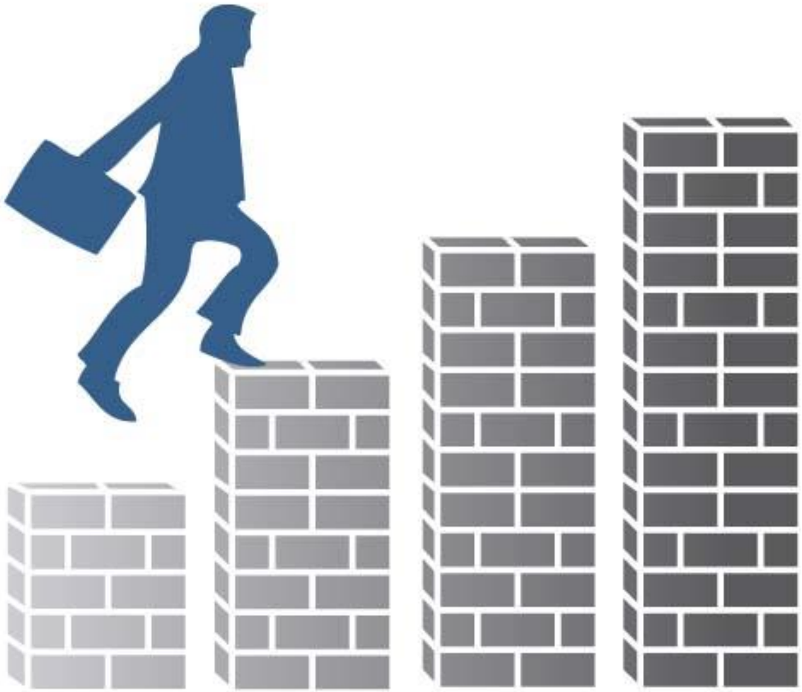
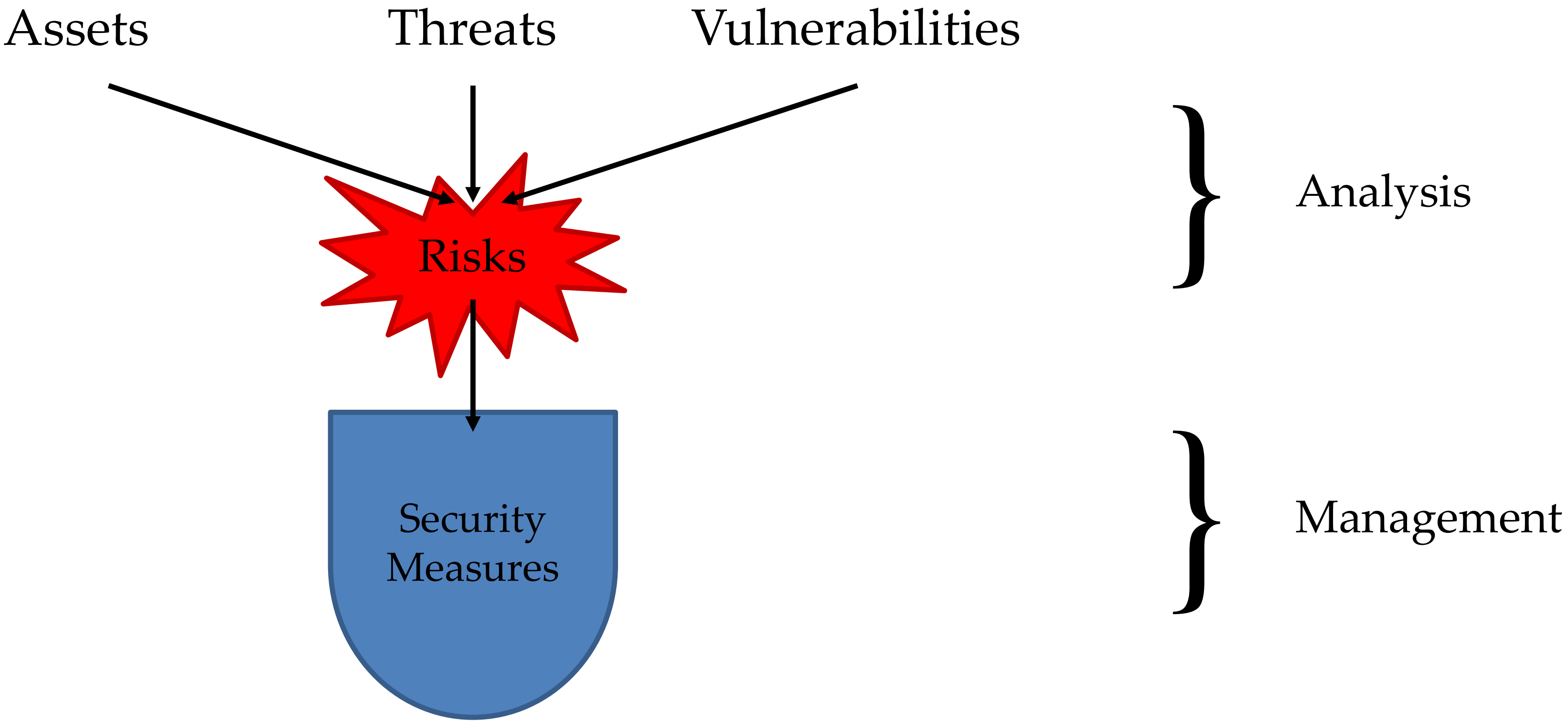


