RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: GRM-R08

The Psychology of Info Sec

Wayne Tufek

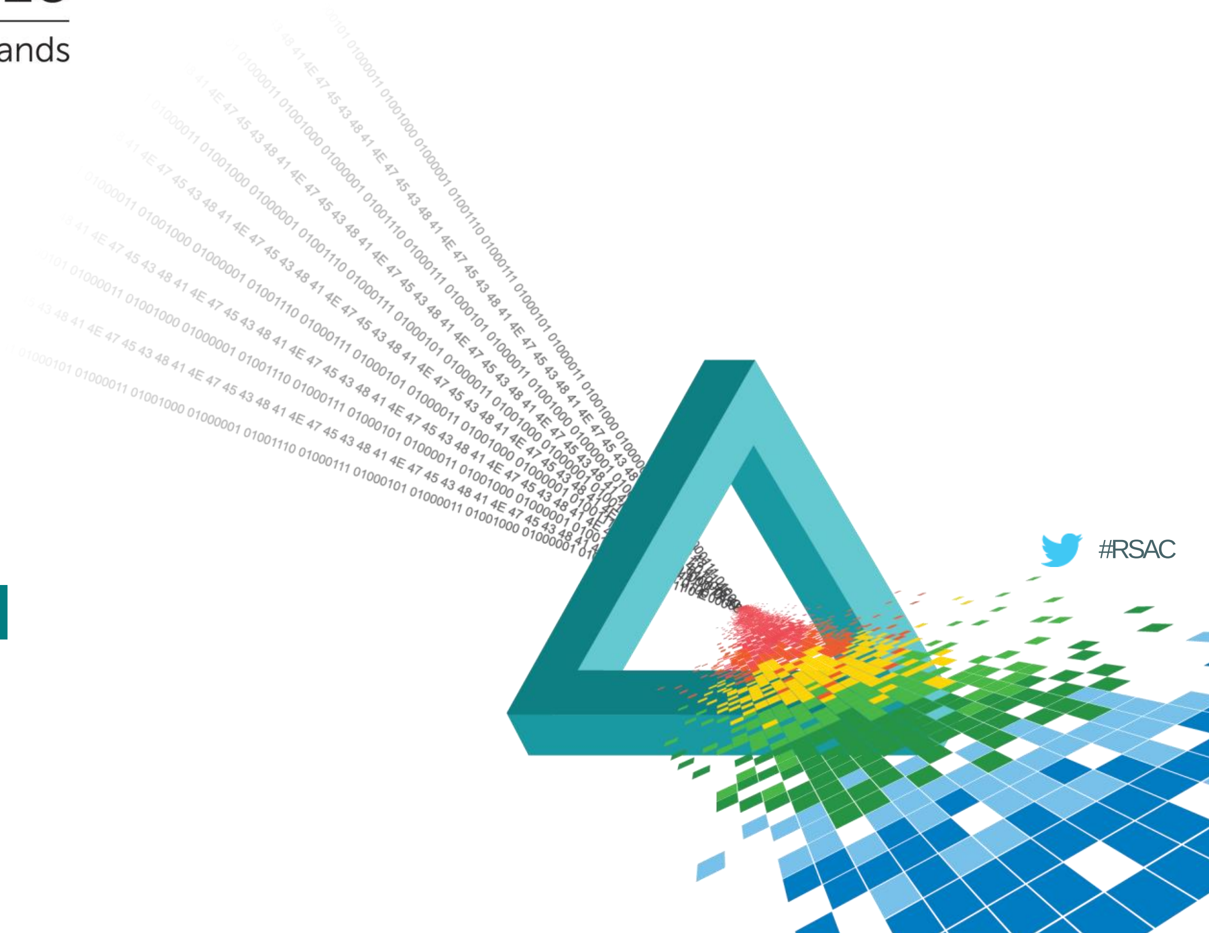
IT Security Architect
Officeworks

Agenda

- Chapter 1: Info Sec – the sell
- Chapter 2: Human decision making in risky situations
- Chapter 3: Persuasion
- Chapter 4: Towards an Info Sec safety culture
- Chapter 5: What next?

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Info Sec – the sell

The Info Sec Salesman

- Who here today is an Info Sec salesman?

The Info Sec Salesman

- A conversation with your CFO
  - CISO: This year I need $1 000 000 more for my security program
  - CFO: How much did you spend last year?
  - CISO: Just what was budgeted
  - CFO: Anything bad happen?
  - CISO: No, nothing
  - CFO: Great! Keep up the good work.

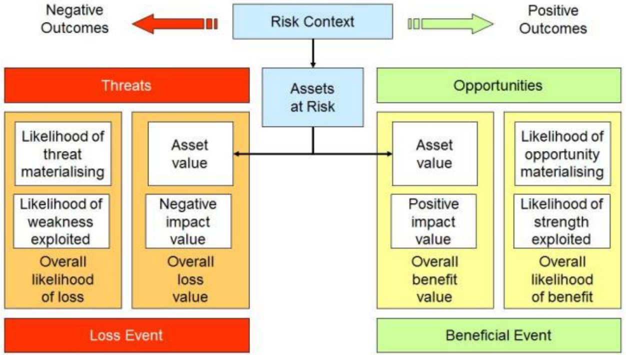
Chapter 1: The Info Sec Sell

- What do you do?
- How much does it cost?
- What value does it provide?

