Finding Security Champions in Blends of Organisational Culture

Ingolf Becker, Simon Parkin & M. Angela Sasse

{i.becker,s.parkin, a.sasse}@cs.ucl.ac.uk

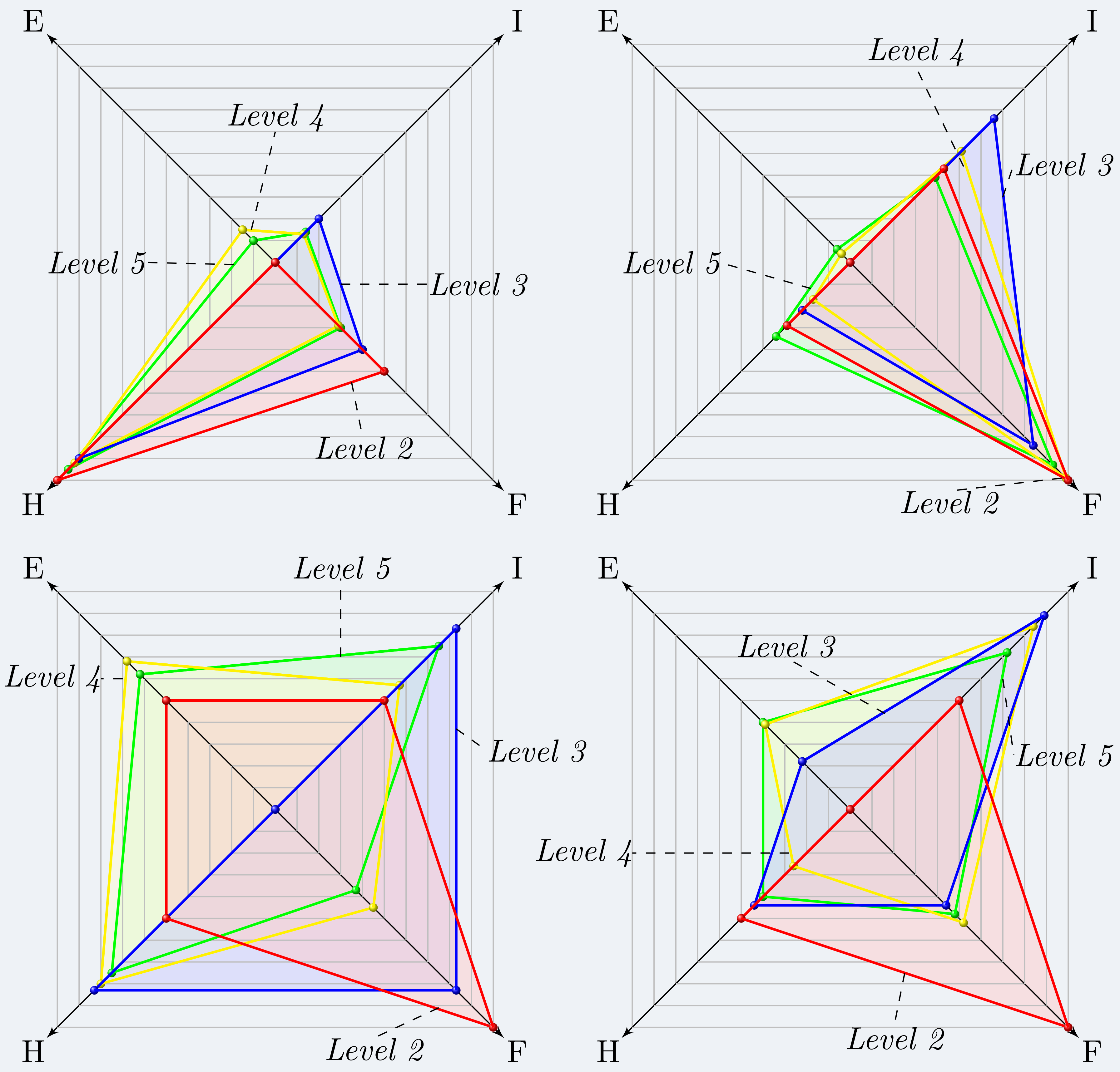
Overview

- Organisations use security policies and procedures to define how employees should ‘do their bit’ to protect the organisation and themselves.
- Policies assume a good fit with business processes and employees’ regular tasks. However, if the day-to-day reality of people’s jobs is not considered, policies can instead cause friction.
- By including employees, it can be easier to identify where policies cause friction, are ambiguous, or just do not apply to business processes. Doing so brings the organisation closer to *workable* security.
- Currently, involving employees in security leads to **security champions** as representatives of policy, rather than representatives of *employees’ security needs.*
- We have conducted secondary analysis [1] of 608 surveys deployed in a large partner organisation. Scenario-based survey questions are situated in realistic security dilemmas, to explore the role of security in employees’ working lives.
- Involving a diverse range of employees as ‘bottom-up’ agents to improve policy can complement existing ‘top-down’ policies. Employees must however be able to question policy; security behaviours and attitudes to policy can act as measures for how security is currently experienced and how to craft security awareness initiatives.

Method

- Each survey is personalised, containing four scenario-based questions based on situations identified in prior *in-depth interviews*;
- Each question offers four actions, with different security, social and productivity implications;
- Responses indicate individual **Behaviour Type** or **Maturity Level**;
- Combined distributions of Behaviour Types vs Maturity Levels indicate how security is approached in day-to-day work activities (see “Results”);
- We communicate this analysis for specific divisions in **Kiviat diagrams**;
- We also analyse 189 **voluntary comments** (see “Free Text Responses”).

Results: Behaviour Types + Maturity Levels



Kiviat diagrams of distributions of behaviour types (axes) for maturity levels (edges) for (clock-wise starting top left) Sales & Services, Operations, Finance and Business divisions. **Core themes:**

Diverse responses to security: The composition of Behaviour Types and Maturity Levels varies strongly between Divisions, e.g. in the Finance division individuals at Level 2 are predominantly *Fatalist*, but switch to *Individualist* at higher levels of maturity and take more personal control of security;