Risk

People and Security
Lecture 2

Risk Analysis & Management Framework



Definitions

- **Threat**: Harm that can happen to an asset
- **Impact**: A measure of the seriousness of a threat
- **Attack**: A threatening event
- **Attacker**: The agent causing an attack (not necessarily human)
- **Vulnerability**: a weakness in the system that makes an attack more likely to succeed
- **Risk**: a quantified measure of the likelihood of a threat being realised

Outcome of Risk Analysis

1. All assets have been identified, and their importance for the business has been rated
2. Threats have been identified, and the likelihood of them being realised has been assessed*
3. Vulnerabilities have been identified, and the likelihood of them being exploited assessed*
4. 1-3 are documented in a risk register.

* Problem: not all threats and vulnerabilities will be known

Risk Registers

- Output of risk analysis for a large and complex system is large and difficult to manage
- RR = way of making output of complex risk analysis more manageable/reusable
- Lists all the identified risks (unique identifier) and the results of their analysis and evaluation
  - Risk type
  - Owner of risk
  - Possible response
  - Residual risk

Impact Valuation

- Identification and valuation of threats - for each group of assets
- Identify threats, e.g. for stored data
  - Loss of confidentiality
  - Loss of integrity
  - Loss of completeness
  - Loss of availability (Denial of Service)
- For many asset types the only threat is loss of availability
- Assess impact of threat
  - Assess in levels, e.g H-M-L or 1 - 10
  - This gives the valuation of the asset in the face of the threat

Process Analysis

1. Every company or organisation has some processes that are critical to its operation
2. The criticality of a process may increase the impact valuation of one or more assets identified
3. So:
   - Identify critical processes
   - Prioritise assets needed for critical processes
   - Revise impact valuation of these assets

Vulnerabilities

For each threat:

1. Identify vulnerabilities
   - How to exploit a threat successfully
2. Assess levels of likelihood of attempt - High, Medium, Low
   - Expensive attacks are less likely (e.g. brute-force attacks on encryption keys)
   - Successful exploitation of vulnerability
3. Combine them

Vulnerability		Likelihood of Attempt		
		Low	Med	High
Likelihood of Success	Low	*Low*	*Low*	*Med*
	Med	*Low*	*Med*	*High*
	High	*Med*	*Med*	*High*

Impact

- If we had accurate probabilities and values, risk would be
  - *Impact valuation* x *probability of threat* x *probability of exploitation*
  - Plus a correction factor for risk aversion
- Since we haven't, we construct matrices such as:

Risk		***Impact valuation***		
		Low	Med	High
Vulnerability	Low	*Low*	*Low*	*Med*
	Med	*Low*	*Med*	*High*
	High	*Low*	*Med*	*High*

Responses to Risk

1. Avoid it completely by withdrawing from an activity
2. Accept it and do nothing
3. Reduce it with security measures
   - Prevention
   - Detection
   - Reaction/recovery
   - Insurance

