Finding Security Champions in Blends of Organisational Culture

Ingolf Becker*
University College London
i.becker@cs.ucl.ac.uk

Simon Parkin*
University College London
s.parkin@ucl.ac.uk

M. Angela Sasse
University College London
a.sasse@ucl.ac.uk

***Abstract*—Security managers define policies and procedures to express how employees should behave to 'do their bit' for information security. They assume these policies are compatible with the business processes and individual employees' tasks as they know them. Security managers usually rely on the 'official' description of how those processes are run; the day-to-day reality is different, and this is where security policies can cause friction. Organisations need employees to participate in the construction of workable security, by identifying where policies causes friction, are ambiguous, or just do not apply. However, current efforts to involve employees in security act to identify employees who can be local representatives of policy — as with the currently popular idea of 'security champions' — rather than as a representative of employee security needs.**

Towards helping organisations 'close the loop' and get input from employees, we have conducted employee surveys on security in the context of their specific jobs. The paper presents results from secondary analysis of one such survey in a large commercial organisation. The analysis of 608 responses finds that attitude to policy and behaviour types — the prevailing security cultures — vary greatly in the organisation and across four business divisions examined in further detail. There is a role in contributing to the effectiveness of security policies not only for those who follow policy, but also for those who question policy, socialise solutions, or expect security to justify itself as a critical part of their productive work. This demonstrates that security champions cannot be uniform across the organisation, but rather that organisations should re-think the role of security champions as diverse 'bottom-up' agents to change policy for the better, rather than communicators of existing 'top-down' policies.

I. Introduction

Security managers in large organisations will define policies to encourage a shared approach to IT security for all members of the organisation. Policies can refer to a mix of procedures and technical controls, which employees in the organisation will interact with, and are expected to use according to the rules of the policy.

The promotion of *security champions* is seen as a way to find local representatives who can promote and monitor security policy at a local level, acting as an extension of company's security management team [12]. However, security champions may only be effective in this way if the policy itself is workable [6].

This brings us to examine the role of policy effectiveness from the perspective of security usability. Employees may feel that policy is too cumbersome, that it actually asks the impossible of them, or that the relevance of security mandates to their work is unclear [16]. This can then lead to deliberate or unwitting non-compliance, and workarounds to prescribed security processes. We look to explore the way that the organisation can engage employees, to give them a role in identifying and solving shortcomings of security policy.

We build on a prior security behaviour survey [4] deployed at a large partner organisation (employing thousands of staff). The survey presented scenario-based questions to 600+ employees, where scenarios and related security dilemmas were based on in-depth interviews with employees at the same organisation. Interview responses were crafted into survey questions grounded in the realities of working with the security procedures and technologies in the company. The survey was designed so that an employee's responses would indicate a combination of behaviour type and security attitude. Distinct behaviour types included *Egalitarian*, *Fatalist*, *Individualist*, and *Hierarchist* (based on work in the area of risk culture [1]). Security attitude followed a scale defined within a security behaviour maturity model; the model moves from an employee being 'uninfluenced' by security policy, up to an 'active approach to security'.

We analyse the 608 survey responses by combining the two dimensions of security behaviour and security maturity as a representation of individual security posture and the wider security culture. We analyse responses across the organisation and in four specific business divisions (Sales & Services, Operations, Business, and Finance & Professional Services). Analysis allows us to draw conclusions through aggregation and statistical validations for larger business divisions and the organisation as a whole. As part of the survey 267 participants chose to elaborate their choices by giving additional free-text responses, not previously analysed. We combine both the two-dimensional security culture dataset and the free-text responses, conducting a novel analysis of the dependencies between maturity levels

*Authors contributed equally.

EuroUSEC '17, 29 April 2017, Paris, France

http://dx.doi.org/10.14722/eurousec.2017.23007

and behaviour types in the organisation. Such an approach can identify local pockets of security expertise and indicate how to engage with those employees to create workable security solutions.

We find that there is a role in the development of effective — and secure — organisation security policies for employees who not only follow and promote policy, but also those who: question the adequacy of policy, or challenge it through finding alternative solutions; socialise security solutions through engagement with peers, and; those who would expect security to justify itself by being a critical part of their productive work. These findings demonstrate that organisations can find a range of security champions if they engage with distinct viewpoints on policy. We find that investing solely in *security champions* who rigidly follow policy misses opportunities to involve the wider organisation in the shaping of effective and workable security. Separate business divisions exhibited different mixes of both behaviour-type and attitude-level; employee feedback identified local challenges and framed alternative security solutions in a manner that could be related to the expectations of policy.

The paper is arranged as follows: Section II discusses related work and the motivation for the analysis described here. Section III summarises the survey methodology and describes the analysis method used for exploring the different roles a security leader or champion might have. Results of the analysis are described in Section IV, followed by discussion of the findings in Section V, with conclusions and future directions closing the paper in Section VII.