Chapter 1: The Info Sec Sell

- Risk
  - Rewarded
  - Unrewarded
- **The flipside of risk is Opportunity**

Revenue
Reputation
Resilience
Regulation



Source: www.sabsa.org

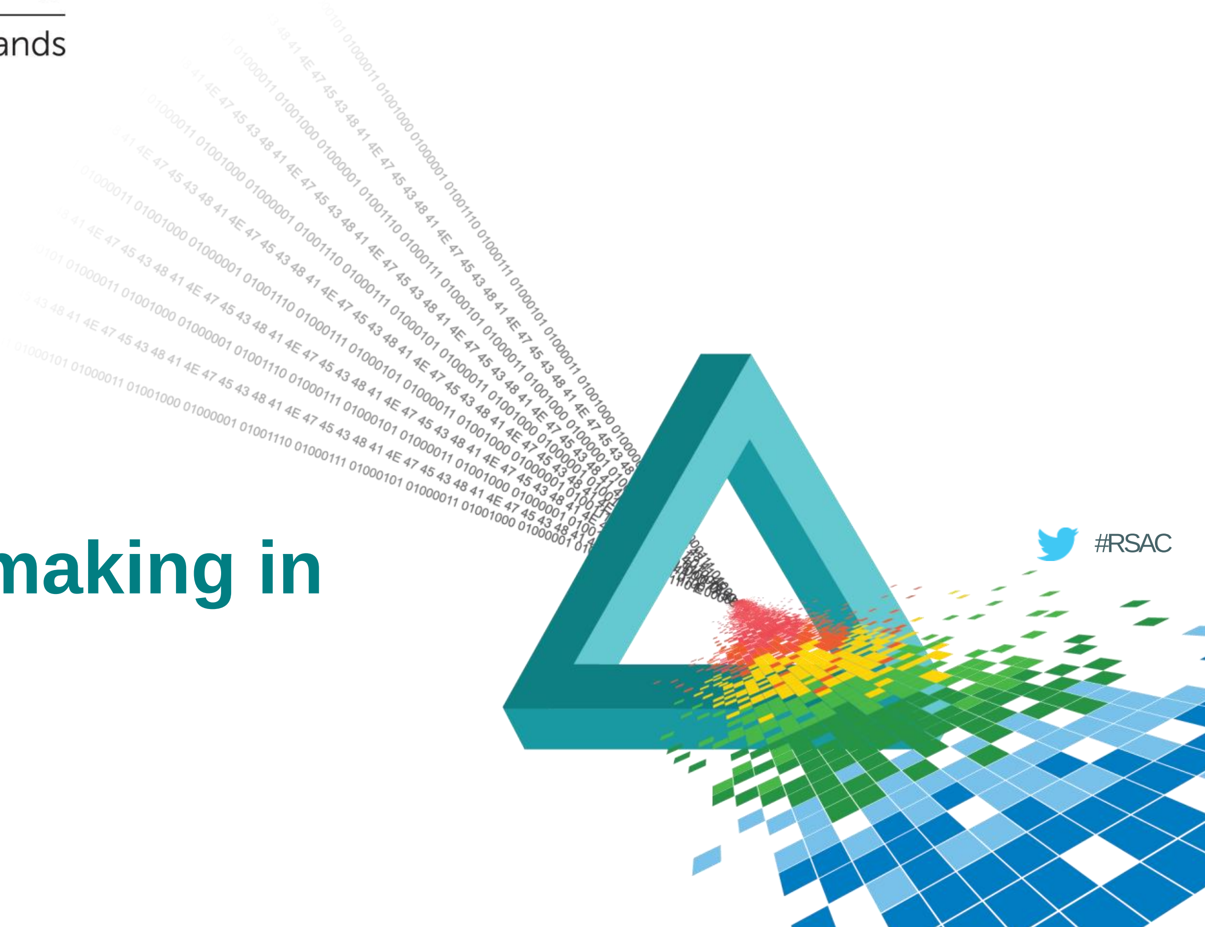
Chapter 1: The Info Sec Sell

- Selling **business value** through the **realisation of rewarded risk** and the **mitigation of unrewarded risk**
- The objective of the Info Sec function is to manage risks to an acceptable level
- The specific risks to be managed will differ between organisations as will the level of tolerable or acceptable risk

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Human decision making in risky situations

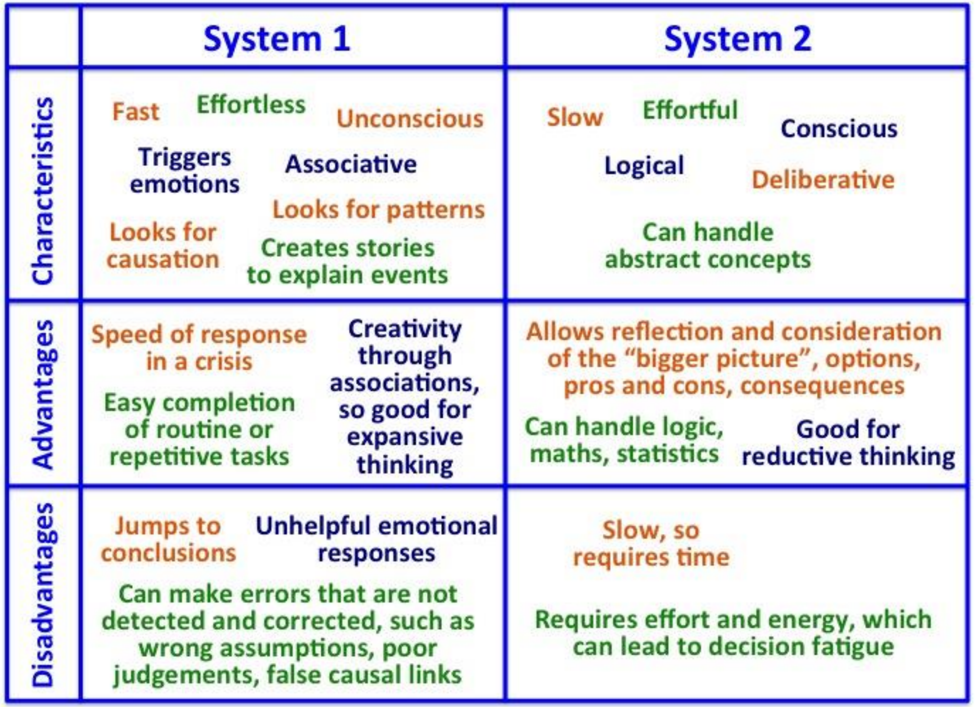


#RSAC

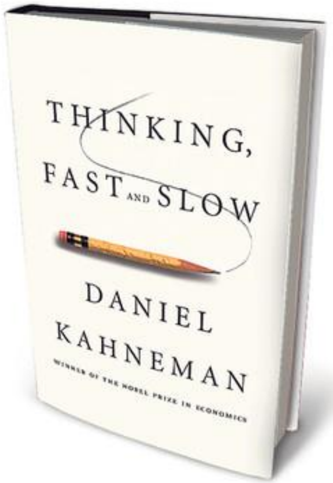
Chapter 2: Human decision making in risky situations