Security Measures

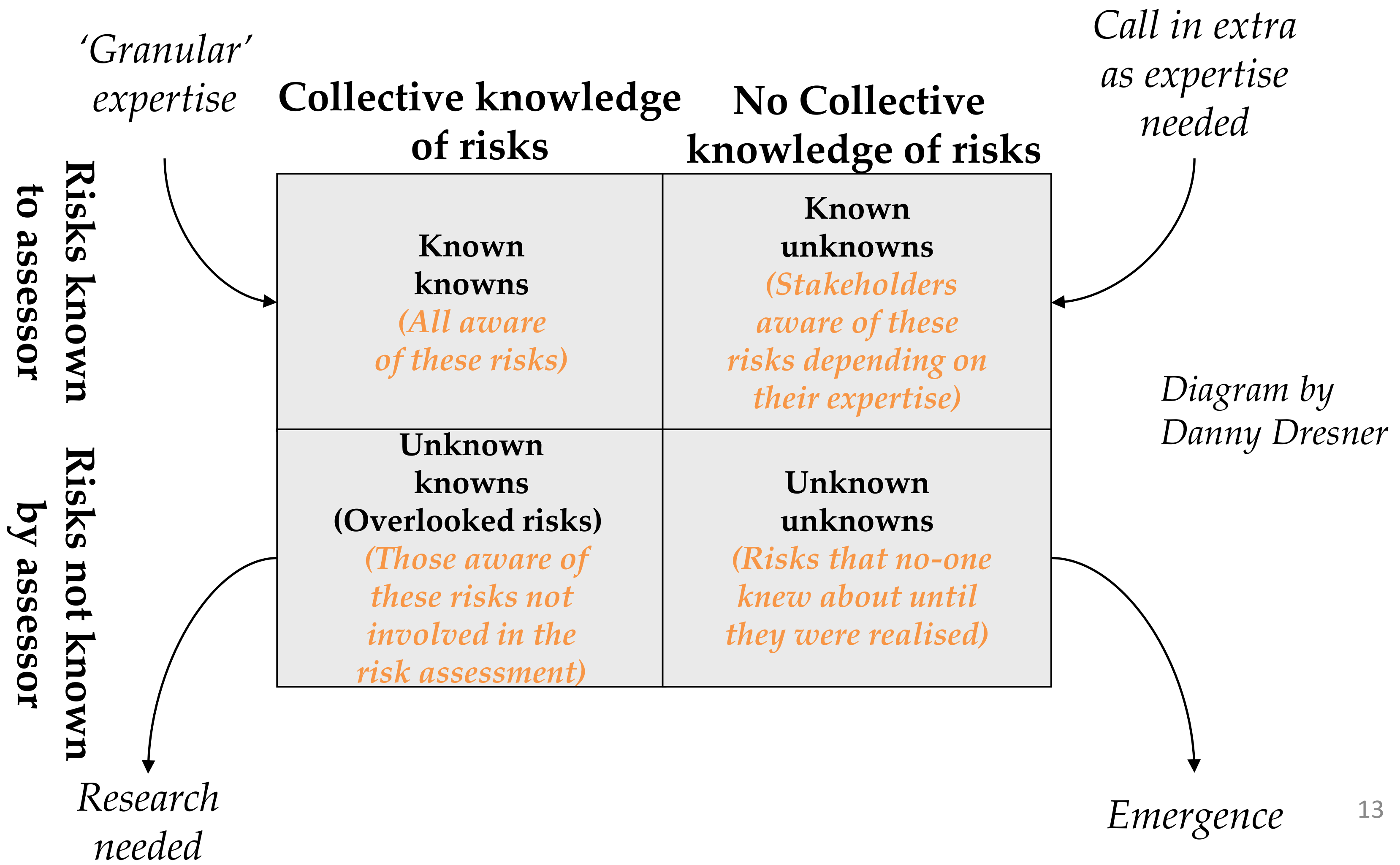
- Reduce vulnerability
  1. Reduce likelihood of attempt
     - e.g. publicise security measures in order to deter attackers
     - e.g. competitive approach - the "lion-hunter's approach" to security
  2. Reduce likelihood of success by preventive measures
     - e.g. access control, encryption, firewall
- Reduce impact, e.g. use fire extinguisher / firewall
- Recovery measures, e.g. restoration from backup

Risks of countermeasures

- Countermeasures reduce risks – but may introduce new ones
- These need to be identified and managed
- Go round the loop again …

"Oh, it was just like any other day at work. Except for the part where I sneezed by the paper shredder."

