GOOD PEOPLE, BAD DECISIONS: AN INTERPLAY OF ECONOMICS, PSYCHOLOGY AND RISK

Dmitry Zhdanov. NIST NICE Workshop 2013

Causes of (in)security in decisions

- Cognitive limitations
- Rewards and outcomes
- It's all about risk
- Garbage in, garbage out

- What to do?

It's all in your head

Let's look at the individuals first

Houston, we have a problem

- Users do not think they are at risk
- Users aren't stupid, they are unmotivated
- Safety is an abstract concept
- Feedback and learning from security-related decisions is weak

R. West "The Psychology of Security", 2008 (CACM)

Houston, we have a problem

- Making trade-offs between risk, losses, gains and costs
- Users are more likely to gamble on a loss than accept a guaranteed loss
- Losses are perceived disproportionally to gains
- Security is a secondary task

R. West "The Psychology of Security", 2008 (CACM)

Users do not think they are at risk

- People tend to believe that they are less vulnerable than others. This includes a wide range of scenarios from consumer products to health to computer security
  - Thus, why patch/firewall/antivirus…? Nothing bad can happen

Users aren't stupid, they are unmotivated

- Cognitive miser = limited capacity for information processing
  - Thus, multitask and rely on heuristics..
    - … which bring good outcomes MOST of the time
    - What do you do when a warning pop-up shows on the screen?

Safety is an abstract concept

- Concrete outcomes dominate abstract
  - Yet, “secure” choice frequently has no visible outcome or visible threat
  - Thus, click that link!

    - Also, fall back on the heuristics

Feedback and learning

- Typical learning: do something right, get a reward. Do something wrong, get a penalty
- Security: do something right, and nothing bad happens
- Security: do something wrong, and the negative impact is not immediate or direct
  - Thus, learning of consequences is difficult