II. Background

A. Related work

A number of works have explored factors and activities within organisations which can influence individual compliance with security policies, implying that the act of declaring a security policy does not in itself guarantee compliance. A survey of works in this area by Sommestad et al. [26] implies that factors such as perceived behavioural control and the types of training delivered around policy are reliable predictors of compliance, summarising that for anticipating compliance constructs for values and norms are more effective than systems around sanctions and rewards. Here we consider ways to engage with characteristics of organisational and security culture at scale, toward aligning individual security responsibility and the accessibility of provisioned security systems. In this regard, some works consider the role of 'security champions' as role models within distinct groups of employees, as examples that others can follow.

Connolly et al. [8] explore the role of deterrent factors in organisational security and the minimisation of 'human error'. The authors examine how organisational culture, national culture, and security countermeasures can influence employee security behaviours. Where employees are encouraged to make local decisions and voice their opinions within the organisation, they are more likely to comply with security policies and procedures. Excluding employees from the conversation around security encourages non-compliance. Compliant behaviours may also rest on secure working being an integral value of the organisation, and the visible presence of countermeasures such as policy and security training. Here we explore how different security cultures can be engaged for their strengths, alongside the provision of controls and the promotion of security skills.

Posey et al. [22] consider the differences between information security professionals and other employees in organisations, in terms of their perceptions around security. Security professionals consider workarounds by employees as a threat to the organisation, where here we consider whether such activities — essentially, deviation from what professionals expect — are an opportunity for the organisation to develop security which integrates naturally with business processes. Posey et al. found that both security professionals and other employees were concerned about careless behaviour threatening the security of the organisation, yet also noted the potential impact of improperly provisioned technologies. It was found that security professionals underestimated the negative impact that security infrastructure had upon employees, and overestimated employees' tendency to distance themselves from security. The authors note that future solutions could act to unify the differences in views between security professionals and employees, rather than determining which group is 'correct'. In their work, perceptions are framed around responses to security events, where here the survey used to drive analysis asks participants to choose amongst responses to scenarios; both the scenario and the range of responses are based on self-reports from employees.

Hsu et al. [14] examine extra-role security behaviours — those not specified in the information security policy recognised by the organisation. The influence of social controls, rather than formal controls alone, is also explored. The authors asserted that employee involvement in the development of information security policy is critical, given that 'involvement' is a foundational social control. The authors also found that maintaining a mix of formal and social controls can benefit an organisation. Here we explore whether variations of following and challenging of policy can be blended to benefit an organisation. Driving compliance through formal controls only is seen to stifle extra-role security behaviour. Combinations of security cultures — security leaders — may be necessary to be able to encourage both proactive security behaviour and allegiance to the fundamentals principles of security policy.

Johnston et al. [15] deploy a scenario-based survey, to 242 individuals with experience of using computers and working in organisations with security procedures, to examine how personality traits and derived perceptions of situational factors (such as sanction certainty and threat severity) determine an individual's inclination toward policy violation. The study focuses on specific dispositional factors, those being stability and plasticity, and how these meta-traits interact with the derived perceptions of sanctions, threat appraisal and coping appraisal. Rather than arguing in terms of dispositional factors, we use scenarios as an experimental construct, to explore participants' perceptions around security. Individuals exhibiting Stability may con-

form with rules, whereas those exhibiting Plasticity may take more risks but only when there is seen to be a benefit in doing so. The authors note that differing forms of persuasive engagement may be necessary to target different personality types, but that controls such as sanctions must be seen as equally fair to all.

Furnell & Rajendran [11] develop a model of the influences on security behaviour, relating *workplace-based influences* and *workplace-independent influences*; colleague behaviour is an element of workplace interactions, for instance. By considering *situational factors*, the authors note that factors such as fatigue and the perceived importance of the primary task can impact the enactment of security behaviours. It is further noted that intention to follow security policy can be separate from factors such as the usability of security controls. Based upon a focus group exercise with a number of professionals, disciplinary procedures are seen as a strong influential factor for compliance, but so is colleague behaviour. Here we explore whether employees and groups of employees, experiencing policy in practice, can actively contribute to the identification and removal of barriers which may otherwise undo any good intentions towards security.

Similar work to [11], Gabriel & Furnell [12] explore the characteristics of a 'security champion', positing that *awareness*, *motivation*, and *compliance* are foundations for defining a security champion, and further that the personality of a security champion rests primarily on increased imagination and minimising any tendency toward immoderation (i.e., fixation on short-term gains rather than long-term consequences). Other factors such as Emotionality, Anxiety, and Altruism were seen as positive elements of a security champion, where here we discuss behaviour types which frame characteristics like these in terms of security culture and the connection to the rest of the organisation. We consider with our security maturity levels that employees have to balance their security competence with a primary task, and that being a security champion may be about finding workable security that allows them to complete their primary, productive tasks in a secure way (for instance limiting the need to make short-term compromises by avoiding cumbersome security controls).