“Rumsfeld Matrix”



	Collective knowledge of risks	No Collective knowledge of risks
Risks known to assessor	**Known knowns** *(All aware of these risks)*	**Known unknowns** *(Stakeholders aware of these risks depending on their expertise)*
Risks not known by assessor	**Unknown knowns (Overlooked risks)** *(Those aware of these risks not involved in the risk assessment)*	**Unknown unknowns** *(Risks that no-one knew about until they were realised)*

‘Granular’ expertise

Call in extra as expertise needed

Research needed

Emergence

Diagram by Danny Dresner

Risks and Uncertainty

- Gigerenzer (2014) delineates between risk and uncertainty
- Known risk : probabilities that can be measured empirically – if risks are known *analytical* thinking lead to optimal decision-making
- Uncertainties cannot be measured empirically as risks are unknown – *intuition/heuristics* also required for good decision-making
- Most risks are a mixture of both so require statistical and logical analysis combined with intuitive or ‘rules-of-thumb’ thinking (Gigerenzer, 2014)

Effective decision making

- With all this to consider how can security managers make effective decisions?
- Effective decisions balance:
  - Security (mitigating risk) and productivity
  - Task requirements and user capabilities
  - Cost of implementation and value of protection
- Economics provides a suitable framework

Key problem

- *"…security-unaware users have specific security requirements, but usually no security expertise."* [Gollmann *2010*]
- How can we help individuals and organisations to make good risk decisions around information security?

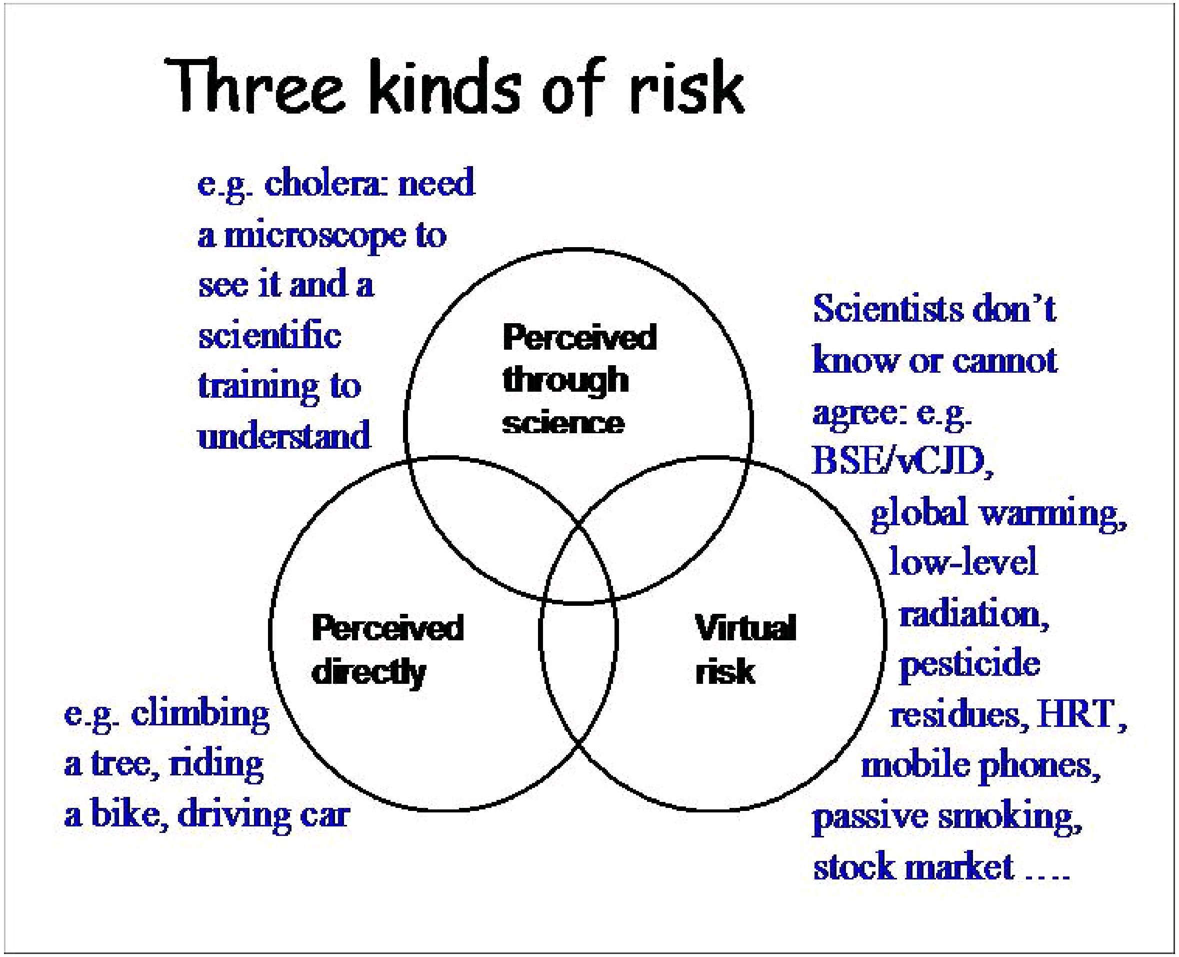
Risk Management – beyond the science bit