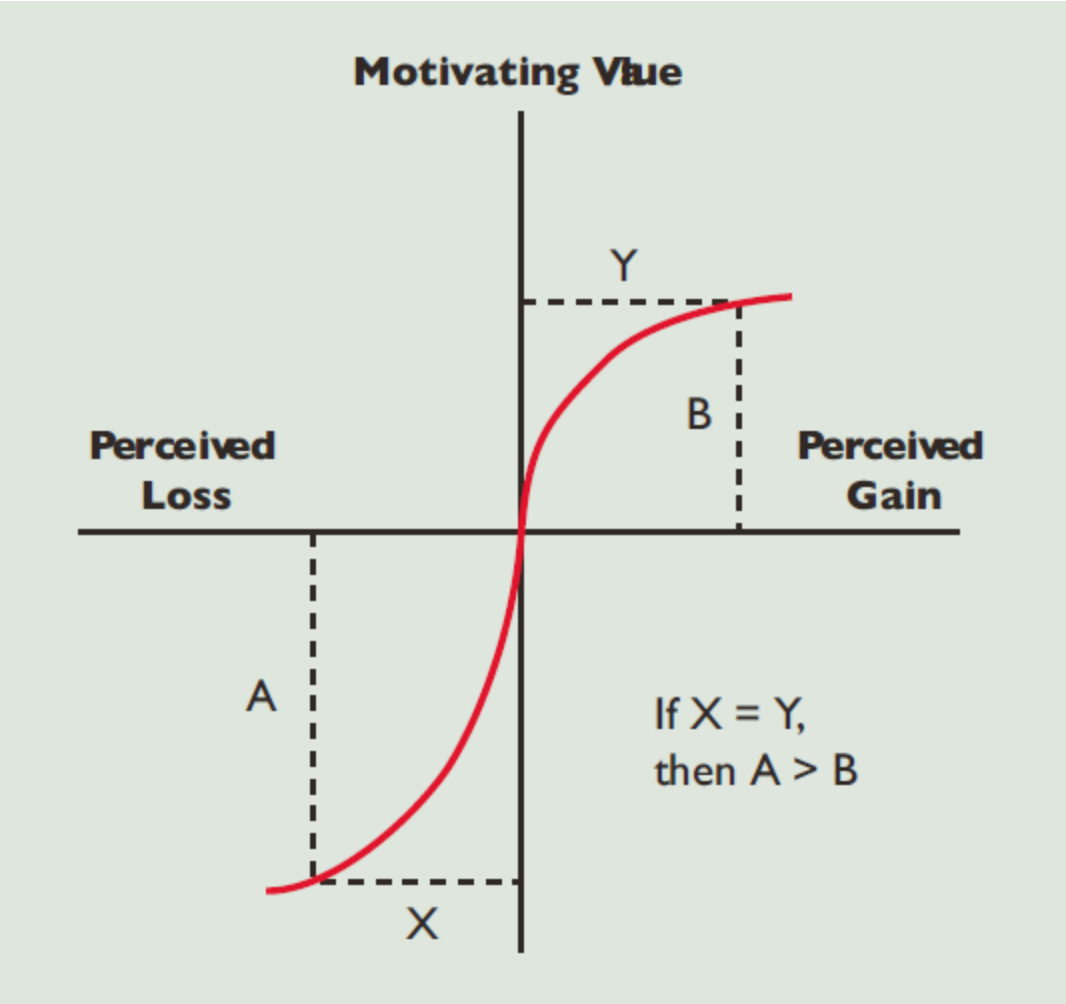
Gain\loss tradeoffs

- Scenario 1: guaranteed GAIN of $5 versus a coin toss with the outcomes $0, $10

Gain\loss tradeoffs

- Scenario 2: guaranteed LOSS of $5 versus a coin toss with the outcomes $0, -$10

Gain\loss tradeoffs



R. West "The Psychology of Security", 2008 (CACM)

Other factors of gains\losses

- Scale – people do not conceptualize very large or very small magnitudes well
- Probability – generally hard to estimate, but the magnitude is also a problem (particularly small one)

Look out!

- Average number of deaths in a year caused by…

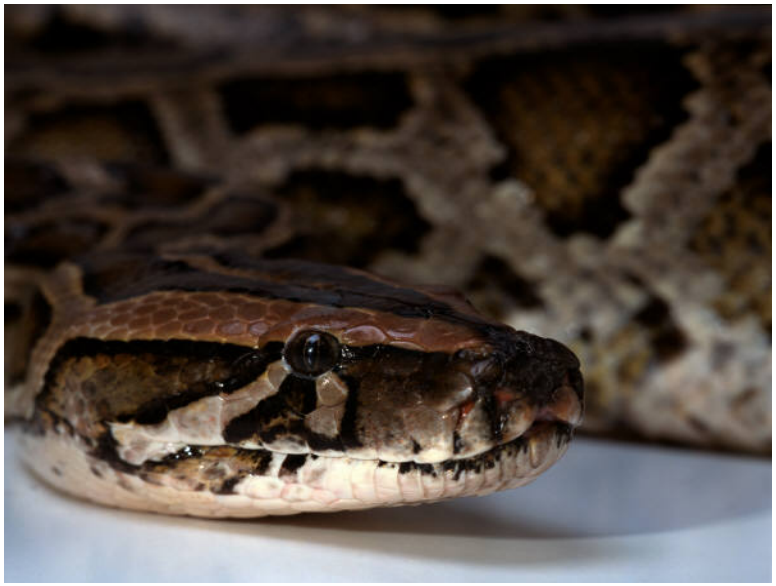
Look out!

- Average number of deaths in a year caused by…

<1

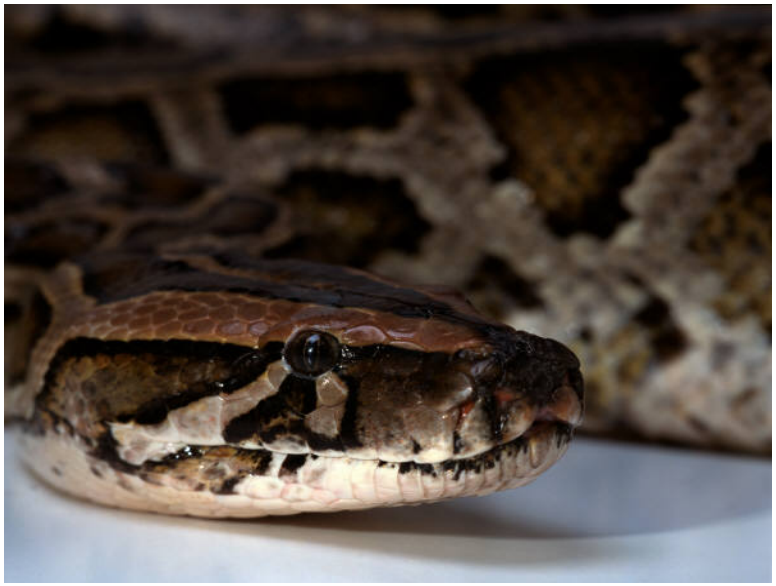
Look out!