Beris et al. [6] identified sixteen theoretical behaviour types based upon the analysis of semi-structured interviews with staff in large organisations. The authors distinguish between *risk understanding* and *affective security*. Risk understanding is regarded as an individual's competence, and affective security the person's emotional response to security. One of the theoretical behaviour types identified by Beris et al. is a 'security champion', someone who is motivated to engage with security while also understanding the risks relevant to their work. An awareness of relevant risks is seen to allow security champions to repurpose their skills to address situations not directly or explicitly addressed by policy; this suggests potential in engaging with staff to shape policy for the better.

B. Motivation

We combine insights from related work around security policy compliance and organisation-based employee engagement with prior work exploring human factors and usability of security. This combination frames a set of new challenges for anyone seeking to deliver effective security policy compliance in larger organisations. These challenges guide our analysis of the dynamics between an organisation's security function and its employees. We discuss the benefits of employee participation in the evolution of security policy, and how security champions can enable this process.

Challenge 1: There is evidence that non-compliance with policy is common, and that it occurs for reasons other than ignorance of policy. A security champion must be able to question policy and negotiate workable solutions, rather than just communicate policy.

Security policies are *designed* to represent how policymakers believe employees should behave [16]. Similarly, a focus on enforcing compliance perpetuates a value gap between security managers and the wider organisation [2]. Pfleeger et al. [20] consider levers for behaviour change based on research in economics, psychology, and sociology, and conclude that values are the crucial 'anchoring points' on which both sides must agree for behavioural norms — such as policies — to be accepted. There can be many dimensions to these values, as defined in Jonathan Haight's 2012 seminal work [13], such as *Care vs. Harm* and *Liberty vs. Oppression*.

The organisation's standpoint on these values must be clear, so that employees can accept that they have to 'do the right thing' by those values, that is, act in line with the behavioural norms anchored in those values. This is generally part of *psychological contracts* that Human Resources departments develop and promote [9]. That means, for instance, that employees are expected to care about the organisation rather than harm it, and show loyalty to the organisation when someone asks them to reveal confidential information in return for some form on inducement. But as in all functional relationships, there needs to be reciprocity — the power of those values depends on visible evidence that the organisation demonstrably cares about employees and is loyal to them. Pfleeger et al. stress that even constant appeal to values cannot overcome lack of security hygiene, a fact summarised by a UK government agency as *"if security doesn't work for people, it doesn't work"*[1].

Security champions then can only promote values and associated policies if security policies are (1) workable, and (2) can be understood as part of *not harming the organisation* in the context of preventing information security risks [6]. An employee faced with an ineffective policy that undermines organisational productivity may resort to *shadow security* [17], getting the job done while securing against risks they know. We know from previous research on workforce interactions with IT and IT security [17], [18] that organisations can learn from the way that employees alter security to fit with their productive tasks. An employee championing security is someone whose efforts are driven by the tenets of the organisation's security policy, but who

[1] "People: The Strongest Link", https://www.ncsc.gov.uk/information/people-strongest-link

may not necessarily be restricted to the policy as a hard set of rules.

Challenge 2: The organisation must reflect on the existing security policy from the perspective of employees, before determining the kind of security champion that the organisation needs in order to engage employees effectively.

Bulgurcu et al. [7] posit that the *quality* and *fairness* of an information security policy, as perceived by employees, are factors in employee security compliance. 'Security hygiene', as defined by Pfleeger et al., is a combination of workable security habits that also delivers effective risk management to the level required by the organisation [20]. This can only be achieved if employees are involved in shaping policy that they can adhere to. Otherwise, employees may wonder why policies or specific rules are necessary, or abandon policy at the first sign of any friction or contradiction with other goals [16].

Posey et al. [22] found in their interview-based study that employees saw compliance with policy as adding excessive effort to the primary task, stifled the general working environment, caused frustration or seemed difficult — and potentially irrelevant — even with good intentions toward security. Security policies and employee work activities must then be considered as part of the same conversation, to understand how security fits with the existing environment from the 'ground up' rather than exclusively 'top down'.

Challenge 3: A champion of workable security cannot be a single person. Developing effective security requires a mix of individuals who interpret, question, follow, and promote security in different parts of the organisation.

Within large organisations, an individual employee's approach to resolving friction with security may be determined by not only their own inclinations but also their interactions with others around them [4], [6]. Not every employee needs to be a 'security champion' but can still be a useful resource for security, as for instance there may be individuals who have knowledge of the risks affecting the business, but who do not have the skill-set of a dedicated security expert [6].