“Risk management is not rocket science – it’s much more complicated.”

“ The risk manager must […] deal not only with risk perceived through science, but also with virtual risk - risks where the science is inconclusive and people are thus liberated to argue from, and act upon, pre-established beliefs, convictions, prejudices and superstitions.”

- John Adams

John Adams: 3 types of risk



Three kinds of risk

e.g. cholera: need a microscope to see it and a scientific training to understand

Perceived through science

Scientists don't know or cannot agree: e.g. BSE/vCJD, global warming, low-level radiation, pesticide residues, HRT, mobile phones, passive smoking, stock market ….

Perceived directly

Virtual risk

e.g. climbing a tree, riding a bike, driving car

Directly perceptible risks

- Dealt with using judgement – a combination of instinct intuition and experience
- *“One does not undertake a formal, probabilistic, risk assessment before crossing the road.”*
- Highly dependent on our sensory capabilities
  - We cannot see germs or other causes of illness

Risk perceived through science

- Rational actor, formal management
- Most published literature on risk management falls into this category

"Here one finds not only biological scientists in lab coats peering through microscopes, but physicists, chemists, engineers, doctors, statisticians, actuaries, epidemiologists and numerous other categories of scientist who have helped us to see risks that are invisible to the naked eye. Collectively they have improved enormously our ability to manage risk – as evidenced by the huge increase in average life spans that has coincided with the rise of science and technology."

Virtual risk

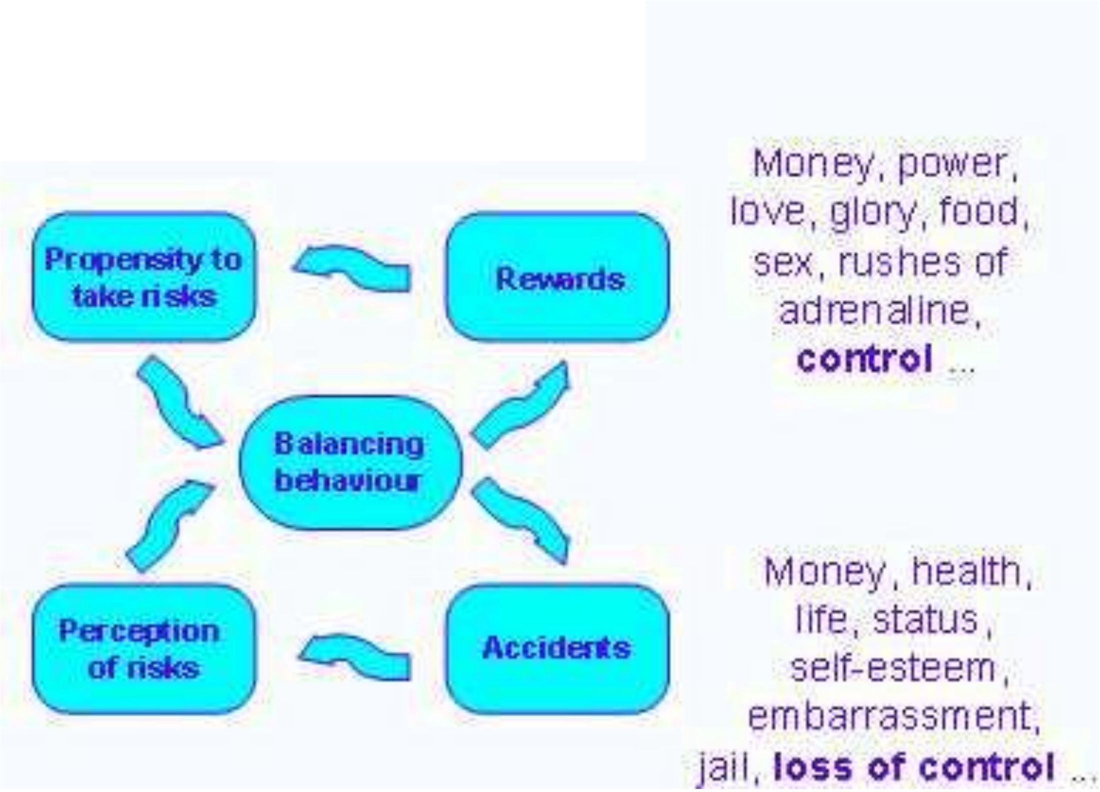
- Where the science is inconclusive, we are thrown back on judgement
- Culturally constructed – when the science is inconclusive people are liberated to argue from, and act upon, pre-established beliefs, convictions, prejudices and superstitions.