- Average number of deaths in a year caused by…



Look out!

- Average number of deaths in a year caused by…



5.5

Look out!

- Average number of deaths in a year caused by…

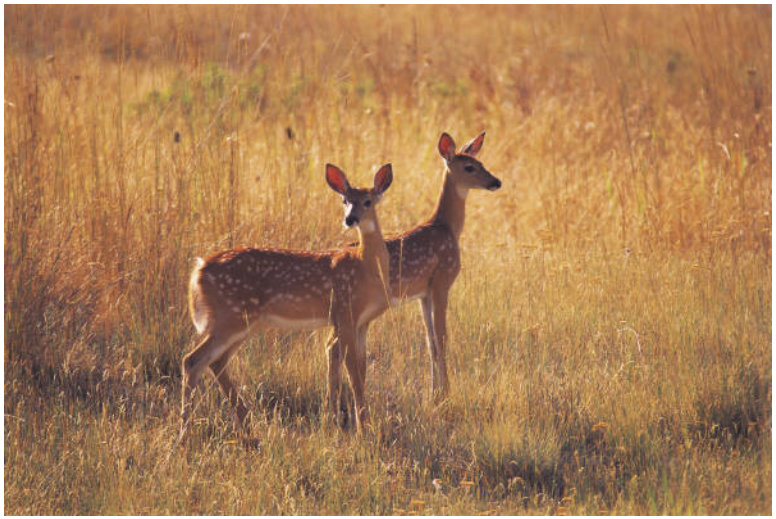
Look out!

- Average number of deaths in a year caused by…

53

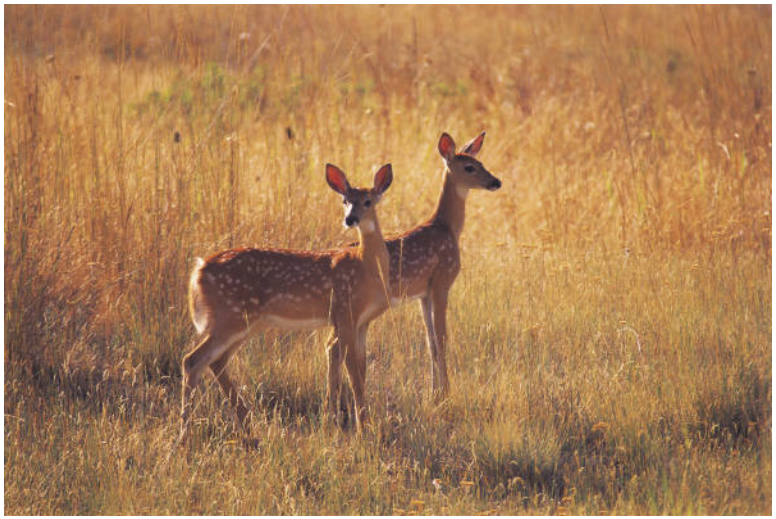
Look out!

- Average number of deaths in a year caused by…



Look out!

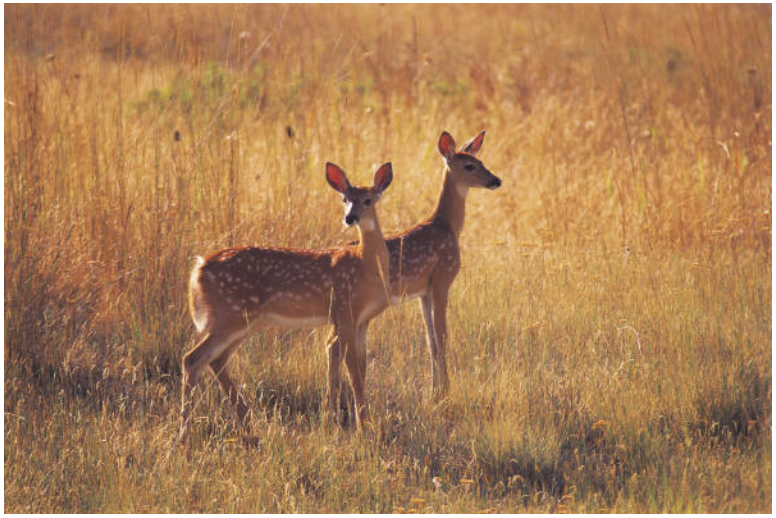
- Average number of deaths in a year caused by…



130

Data from http://historylist.wordpress.com/2008/05/29/human-deaths-in-the-us-caused-by-animals/

Yet, who are we afraid of?



