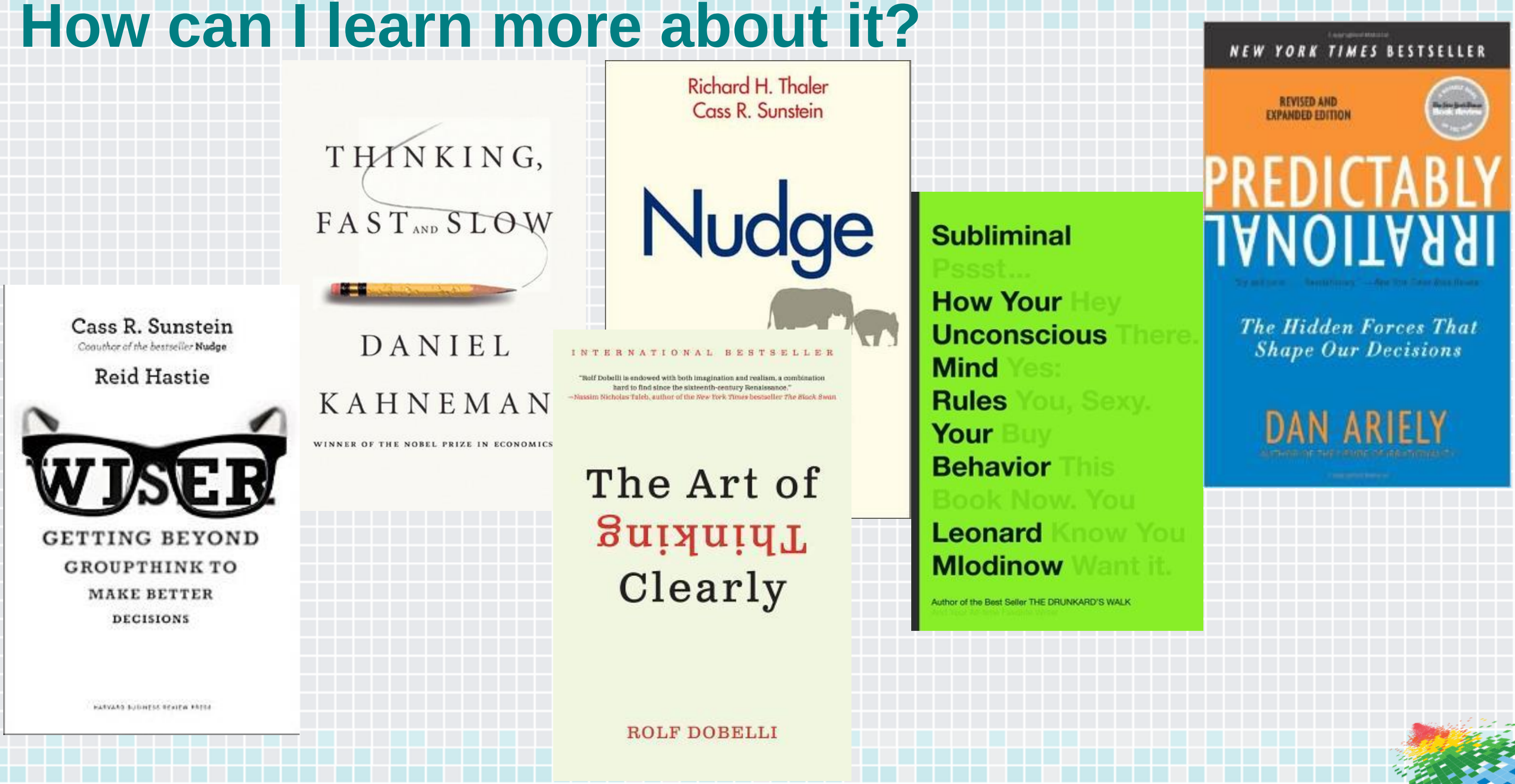
- Information Security is also affected by behavior economics
- People are not always rational
  - But they are “predictably irrational”: cognitive biases
- Understanding the effect of cognitive biases can help against social engineering, improve security training, risk assessments and user interfaces



Apply Slide

- Next week you should:
  - Leverage behavior economics concepts to get better results in discussions about risk
- In the first three months following this presentation you should:
  - Review your security awareness program to consider behavior economics concepts
- Within six months you should:
  - Incorporate behavior economics in security decision making and user interfaces development

How can I learn more about it?


Cass R. Sunstein
Coauthor of the bestseller Nudge
Reid Hastie
WISER
GETTING BEYOND GROUPTHINK TO MAKE BETTER DECISIONS
HARVARD BUSINESS REVIEW PRESS
THINKING, FAST AND SLOW
DANIEL KAHNEMAN
WINNER OF THE NOBEL PRIZE IN ECONOMICS
Richard H. Thaler
Cass R. Sunstein
Nudge
INTERNATIONAL BESTSELLER
"Rolf Dobelli is endowed with both imagination and realism, a combination hard to find since the sixteenth-century Renaissance." —Nassim Nicholas Taleb, author of the New York Times bestseller The Black Swan
The Art of Thinking Clearly
ROLF DOBELLI
Subliminal
Pssst...
How Your Hey
Unconscious There.
Mind Yes:
Rules You, Sexy.
Your Buy
Behavior This
Book Now. You
Leonard Know You
Mlodinow Want it.
Author of the Best Seller THE DRUNKARD'S WALK
NEW YORK TIMES BESTSELLER
REVISED AND EXPANDED EDITION
PREDICTABLY IRRATIONAL
The Hidden Forces That Shape Our Decisions
DAN ARIELY

Thank You

- blog.securitybalance.com
- Twitter: @apbarros
- augusto@securitybalance.com