"Such risks may or may not be real, but they have real consequences. In the presence of virtual risk what we believe depends on whom we believe, and whom we believe depends on whom we trust."

People and Risk

- People vary in their propensity to take risks
- Propensity to take risks is partly personal disposition, but mostly influenced by *perception of risk*
  - by the potential rewards of taking risks
  - by the experience of losses – one's own and others
- Individual decision to take risk: perception of risk weighed against the propensity to take risk
- Science, or culturally constructed?

Risk Thermostat



Money, power, love, glory, food, sex, rushes of adrenaline, **control** ...

Money, health, life, status, self-esteem, embarrassment, jail, **loss of control** ...

Risk compensation

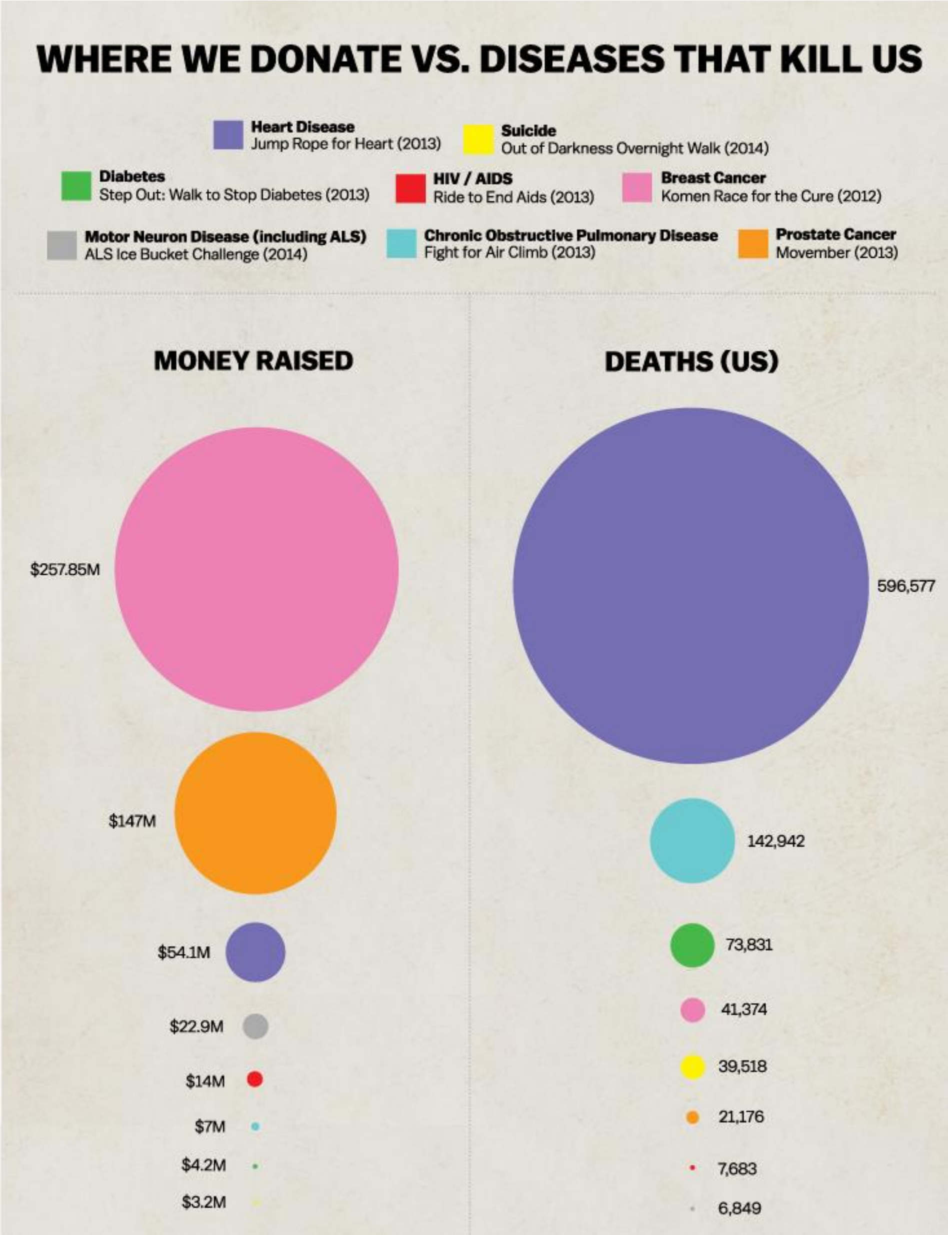
- Introducing a safety measure may change behaviour
- Adjustment takes place in risk thermostat
- Example:
  - Seat belts save lives in a crash
  - So people take more risks when driving
  - Number of accidents increases
  - Overall number of deaths remains unchanged