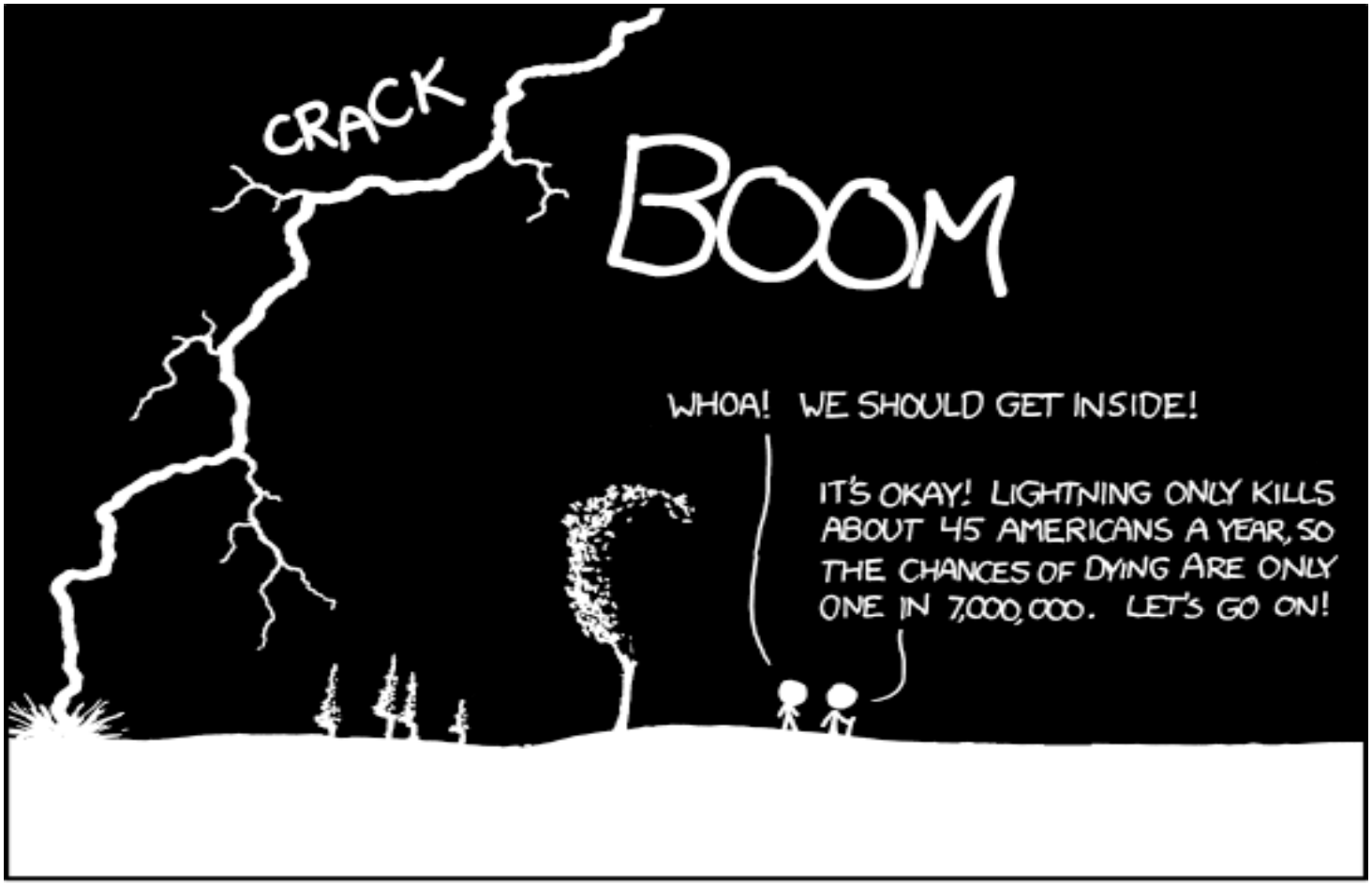
Security is a secondary task

- When under time pressure, people tend to focus more on the losses affecting their immediate task
  - Thus, take shortcuts, ignore policies, etc.