- Decisions involve risk
- Kahneman and Tversky

Chapter 2: Human decision making in risky situations



	System 1	System 2
Characteristics	Fast Effortless Unconscious Triggers emotions Associative Looks for patterns Looks for causation Creates stories to explain events	Slow Effortful Conscious Logical Deliberative Can handle abstract concepts
Advantages	Speed of response in a crisis Creativity through associations, so good for expansive thinking Easy completion of routine or repetitive tasks	Allows reflection and consideration of the "bigger picture", options, pros and cons, consequences Can handle logic, maths, statistics Good for reductive thinking
Disadvantages	Jumps to conclusions Unhelpful emotional responses Can make errors that are not detected and corrected, such as wrong assumptions, poor judgements, false causal links	Slow, so requires time Requires effort and energy, which can lead to decision fatigue



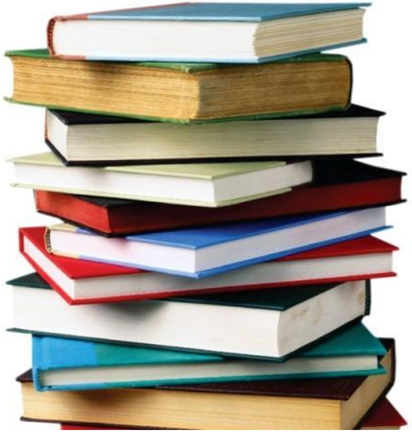
Source: http://electia.co.uk/tag/daniel-kahneman/

Chapter 2: Human decision making in risky situations

- **"If it takes 5 machines 5 minutes to make 5 widgets, how many minutes does it take 100 machines to make 100 widgets?"**

- The answer "100 minutes" leaps to mind (System 1 at work), but it is wrong. But a bit of reflective thought (by System 2) leads to "five minutes," the right answer.

Chapter 2: Human decision making in risky situations



An individual has been described as follows:

“Steve is very shy and withdrawn, invariably helpful but with very little interest in people or in the world of reality. A meek and tidy soul, he has a need for order and structure, and a passion for detail.”

Is Steve more likely to be a librarian, a pilot, surgeon or a farmer?

Chapter 2: Human decision making in risky situations

- Heuristics

Chapter 2: Human decision making in risky situations

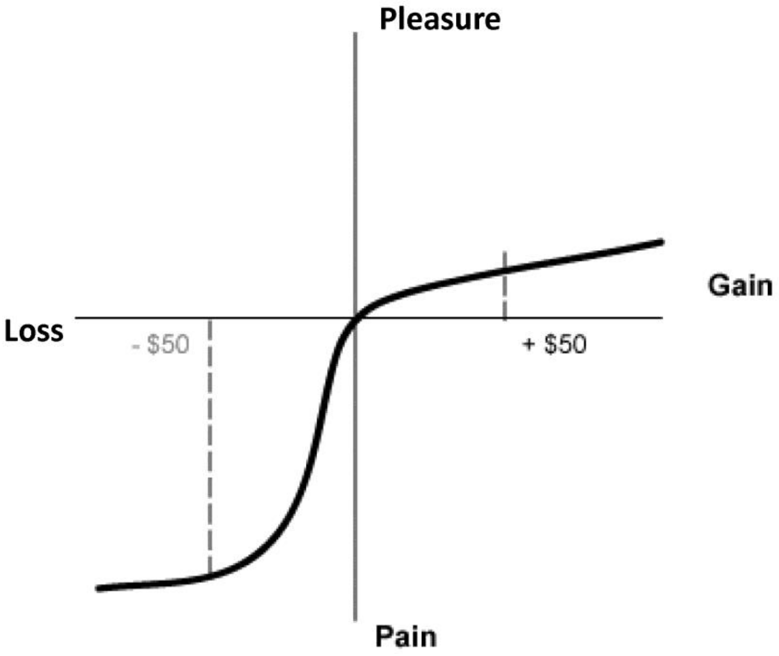
- Representativeness
- Availability
- Adjustment and anchoring

Chapter 2: Human decision making in risky situations

- Biases
  - Optimism bias
  - Hindsight bias
  - Confirmation bias

Chapter 2: Human decision making in risky situations

- Prospect theory



Chapter 2: Human decision making in risky situations

- Scenario One – The test subject was asked to pick between:
  - Option A: A 100% chance of losing $3000 or
  - Option B: An 80% chance of losing $4000, and a 20% chance of losing nothing.

- Scenario Two – Next, choose between:
  - Option C: A 100% chance of receiving $3000 or
  - Option D: An 80% chance of receiving $4000, and a 20% chance of receiving nothing.

Chapter 2: Human decision making in risky situations

- Scenario One: An epidemic breaks out that is likely to kill 600 people if left untreated.
  - Treatment strategy A: will save 200 people.
  - Treatment strategy B: has 1/3 chance of saving 600 people and 2/3 chance of saving nobody.

- Scenario Two: An epidemic breaks out that is likely to kill 600 people if left untreated.
  - Treatment strategy C: 400 people will die.
  - Treatment strategy D: there is a 1/3 probability that nobody will die, and a 2/3 probability that 600 people will die.

