Productive Security: A scalable methodology for analysing employee security behaviours

Adam Beautement, Ingolf Becker, **Simon Parkin**, Kat Krol, M. Angela Sasse

University College London

Background

- Security managers declare central security policy
    - Based on expertise and experience
- Restrictive technology can hinder employees
    - Employee co-operation critical
    - Over-burden and misalignment impacts business
- Policies must consider employees
    - Daily working lives are not all security – other tasks
    - Employee populations are not all the same

Motivation

Goal: generate rich snapshot of security maturity and security behaviours within a large organisation's employee population, for direct use in aligning security with business

Aim:

- Elicit realistic survey responses from employees
- Consider both scalability and meaning of the survey
- Support policy decision-making with data
 - Represent operational reality of the organisation

Motivation – security culture

- Consider employees as members of a larger organisation

- Cultural theory predicts impact that organisation norms can have upon risk perception
  - *Individualists* rely on themselves for solutions
  - *Egalitarians* rely on group solutions to problems
  - *Hierarchists* rely on existing systems or technologies
  - *Fatalists* feel that their actions are not significant

Motivation – security maturity

- Model of behaviour maturity
  - Based on CMU maturity model
- Consider security competence relative to business
  - Competence supports secure working habits
- Five levels
  - *Level 1: Is not engaged with security in any capacity*
  - Level 2: Follows security policy when forced to
  - Level 3: Knows a policy exists and follows it by rote
  - Level 4: Has internalised policy, adopts secure practices
  - Level 5: Champions security, challenges breaches

Overview of approach
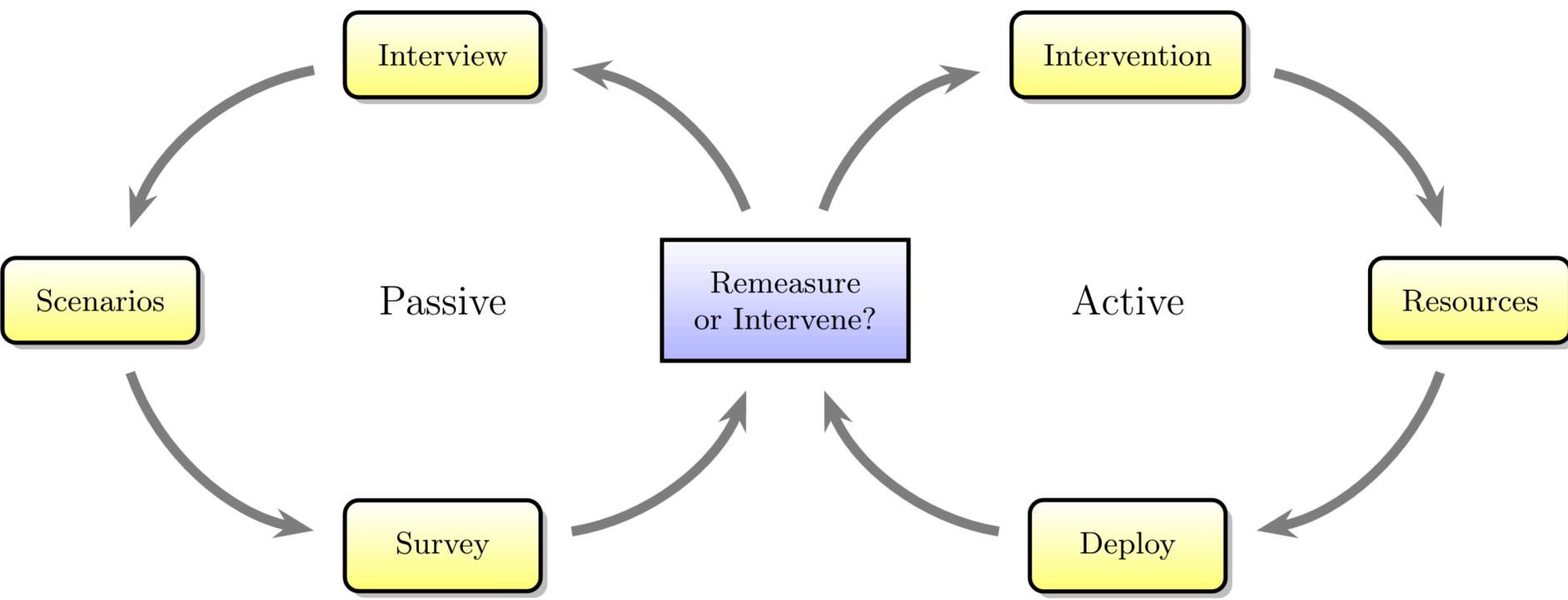
Survey – example attitude question

Jessica is heading toward an unmanned turnstile and notices a man she does not recognise in front of her pass through the barrier by following close behind someone else unfamiliar. The two men are walking close together although they do not appear to obviously be in conversation. The second man is holding a cup of coffee in one hand and his laptop in the other. His ID badge is not immediately visible. Jessica decides to:

A. Follow the man and ask to see his ID badge.

B. Find a security guard at one of the manned turnstiles and tell them what happened.

C. Return to her desk, she sees this sort of thing quite regularly and it is probably because his hands were full that he did not swipe through himself.