Losses perceived disproportionally

- When users perceive a gain and a loss to have the same value, loss is actually more motivating
  - Thus, even if the cost of security effort is “small”, it may seem worse for the users

Conditional probability



Xkcd.org

Got brakes?

- Munich Taxi study (early 1980s)
- Used ABS brakes on 50% of cabs
- Accelerometers installed unknown to drivers

- Results:
  - No significant difference in accident rates
  - Cabs with ABS were driven more aggressively (acceleration, harsh stops)
- http://www.drivers.com/article/411

A driving lesson

- British study: accidents by type of training
  A. Driving school only
  B. With friends or relatives only
  C. Combined training

- Atlanta, DeKalb County, Georgia - similar variation by the number of training hours (Safe Performance Curriculum, basic training, no formal training)

A driving lesson

- British study: results (km driven per accident)
  A. 19,392
  B. 22,801
  C. 14,536

- Atlanta, DeKalb County, Georgia
  - No significant difference in crashes for minimal training or no formal training
  - MORE accidents for SPC

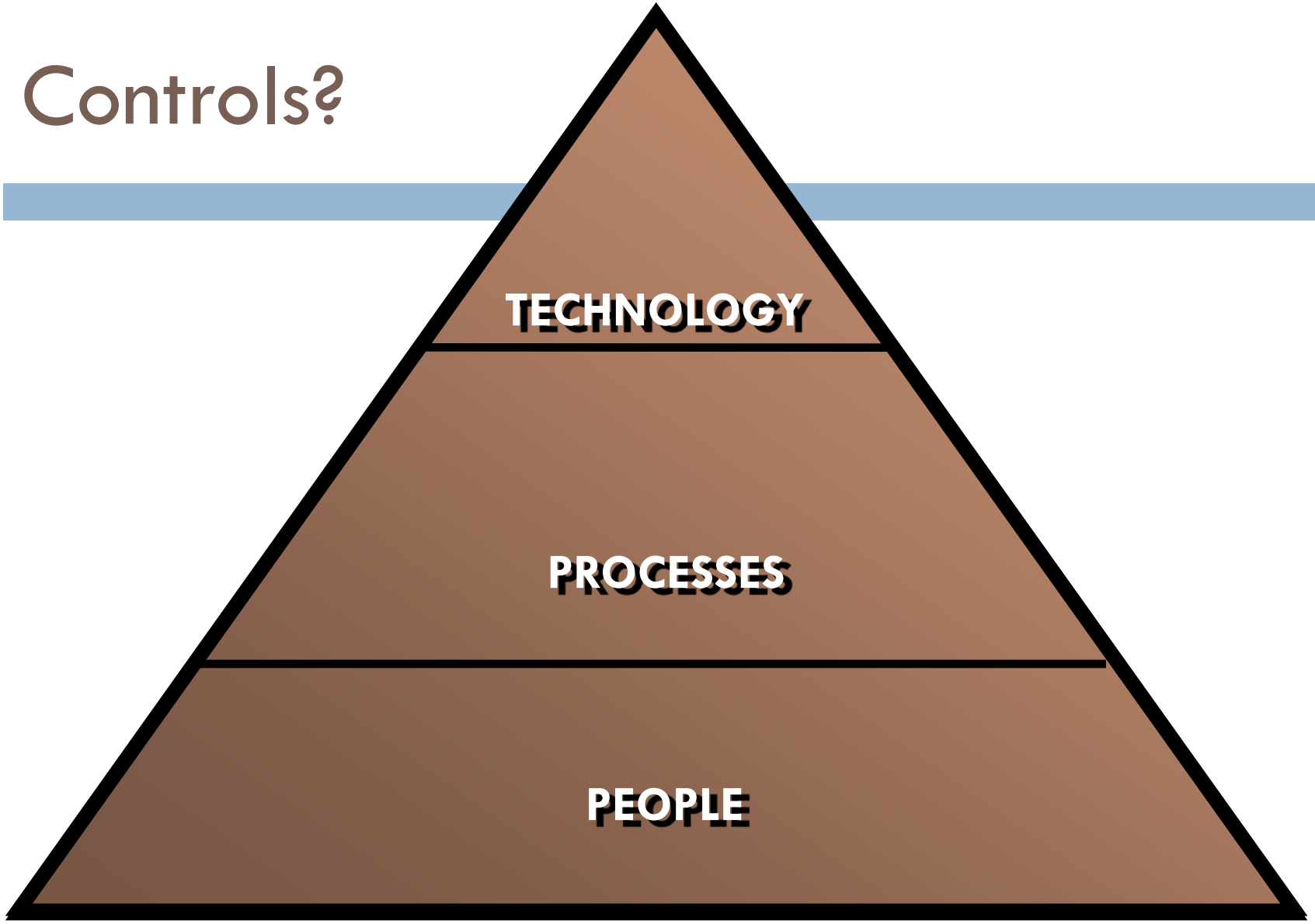
http://psyc.queensu.ca/target/chapter06.html