No one-size-fits-all: Effective engagement with employees would ideally consider such variations (e.g., the large number of Level 5 *Hierarchists* in Sales & Services may already know policy, compared to the diverse behaviour types present in the Business division which would require a range of approaches to engage everyone, see diagrams above).

Policy can be informed from the ‘ground up’: employees can offer additional insights about their localised experience of security (see “Free Text Responses”).

Behaviour Types, informed by Adams [2]

(I)ndividualists rely on themselves for solutions to problems.
(E)galitarians rely on social or group solutions to problems.
(H)ierarchists rely on existing systems or technologies for solutions.
(F)atalists take a ‘naive’ approach, that their own actions do not create outcomes.

Maturity Levels, as defined by Beautement et al. [3]

These maturity levels describe the relationship the individual has with the organisation and its security policy:

1 – Uninfluenced: Security behaviour is driven by personal knowledge.
2 – Technically Controlled: Technical controls enforce policy compliance.
3 – Ad-hoc Knowledge and Application: Shallow understanding of policy. Knowledge absorbed from surrounding work environment.
4 – Policy Compliant: Comprehensive knowledge and understanding of policy, and willing policy compliance.
5 – Active Approach to Security: Actively promote and advance security culture, carrying the intent of policy into work activities to support both security and business.

Free-Text Responses

Voluntary responses give additional insights into how security fits into local practices:

Sales and Service; when considering sharing data insecurely:

> *“The employee is put in a no-win situation. If the business permit flexible working then the only allowable option here is for the data not to be sent.”* (*Hierarchist*, Level 3 / ‘Ad-hoc’)

Business; when contemplating authorisations:

> *“Assuming the colleagues are from the same team and have the same clearance then they are equally trustworthy.”* (*Fatalist*, Level 2 / ‘Ad-hoc’)

References

1. Becker, I., Parkin, S. & Sasse, M. A. in. EuroUSEC ’17 (Internet Society, Paris, France, 2017), 11. doi:10.14722/eurousec.2017.23007.
2. Adams, J. “Risk and morality: three framing devices”. *Risk and morality,* 87–106 (2003).
3. Beautement, A., Becker, I., Parkin, S., Krol, K. & Sasse, A. in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (USENIX Association, Denver, CO, 2016), 253–270.

Acknowledgements

We would like to thank the participating organisation for their assistance.
UK EPSRC Grant no:
EP/G037264/1 & EP/K006517/1