Measuring the Success of Context-Aware Security Behaviour Surveys

Ingolf Becker, Simon Parkin, Angela Sasse
University College London
i.becker@cs.ucl.ac.uk

Background

- To gather large scale data sets on employee behaviour and attitudes via scenario-based surveys
- Survey questions are grounded in rich data drawn from interviews, and probe perceptions of security measures and their impact
- 2 organisations, A & B
  - Large multinationals
  - 118 and 85 interviews
  - 1486 and 641 responses
  - 516 and 195 comments
- Findings of the analysis published in [4, 7], and related work in [8, 21, 22]

A scenario

Concerned about the safety of his current work, Shamal decides to back up his data, some of which is confidential. As he uses his own laptop under the 'bring your own device' scheme, he usually stores all his work on his drive on the central server but he wants to have a second copy just in case something happens or he loses connectivity to the company network.

He thought about using one of the common drives but none of the ones he regularly uses have sufficient space.

Individualist:	Create a local copy on the hard drive of your BYOD laptop, it is the only machine you work on so you know it will be safe and this ensures you will always have access to it if needed.
Egalitarian:	Use a common drive that you used for an old project and still have access to, as your credentials were never revoked. It has enough space although you do not know who manages it now.
Hierarchist:	Use an online service, such as Dropbox, to store the data as it is more under your control.
Fatalist:	Back your work up onto a USB stick – you have ordered an encrypted one but while you wait for it to arrive you use a personal stick you have to hand.

A: Attitude Types & Behaviour Types

1. Discount suspicions, cause no bother, passive,
2. Report suspicions but take no direct action,
3. Take direct action through official channels,
4. Take direct personal action against the threat.

1. Prepared to perform insecure acts to maximise productivity,
2. Show a minor priority for work over security when the two conflict,
3. Passive, expects others to take the initiative to ensure security,
4. Tries to remain secure wherever possible.

B: Maturity Levels & Behaviour Types

1. Is not engaged with security in any capacity,
2. Follows security policy only when forced to do so by external controls,
3. Understands that a policy exists and follows it by rote,
4. Has internalised the intent of the policy and adopts good security practises even when not specifically required to,
5. Champions security to others and challenges breaches in their environment.

Individualists rely on themselves for solutions to problems,

Egalitarians rely on social or group solutions to problems,

Hierarchists rely on existing systems or technologies for solutions to problems,

Fatalists take a ‘naive’ approach to solving problems, feeling that their actions are not significant in creating outcomes.

Our work

- Is the mapping between answer options and types correct?
- Do the participants relate to the scenarios and their answer options?
- Has our survey design improved?

Free text responses

- 516 and 195 in A & B
- Coded for Attitude/Behaviour/Maturity types by 2 annotators
- "*Shamal needs to find out who manages the common drive now, and whether the company authorises use of Dropbox and personal USB sticks, before using any of those options.*"
- "*This scenario could easily be avoided by providing sufficient space on the common drives.*"

Agreement tables

Coder B	Coder A T1	T2	T3	T4
T1	4	3	0	0
T2	0	36	2	15
T3	0	2	59	1
T4	0	0	1	32

Rank	Coding type T1	T2	T3	T4
1	2	6	84	3
2	5	26	22	10
3	2	19	12	34
4	2	43	6	34

Krippendorff's α with 95% confidence intervals

Question	#	Mapping α	Coder's α
Q4	40	0.21 ± 0.02	0.29 ± 0.02
Q5	34	0.35 ± 0.02	0.02 ± 0.03
Q6	2	-0.33 ± 0.76	0.00 ± 0.67
Q8	29	0.30 ± 0.04	0.94 ± 0.02
Q10	37	0.23 ± 0.03	0.73 ± 0.02
Q1	155	-0.03 ± 0.01	0.77 ± 0.00
Q2	137	0.43 ± 0.01	0.91 ± 0.00
Q3	12	0.33 ± 0.08	0.38 ± 0.10
Q7	25	0.24 ± 0.03	0.13 ± 0.04
Q9	45	0.13 ± 0.02	0.76 ± 0.02

Question	#	Mapping α	Coder's α
QID	33	0.27 ± 0.02	0.85 ± 0.02
QCDP	53	0.31 ± 0.01	0.38 ± 0.02
QT	22	0.24 ± 0.04	0.34 ± 0.05
QSD	27	0.53 ± 0.02	0.47 ± 0.04
QRM	12	0.27 ± 0.07	0.42 ± 0.07
QVPN	23	-0.09 ± 0.03	0.37 ± 0.04
QFS	18	0.19 ± 0.05	0.46 ± 0.05
QCC	7	0.38 ± 0.13	0.75 ± 0.21

Appropriateness & Severity

- 5-point Likert scale from "*Not acceptable*" to "*very acceptable*" / "*Not severe*" to "*very severe*"
- Either *Appropriateness* or *Severity* for each answer options
  - Ideally all options similarly highly acceptable / equally severe
- "*Acceptability of failing to complete the task*" on Behaviour type scenarios
  - Ideally identical for all scenarios

Appropriateness results

- Range 0 -> 1
- Std of mean greater in A than B
- Participant's first choice highly appropriate
  - lower in B than in A though

Question	#	Mean		1st choice	
		mean	std	mean	std
Company A					
Q4	374	0.626	0.120	0.923	0.195
Q5	820	0.570	0.110	0.925	0.161
Q6	137	0.427	0.138	0.821	0.321
Q8	364	0.529	0.085	0.983	0.084
Q10	903	0.483	0.082	0.917	0.185
Company B					
QID	152	0.488	0.122	0.778	0.316
QCDP	456	0.508	0.108	0.893	0.220
QT	164	0.499	0.095	0.873	0.252
QSD	292	0.546	0.118	0.939	0.181

Severity and acceptability of failing to complete the task

- A are more likely to see a dilemma between security and other demands in their assigned questions
- Severity scores lower in A, but less varied

Question	#	Failing		Std of Severity	
		mean	std	mean	std
Company A					
Q1	903	0.281	0.307	0.270	0.128
Q2	893	0.270	0.296	0.239	0.123
Q3	137	0.394	0.340	0.271	0.122
Q7	291	0.458	0.393	0.296	0.144
Q9	374	0.668	0.449	0.274	0.123
Company B					
QRM	152	0.196	0.312	0.377	0.101
QVPN	152	0.439	0.370	0.323	0.120
QFS	164	0.430	0.318	0.297	0.114
QCC	292	0.240	0.410	0.182	0.163

Conclusions

- We explored the validity of the scenario mapping
  - The surveys help target interventions
- Some of our scenarios are valid, and we know how applicable they are
  - i.e. what to ignore, where to focus
- There is measurable progression in the survey design between A & B.
- Advice: Open questions are extremely useful!