Risk Homeostasis Theory

- In all activities, people balance subjective estimates of risk with the benefits they are hoping to receive

- There may be such thing as "too little risk"
  - i.e., "optimal" risk level is not equal to zero

Controls?



Fundamentally, only THREE countermeasures are available to protect critical information infrastructures.

Solutions

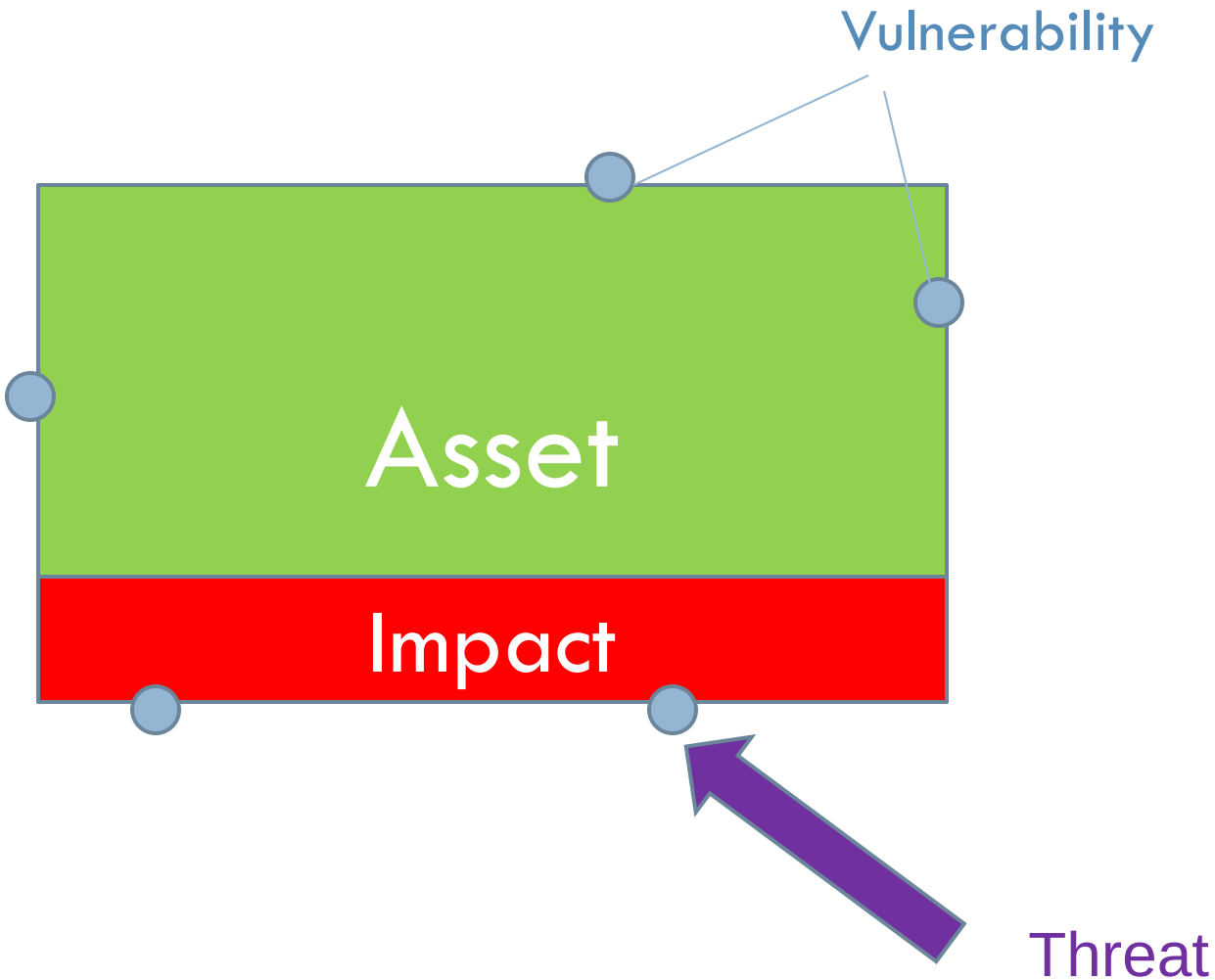
- Technical
  - Doesn't look like it's working – from ABS to antivirus
- Policies/processes (enforcement)
  - Sometimes it's working, if the rewards are positive
  - Beware of reactance; reciprocity
- People-oriented (education)
  - Sometimes it's working, if it focuses on positive reinforcement and simple messages
  - Beware of building overconfidence