Chapter 2: Human decision making in risky situations

- Mental models

Chapter 2: Human decision making in risky situations

- Risk and decision making in groups

Chapter 2: Human decision making in risky situations

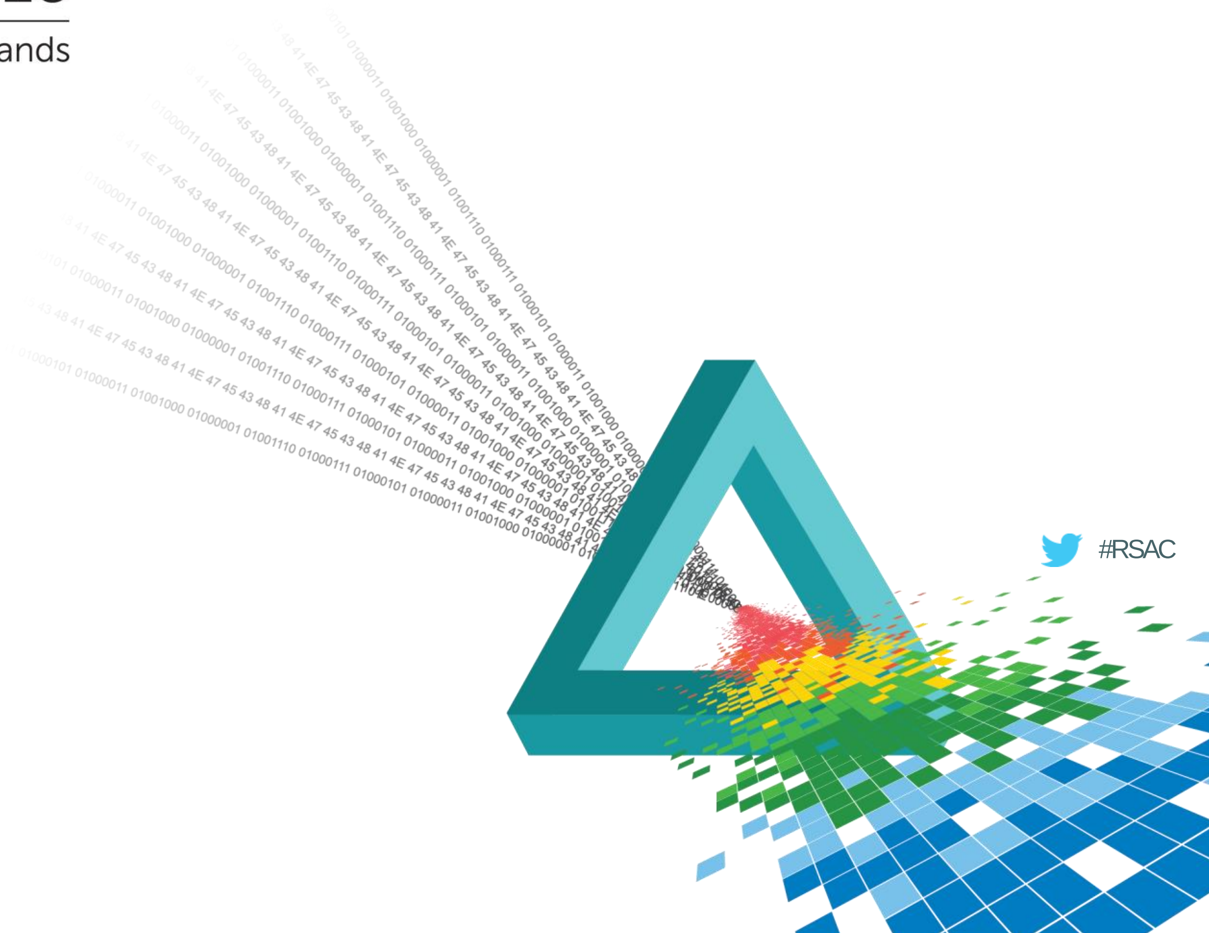
- Risk communications and the factors influencing the persuasiveness of a message
  - Order effects
  - One-sided vs two-sided presentations
  - Simplicity and repetition
  - Message medium

Chapter 2: Human decision making in risky situations

- Combating biases
  - Before finalising a decision, imagine that, a year after it has been made, it has turned out horribly, then write a history of how it went wrong and why
  - hbr.org/2011/06/the-big-idea-before-you-make-that-big-decision

RSAConference2015

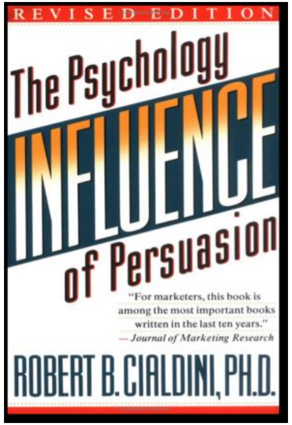
Singapore | 22-24 July | Marina Bay Sands



#RSAC

Persuasion

Chapter 3: Persuasion


REVISED EDITION
The Psychology
INFLUENCE
of Persuasion
"For marketers, this book is among the most important books written in the last ten years."
— Journal of Marketing Research
ROBERT B. CIALDINI, PH.D.

"Influence means change and moving people in a particular direction" – Robert Cialdini

Chapter 3: Persuasion

- People repay in kind
- Free stuff
- Disabled American Veterans organisation improved response (donations) from 18% to 35% by enclosing a small gift – address labels
- ‘Sure glad to help. I know how important it is for me to count on your help when I need it”

RECIPROCITY

✓ the obligation to give back what you have received from others

Chapter 3: Persuasion

- People want more of what they can have less of
- People are motivated to act by the idea of losing something rather than gaining that very thing

Chapter 3: Persuasion

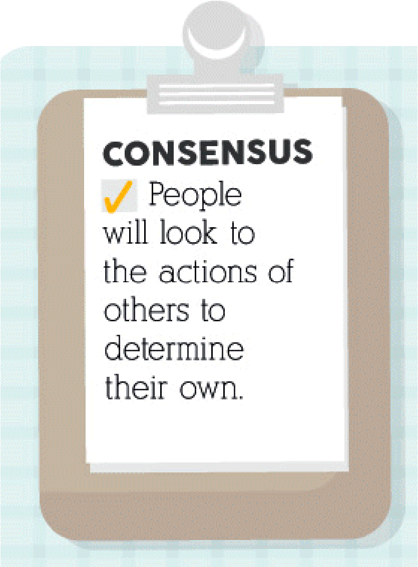
- People like those that like them
- No 1 rule of sales is to like the other person
- Bargaining by email

LIKING

✓ People prefer to say yes to those they like. But what causes a person to like another?