Thinking about risk

- Risks can be emotionally processed
  - Linked to automatic risk judgements
  - Not consciously experienced
  - "System 1" thinking, so fast and intuitive
- Consciously thinking about risk:
  - "System 2" thinking, so slower
  - More effortful…
  - … but analytical and less prone to being mislead

How good are people are at assessing risks?

- Do not assess probabilities correctly (do not take base-rate probabilities into account) – Kahnemann, Slovic & Tversky (1982)
- Over-estimate threats that are current, or have affected people/organisation they know
- Easily recalled & vivid events are likely to evoke the “Availability heuristic” which increases risk perception (Tversky & Kahneman, 1973)
- Common and familiar risks become less novel – lower perception of risk
- Forget about risks introduced by countermeasures (security measures)
- Shift of risk to other assets/stakeholders – not realising that risk remains in the system.



WHERE WE DONATE VS. DISEASES THAT KILL US

- **Heart Disease** Jump Rope for Heart (2013)
- **Suicide** Out of Darkness Overnight Walk (2014)
- **Diabetes** Step Out: Walk to Stop Diabetes (2013)
- **HIV / AIDS** Ride to End Aids (2013)
- **Breast Cancer** Komen Race for the Cure (2012)
- **Motor Neuron Disease (including ALS)** ALS Ice Bucket Challenge (2014)
- **Chronic Obstructive Pulmonary Disease** Fight for Air Climb (2013)
- **Prostate Cancer** Movember (2013)

Public spending on risk reduction

- Governments tend to spend far more, in terms of cost per life saved, on ‘dread’-type risks (e.g. exposure to arsenic) than on the mundane (e.g. road traffic incidents)
- A figure of $1-2 million per life saved is considered appropriate yet this is often exceeded for high-profile risks
- TSA measures introduced after 9/11 fall in to this category:
  - Hardening cockpit doors = $800,000 per life saved
  - Sky marshals = $180 million per life saved

See http://politicalscience.osu.edu/faculty/jmueller//stewarr2.pdf for full discussion

Risk perception pitfalls (Borge, 2001)

1. Overconfidence
2. Optimism
3. Faulty hindsight
4. Pattern-seeking
5. Overcompensation
6. Myopia (short-sightedness)
7. Inertia
8. Complacency
9. Zealotry

Other Biases: Illusions of Certainty (Gigerenzer, 2014)

1. The Zero-Risk Illusion:
   - Known risks mistaken for absolute certainty
   - Belief that technologies may be infallible
   - “It can’t happen to me” syndrome
   - Also lead to false positives
2. Calculable Risk Illusion:
   - Problem occurs when risk calculation is based on assumption of known risks in an uncertain environment
   - Precise numbers for uncertain risk lead to illusory certainty

