SECURITY (COMP0141): ECONOMICS OF SECURITY

CAUSES OF DEATH

Which do you think causes more deaths, and by how wide a margin?

Strokes or an accident (so, all accidents combined)?

Tornadoes or asthma?

Lightning or botulism?

Disease or an accident (again, all accidents combined)?

Diabetes or an accident (again, all accidents combined)?

These and all the examples in this lecture are taken from a (fantastic) book called Thinking, Fast and Slow by Daniel Kahneman

CAUSES OF DEATH

Which do you think causes more deaths, and by how wide a margin?

Strokes or an accident (so, all accidents combined)?
Strokes cause almost twice as many deaths
Tornadoes or asthma?
Asthma causes 20 times more deaths
Lightning or botulism?
Death by lightning is 52 times more frequent
Disease or an accident (again, all accidents combined)?
Death by disease is 18 times more frequent
Diabetes or an accident (again, all accidents combined)?
Death by accident is 4 times more frequent

Most people tend to get these numbers wrong or backwards

ECONOMICS OF SECURITY

We make the same estimates when considering security threats, which we have **limited resources** to address

Economic theory provides a framework for understanding the driving factors behind security behaviour (for both decision makers and users)

This shows up in evaluating security threats as well

GAMBLING

Choose between the following two options:

- (A) A 100% chance to win £80
- (B) An 80% chance to win £100 and a 20% chance to win £10

Let's now look at how we (humans) feel about gains and losses

GAMBLING

Choose between the following two options:

- (A) A 100% chance to win £80
- (B) An 80% chance to win £100 and a 20% chance to win £10

Did you pick A? But in expectation we have

E[A] = 80
E[B] = 0.8 * 100 + 0.2 * 10 = 82

So **B is strictly better than A**

Most people would pick the sure gain

GAMBLING

Choose between the following two options:

- (A) A 100% chance to get £240
- (B) A 25% chance to get £1000 and a 75% chance to get nothing

Choose between the following two options:

- (C) A 100% chance to lose £750
- (D) A 75% chance to lose £1000 and a 25% chance to lose nothing

GAMBLING

Choose between the following two options:

- (A) A 100% chance to get £240
- (B) A 25% chance to get £1000 and a 75% chance to get nothing

Choose between the following two options:

- (C) A 100% chance to lose £750
- (D) A 75% chance to lose £1000 and a 25% chance to lose nothing

Did you pick A and D? So did 73% of participants (and only 3% of participants picked B and C), even though in expectation **A is strictly worse than B** (and C and D are exactly the same)

Humans are risk averse when it comes to gains and risk seeking when it comes to losses

GAMBLING

Consider the following two options:

- (AD) A 25% chance to win £240 and a 75% chance to lose £760
- (BC) A 25% chance to win £250 and a 75% chance to lose £750

BC is the combination of the two previously rejected options

E[AD] = 0.25 * 240 + 0.75 * (-760) = -510
E[BC] = 0.25 * 250 + 0.75 * (-750) = -500

But **BC is strictly better than AD**!

We also don't see how our decisions affect each other

PROSPECT THEORY

Utility theory: Humans are rational actors who are looking to maximise their own **utility** (satisfaction, happiness, wealth, etc.)

Prospect theory: Humans have bounded rationality: limited time and resources when making decisions

- Substitute heuristics instead (like loss aversion)
- Simplify the decision
- Choose a satisfactory option (but maybe not the best)

Prospect theory is a more realistic view of human behaviour

SECURITY DECISION-MAKING

So how do humans make security-related decisions? Motivating factors are:

- Visible enforcement of policies
- Allegiance to organisation
- Respect for others (role models)
- Professional standards

more organisational

- (Vicarious) experience of threat
- Avoiding personal embarrassment
- Reputation

These motivations are not distinct – there can be a lot of overlap between them

SECURITY IN ORGANISATIONS

Organisations suffer from information asymmetry

- Security manager knows more about security but is not the one making decisions
- Employee is making decisions but might know very little about security (knows a lot about doing their job)

Employees are already busy, time for security is taken from other tasks

As we've already seen, security is never a primary goal – this is especially true for individuals rather than the organisation as a whole

GAINS AND LOSSES

employees need incentives to act how the organisation wants

Individual costs:

- Physical workload
- Cognitive workload
- Reduced productivity

Individual benefits:

- Inherited from organisation
- Knowing you are compliant
- ?