Chapter 3: Persuasion

- People follow the lead of similar others
- Restaurant menus, “These are our most popular dishes”, increased sales from 13% to 20%



CONSENSUS

✓ People will look to the actions of others to determine their own.

Chapter 3: Persuasion

- People align with their public commitments
- UK Doctors surgery reduced no show appointments by 18%
- “What would you like to achieve?”
- “When you made that decision in the past, I have no doubt it was the right on, but circumstances have changed. Let me show you how.”

CONSISTENCY

✓ Activated by looking for and asking for small initial commitments that can be made.

Chapter 3: Persuasion

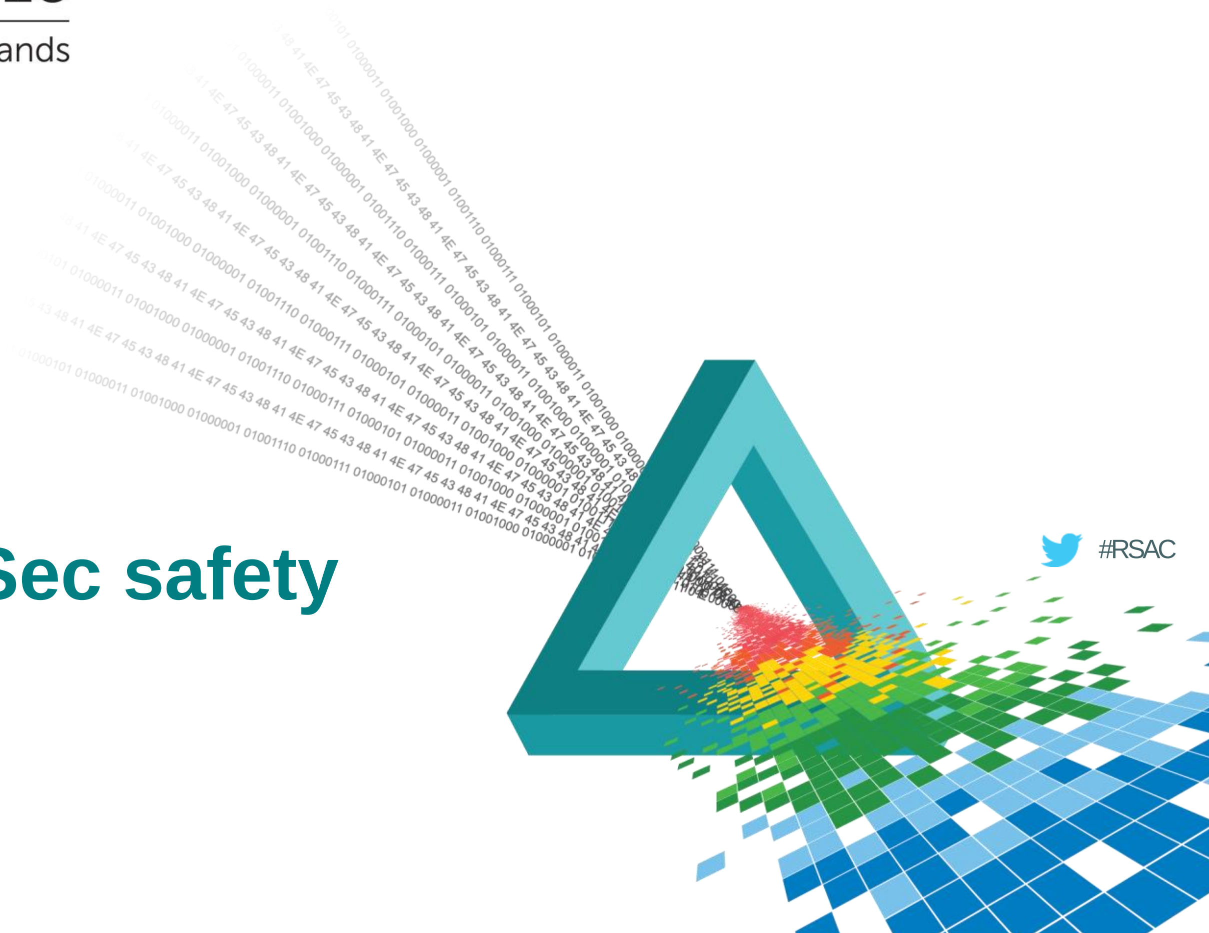
- People defer to experts
- Trustworthiness
- “The credible communicator who has both expertise and trustworthiness is the single most powerful communicator that social science has ever uncovered”
- Mention a drawback

AUTHORITY

✓ People will follow the lead of credible and knowledgeable experts.