D. Do nothing, if he is up to some mischief the security guards will catch him later on.

Survey results – statistical analysis

Business Division	Level 2		Level 3		Level 4		Level 5		τ
	Rank**	Accept**	Rank**	Accept**	Rank**	Accept**	Rank**	Accept**	
Business	0.33**	0.29*	−0.23*	−0.32*	0.10	0.33**	−0.21**	−0.14*	0.61**
Finance & Prof. Services	0.37**	0.24**	−0.12*	−0.23*	0.13*	0.37**	−0.38**	−0.34**	0.59**
Human Resources	0.23**	0.18	−0.21	−0.47	0.14	0.20**	−0.16**	−0.15	0.66**
Marketing & Consumer	0.43**	0.37**	0.12*	−0.15	−0.10	0.29	−0.45**	−0.42**	0.50**
New Business	0.33*	0.32	−0.32*	−0.23	0.19	0.47**	−0.21*	0.04	0.55**
Operations	0.23*	0.14	0.25**	−0.34**	−0.13**	−0.23**	−0.34	0.06**	0.45**
Other	0.30**	0.30**	−0.33**	−0.42**	0.25*	0.27*	−0.22**	−0.38**	0.65**
Sales & Service	−0.31**	−0.23**	−0.03**	0.34**	−0.00**	−0.06**	0.34**	0.12**	0.76**
mean	1.48	1.50	2.13**	2.19**	3.08**	3.98**	3.30**	4.51**	0.62**

Business Division	Scenario	Individualist		Egalitarian		Hierarchist		Fatalist		τ
	Sev**	Rank**	Sev**	Rank**	Sev**	Rank**	Sev**	Rank**	Sev**	
Business	0.52**	0.17	−0.10**	0.59**	−1.18**	−0.53*	0.29	−0.23	0.10	−0.22**
Finance & Prof. Services	0.38**	0.34*	−0.24	0.50**	−0.76**	−0.67**	0.29	−0.16	0.15	−0.19**
Human Resources	0.62*	0.53*	−0.13	−0.09	−0.90**	−0.16	−0.41	−0.29	−0.73	0.08
Marketing & Consumer	0.84**	0.32	−0.74**	0.86**	−0.84**	−0.47*	0.34*	−0.71**	0.18	−0.22**
New Business	0.58	0.59*	−0.58	0.62	−0.39	−0.80*	−0.11	−0.41	0.01	−0.39**
Operations	0.03**	−0.02**	−0.33**	−0.34**	0.38*	−0.40**	−0.39**	0.76**	−0.96**	−0.48**
Other	0.24	0.35**	−0.46*	0.04	−0.53**	−0.26	0.11	−0.13	−0.16	−0.28**
Sales & Service	−0.28**	−0.18**	0.37**	−0.06	0.25**	0.48**	0.10*	−0.24**	0.50**	−0.17**
mean	2.24	2.68**	3.49	2.02	3.76**	2.80*	3.20	2.50**	3.44**	−0.20**

Results overview – maturity levels

- Participants more likely to choose more acceptable options

- 35-39 age group shows lower average level 5 rank than other groups
  - Also ranks level 4 higher than other age groups

- HQ rank maturity level 4 higher than level 5 + rank level 2 significantly higher than other locations

Results overview – behaviour types

- Human resources a *hotspot* - employees choose options independent of assigned severity

- 25-29 and 30-34 *more* Hierarchist than other age groups, 50-54 *less* Hierarchist
  - 30-34 less Fatalist, 50-54 and 55 more so

- HQ and Homeworkers rank Individualist highest

High-level outcomes

- Organisation has very positive security posture
  - Employees pick more acceptable, less severe options
  - Good security practices adopted, even when not required to by technology or policy

- Where friction exists between business and security, approaches predominantly Individualist
  - "Shadow security", relying on own skills and knowledge
  - Hierarchists abide by existing structures; Individualists may identify and solve new challenges

Areas to investigate

- Sales and Service have stronger maturity levels + able to assess severity of options

- HQ ranks maturity level 4 higher than level 5 + Individualist first + absence of Hierarchists
  - Hot-desking policy may factor here
  - HQ constantly reinvents itself with new advances

- 25-34 more Hierarchist, 50+ more Fatalist
  - Younger employees mostly in Sales (fraud exposure)

- Reported to board; resources targeted to these areas

Conclusion

- Scalable surveys based on rich interview data
- Multi-purpose questions provide multi-dimensional view of employee security
- Organisation used results to target interventions
- Scope to adapt scenarios across companies
- Can explore potential for managers and employees to find collaborative solutions