Miles Edmundson, RSA talk http://www.youtube.com/watch?v=InVAztkJtFc

Strength in numbers

Corporate decision making

Risk Management



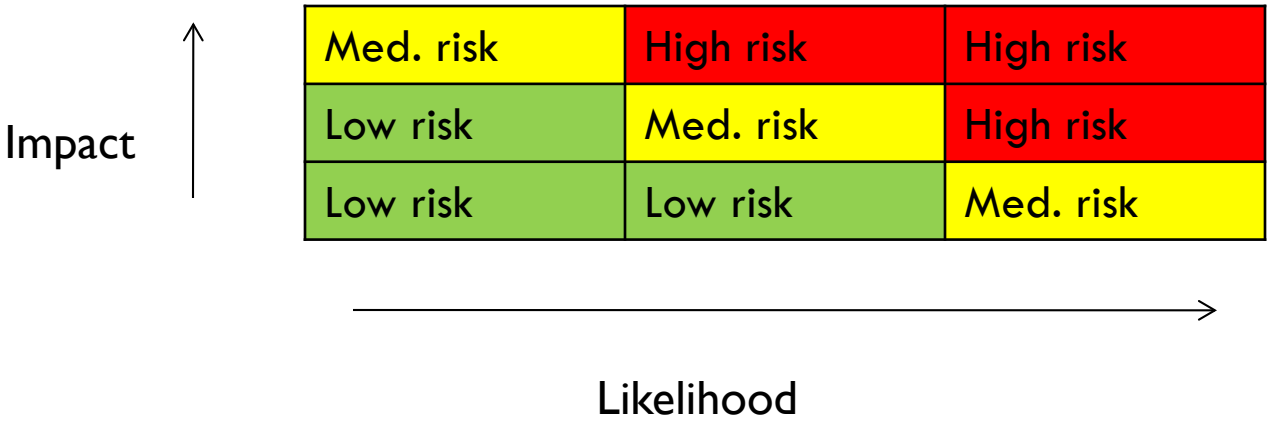
Ways of dealing with risk

- Accept
  - "Do nothing" – does not mean being oblivious to risk!
- Transfer
  - Legal agreement, insurance, pooling arrangements
- Mitigate
  - Implement countermeasures yourself

Qualitative versus Quantitative Risk Assessment

- It is impossible to conduct risk management that is purely quantitative.
- Usually risk management includes both qualitative and quantitative elements, requiring both analysis and judgment or experience.
- It is possible to accomplish purely qualitative risk management.

Qualitative risk assessment



Quantitative risk assessment

- ALE = ARO x SLE
  - SLE = AV x EF

- ALE = Annualized loss expectancy
- ARO = Annual rate of occurrence
- SLE = Single loss expectancy
- AV = Asset value
- EF = Exposure factor

Is there something wrong with this approach?