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Towards an Info Sec safety culture

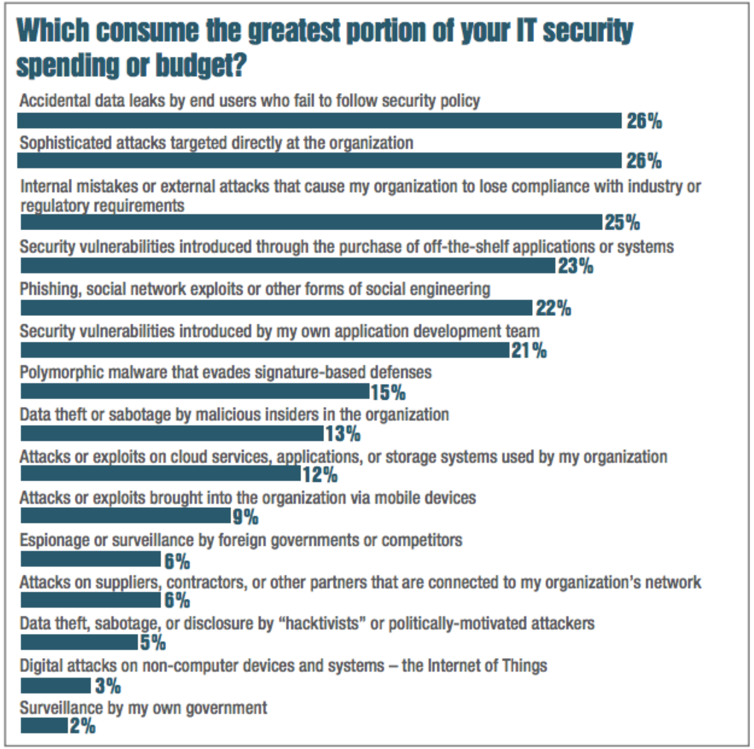
Chapter 4: Towards an Info Sec safety culture

- People, people people

Chapter 4: Towards an Info Sec safety culture

Figure 3

The 2015 Black Hat Attendee Survey

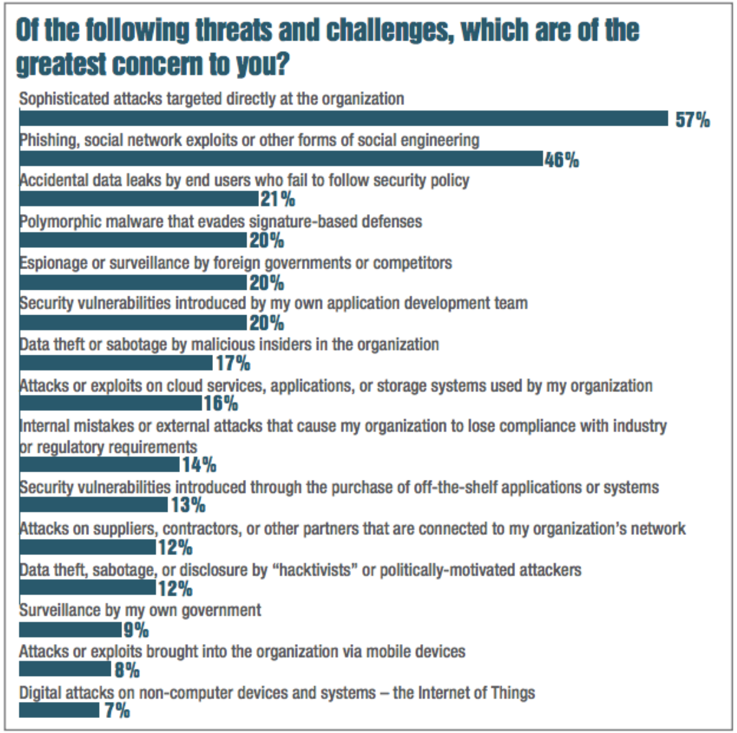


Which consume the greatest portion of your IT security spending or budget?

Note: Maximum of three responses allowed
Data: UBM survey of 460 security professionals, June 2015

Figure 1

The 2015 Black Hat Attendee Survey



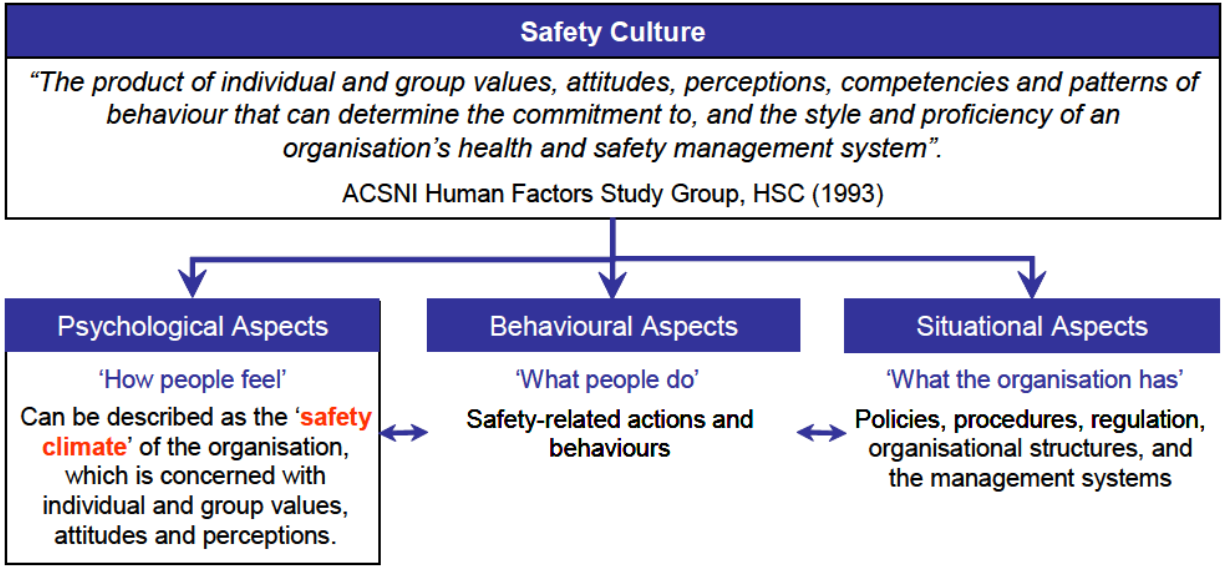
Of the following threats and challenges, which are of the greatest concern to you?

Note: Maximum of three responses allowed
Data: UBM survey of 460 security professionals, June 2015

Chapter 4: Towards an Info Sec safety culture

- What is a safety culture?
- Product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of an organisations health and safety management (http://www.hse.gov.uk/humanfactors/topics/common4.pdf)
- The way we do things around here
- A set of attitudes, beliefs or norms
- Change "health and safety" to information security

Chapter 4: Towards an Info Sec safety culture



Safety Culture

"The product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that can determine the commitment to, and the style and proficiency of an organisation's health and safety management system".