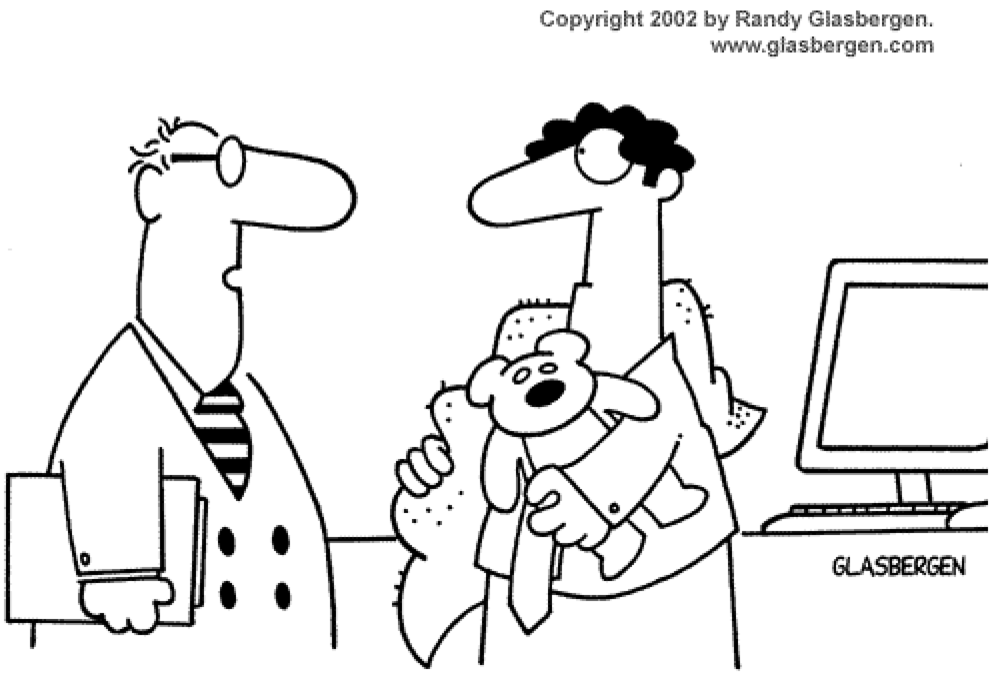
Emotion and Risk

- Psychological literature shows emotion or affect impacts risk perception
- Affect Heuristic (Slovic,2006) – use positive & negative feelings as a cue to assess risks and benefits
- "Risk-as-feelings" hypothesis (Lowenstein *et al*, 2001)
- Emotional processing heightens risk perception (Loewenstein *et al*, 2001)
- Risk perception influenced by what we like and don't like : inverse relationship between risk and benefit (Finucane *et al*, 2000)
- Affective biases underpin risk perception which in turn influences security compliance behaviour

Impact on security

- Individuals make risk calculations based on their affect heuristic
  - Risk perception is emotionally influenced and therefore subjective
- Risks with no benefit to primary task are attended to
- Risks that are perceived to improve productivity are downplayed
  - Time pressure increases the effect, so fluctuations in business process result in varied risk assessments

Security Theatre



Copyright 2002 by Randy Glasbergen.
www.glasbergen.com

"Stage one of our new emphasis on security: everyone gets a teddy bear and a blankie."

Security Theatre

- Aim of security measures is not always to increase *actual* security (Schneier 2003)
- When purpose of security measure is to increase perceived, rather than actual, security
- Example: National Guard in Airports post 9/11
- Motivation
  - Managing risk perception/re-assurance
  - Deception
  - Economics

ST example

“The other week I visited the corporate headquarters of a large financial institution on Wall Street; let′s call them FinCorp. FinCorp had pretty elaborate building security. Everyone -- employees and visitors -- had to have their bags X-rayed.

Seemed silly to me, but I played along. There was a single guard watching the X-ray machine′s monitor, and a line of people putting their bags onto the machine. The people themselves weren′t searched at all. Even worse, no guard was watching the people. So when I walked with everyone else in line and just didn′t put my bag onto the machine, no one noticed.”

"It was all good fun, and I very much enjoyed describing this to FinCorp's VP of Corporate Security. He explained to me that he got a $5 million rate reduction from his insurance company by installing that X-ray machine and having some dogs sniff around the building a couple of times a week.

I thought the building's security was a waste of money. It was actually a source of corporate profit."

“The point of this story is one that I’ve made in Beyond Fear *and many other places: security decisions are often made for non-security reasons. When you encounter a security risk that people worry about inordinately, a security countermeasure that doesn’t counter the threat, or any security decision that makes no sense, you need to understand more of the context behind the decision. What is the agenda of the person who made the decision? What are the non-security considerations around the decision? Security decisions make sense, as long as you understand them properly.”*

Bruce Schneier: CRYPTO-GRAM, July 15, 2004

Is he right?

- Consider risk distribution for different stakeholders
- What about other kinds of costs?