Economics, rationality and risk

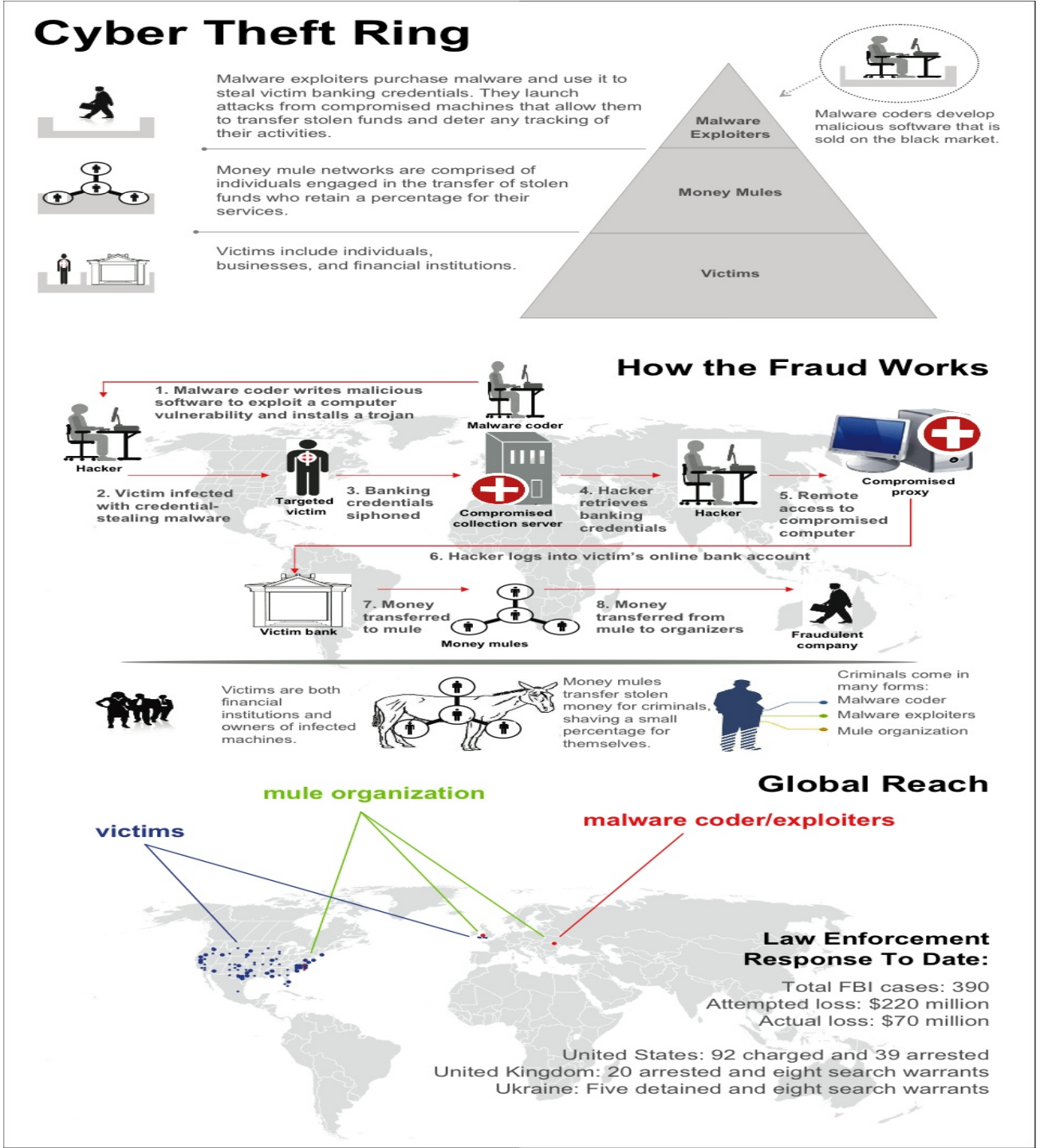
- What is “economic rationality”?
- What is “rational” attitude towards risk?
- Alternative theories of risk
  - Value at risk
  - Ruin theory
  - Info-gap decision theory

Meanwhile, on the dark side…

Black market at work

Zeus

- Accounted for about 50% of all financial information stolen in 2009-2010
- Basic configuration tool sold for $700, versions with updates(!) and support(!!!!) sold for up to $15,000
- Highly customizable
- 55% of infected machines had up-to-date antivirus (effective detection rate of 23% - Trusteer 2009)



Source: FBI, via Wikipedia

Zeus is dead? All hail SpyEye!

- Competition between trojans
- Zeus writer announced “retirement” in Oct. 2010
- Word was that SpyEye writers bought out Zeus
- Zeus source code leaked to public in May’11

- In March 2011, there were 230 verified SpyEye C&C servers, 25 with files online
- Average detection rate by antivirus is 29.72% (malwarehelp.org)

Evolution of Zeus and SpyEye

- Variants for Android, Blackberry platforms
- Capable of bypassing two-factor authentication (e.g., via intercept of text messages)
- Intercepting bank web pages and presenting fake account balances in the browser

Thank you!