ACSNI Human Factors Study Group, HSC (1993)

Psychological Aspects

'How people feel'

Can be described as the '**safety climate**' of the organisation, which is concerned with individual and group values, attitudes and perceptions.

Behavioural Aspects

'What people do'

Safety-related actions and behaviours

Situational Aspects

'What the organisation has'

Policies, procedures, regulation, organisational structures, and the management systems

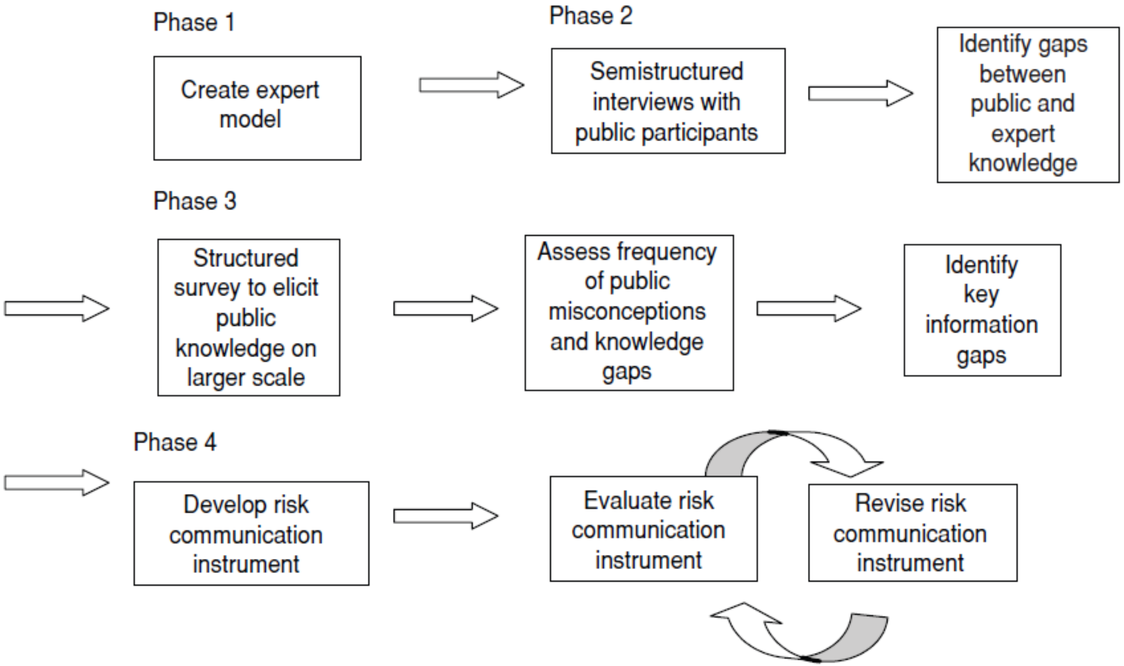
Figure 1 - A Three Aspect Approach to Safety Culture (based upon Cooper, 2000)

Chapter 4: Towards an Info Sec safety culture

- Activating the human firewall
  - What is security awareness?
  - Are you just checking the box?
  - Security awareness is not easy!
  - Engage, engage, engage
  - Measure, measure, measure
  - Have reasonable expectations
  - Reinforce, reinforce, reinforce

Chapter 4: Towards an Info Sec safety culture

FIGURE 1. Mental models risk communication framework



Phase 1

Create expert model

Phase 2

Semistructured interviews with public participants

Identify gaps between public and expert knowledge

Phase 3

Structured survey to elicit public knowledge on larger scale

Assess frequency of public misconceptions and knowledge gaps

Identify key information gaps

Phase 4

Develop risk communication instrument

Evaluate risk communication instrument

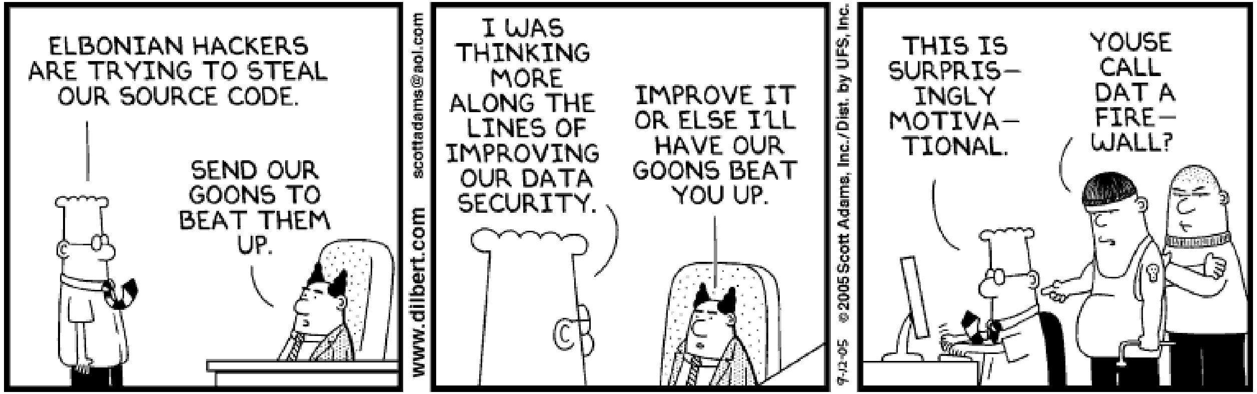
Revise risk communication instrument

Chapter 4: Towards an Info Sec safety culture

- Implementing a safety culture
  - Who’s Info Sec safety culture consists of “broadcasting” facts?
- Framing risk communications
- Mental models differ between lay people and technical experts
- Determine the difference
- Tailor your Info Sec safety culture messages