Organisational costs:

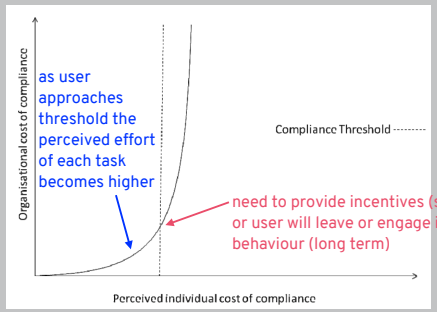
- Investment in infrastructure
- Investment in policies
- Interference with other tasks

Organisational benefits:

- Compliance
- Productivity
- Protection of IP
- Reputation

Costs here represent losses and benefits represent gains

COMPLIANCE BUDGET



The more that compliance-related tasks are pushed down to individuals, the more their perceived cost of them goes up

DECISION MAKING

So how do humans make security-related decisions? Motivating factors are:

- Visible enforcement of policies
- Allegiance to organisation
- Respect for others (role models)
- Professional standards
- (Vicarious) experience of threat
- Avoiding personal embarrassment
- Reputation

more personal

ANOTHER GUESSING GAME

Do you think English has more words starting with the letter K or with K as their third letter?

ANOTHER GUESSING GAME

Do you think English has more words starting with the letter K or with K as their third letter?

There are three times as many words with K as the third letter

Was your guess wrong? Did you form it by thinking of examples? This follows the **availability heuristic**: our perceptions are biased by how quickly we can find examples

CAUSES OF DEATH

Which do you think causes more deaths, and by how wide a margin?

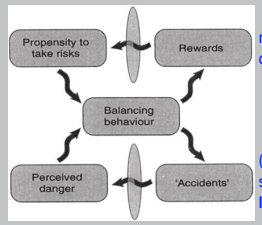
Strokes or an accident (so, all accidents combined)?
Strokes cause almost twice as many deaths
Tornadoes or asthma?
Asthma causes 20 times more deaths
Lightning or botulism?
Death by lightning is 52 times more frequent
Disease or an accident (again, all accidents combined)?
Death by disease is 18 times more frequent
Diabetes or an accident (again, all accidents combined)?
Death by accident is 4 times more frequent

This goes back to how we formed those estimates at the beginning of the lecture

PEOPLE AND RISK

People vary in their willingness (propensity) to take risks

This is partly personal disposition, but mostly **perception of risk** (influenced by availability heuristic)



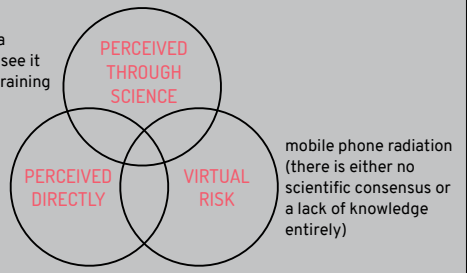
money, power, love, glory, food, **control**

(loss of) money, health, status, self-esteem, **loss of control**

This risk thermostat is due to John Adams ("Cars, cholera, and cows, the management of risk and uncertainty", 1999)

THREE TYPES OF RISKS

cholera (need a microscope to see it and scientific training to understand)

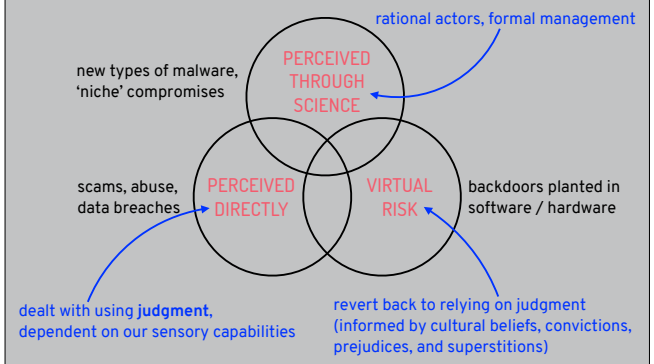


climbing a tree, extreme sports, driving a car

mobile phone radiation (there is either no scientific consensus or a lack of knowledge entirely)

These categorisations are also due to John Adams

THREE TYPES OF SECURITY RISKS



21

One example with virtual risk is not using online banking (or banking at all)

RISK VS. UNCERTAINTY

Uncertainty occurs when outcomes or probabilities are unknown

If a small risk is uncertain, this leads to the perception of it being non-existent (easy to downplay)

A focus on certain risks means people put disproportionate effort/ resources into their management (and neglect uncertain risks)

But humans are bad at both:

- Estimating the seriousness of a risk (**outcome**)
- Estimating the chance of it happening to them (**probability**)

22