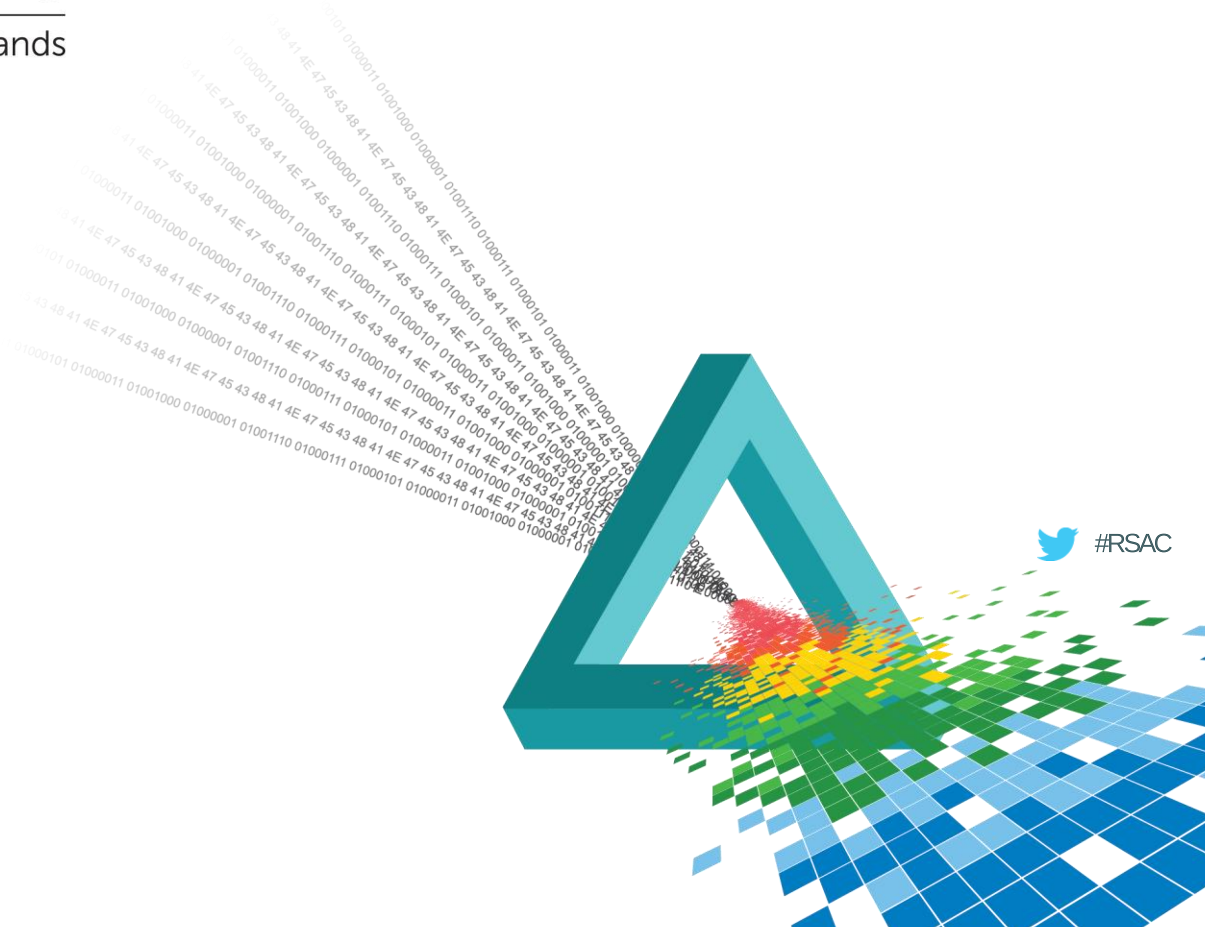
Chapter 4: Towards an Info Sec safety culture

- Simply communicating facts such as policies, does not work
- Focus on the needs of your audience


ELBONIAN HACKERS ARE TRYING TO STEAL OUR SOURCE CODE.
SEND OUR GOONS TO BEAT THEM UP.
scottadams@aol.com
www.dilbert.com
I WAS THINKING MORE ALONG THE LINES OF IMPROVING OUR DATA SECURITY.
IMPROVE IT OR ELSE I'LL HAVE OUR GOONS BEAT YOU UP.
©2005 Scott Adams, Inc./Dist. by UFS, Inc.
9-12-05
THIS IS SURPRIS-INGLY MOTIVA-TIONAL.
YOUSE CALL DAT A FIRE-WALL?

Chapter 4: Towards an Info Sec safety culture

- Resources
  - Judgement under uncertainty: Heuristics and Biases
    - psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf
  - Affect, risk and decision making
    - www.skidmore.edu/~hfoley/Exp.Labs/Lab%203.S06/Slovic_2005.pdf
  - Prospect Theory
    - www.princeton.edu/~kahneman/docs/Publications/prospect_theory.pdf
  - www.securingthehuman.org
  - scf.roer.com
  - www.restrictedintelligence.co.uk



What next?

Chapter 5: What Next?

- Summary
  - Info sec is selling **business value** through rewarded and unrewarded risk
  - **Heuristics and biases** impact decision making when risk is involved
  - How to **persuade** effectively
  - How to activate the **human firewall**
  - Synergies between a **safety culture** and security awareness
  - **Mental model** approach to implementing a safety culture

Chapter 5: What Next?

- Next week you should:
  - Revisit your organisation’s business strategy
  - Identify the business value your info sec function can provide
  - Review your security strategy
- In the first three months following this presentation you should:
  - Review and assess your info sec safety program (security awareness)
  - Start selling info sec more effectively through persuasion and understanding how risk based decisions are made (heuristics and bias)
  - Start framing risk communications more effectively
  - Start selling business value

Chapter 5: What Next?

- Within six months you should:
  - Determine your audience’s mental model as it relates to your Info Sec safety and broader programs and respond accordingly

Questions?

Contact me

- Wayne (dot) Tufek (at) gmail.com