Equally, there can be employees for whom security is not a natural part of the job, but a *levy on productivity*. This can inadvertently perpetuate the myth that there is a 'tradeoff' between security and productivity [24]. In the realm of safety, Dekker [10] deprecates the oft-expressed desire of experts to *'get people engaged'*. He argues that the problem is not that 'operational people' need to engage with safety, but that *"safety experts are not engaged with operational people"*. Dekker further refers to the work of Pink [21] in that motivation to be safe involves *autonomy, mastery*, and *purpose*. These elements together allude to a larger purpose than safety, best served with an open dialogue around workable behaviours and meaningful interaction between experts and non-experts. Similar arguments may be applied to security.

Employees who rigidly follow the rules are powerless in situations where rules are unwritten or unclear. Organisations who want employees who can be a 'hero' who keeps the organisation secure in unanticipated circumstances need to enable them by supporting individual and collective awareness of the risks and an understanding of actions that could mitigate those effects [23].

Where security is important to the business, it will enter the discourse of discussions between peers, who may approach security as a social responsibility. Those who are firmly *part of the organisation* — but not necessarily 'on board' with security — are nonetheless part of the 'pulse' of the organisation. A proactive security champion or network of champions *will* find gaps in policy and process, so the organisation must have the capability to approach shortcomings in policy. This can nonetheless be done in a way that aligns with the *intent* of the security policy, where this is most naturally achieved through alignment of security with the goals of the business.

III. Methodology

The methodology described here builds on a prior security behaviour survey exercise with a large partner organisation [4]. We re-interpret the survey responses and examine the additional free-text comments that participants provided, in line with the security engagement challenges outlined in Section II-B.

A. Security behaviour survey development

The overarching methodology described in [4] is a multi-stage process that begins with qualitative interviews themed around security, conducted with a cross-section of employees. Outcomes ground security in the work environment, motivating targeted, realistic survey questions that are relevant to large parts of the organisation. This then serves as a snapshot of the security culture of the organisation across dimensions such as business function, location, and employee age. It is designed to provide researchers with a repeatable and scalable data gathering process for capturing security behaviours of individuals and groups.

B. Attitude level and behaviour type scenarios

The survey consists of scenario-based questions which present a security workplace dilemma to participants. The available options correspond to *attitude levels* and *behaviour types*, which where attitude and behaviour were analysed independently. The distinction between attitude-level and behaviour-type is similar to the work of Beris et al. [6], who compare *risk understanding* and *affective security* (or 'emotional stance') to identify groups of employees with skills and expertise that are potentially beneficial to organisational security. Here we combine the dimensions of attitude and behaviour, using them together to explore whether distinct security cultures exist in an organisation and different business divisions.

The behaviour types captured in the survey are informed by an examination of risk culture by Adams [1], and are summarised as:

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.

Attitude levels correspond to a security behaviour maturity model underpinning the survey, as described below (and in further detail in [4]).Each level describes the relationship the individual has with the organisation and its security policy, and in turn the role played by the whole organisation and the employee in making secure working viable. Those at lower levels engage with security as and when necessary, and at higher levels employees are local security experts:

Level 1: Uninfluenced Security behaviour is driven by personal knowledge, instincts, goals and tasks, with no influence from any security infrastructure.
Level 2: Technically Controlled Technical controls enforce compliance with policy, outside of which employees fall back on personal security rules.
Level 3: Ad-hoc Knowledge and Application Employees adhere to a shallow understanding of policy. Security knowledge is absorbed from the surrounding work environment rather than from policy.
Level 4: Policy Compliant Comprehensive knowledge and understanding of policy, and compliance with it, even when not required to. Employees at this level can be considered as role models and guides for security culture within the organisation.
Level 5: Active Approach to Security Employees actively promote and advance security culture. The intent of policy is carried into work activities as a supporting capability of the organisation. The values within security policy relative to organisation goals are understood, driving respect for both security and business processes.

Broadly speaking, individuals at Level 1 will not be found in an organisational environment where a minimum infrastructure typically requires employees to use a registered username and password to access IT resources. Survey responses here then utilise Level 2 and upwards.

C. Free-text survey responses

A participant could provide additional comments on each question, scenario and the available options, via an associated free-text field in the survey. The security-work dilemmas and answer options were based on a large-scale interview study with employees at the same organisation, and included an element of non-compliance or an implicit cost that had been described and justified by multiple interviewees. Participants may then feel that there are other solutions available, informed by their local work environment (and which the security function may not be aware of). There was no direct incentive associated with providing additional comments; where employees provided further comment they were in effect being proactive toward security.

D. Source data

608 complete survey responses were analysed. The survey captured business division, but also each participant's main place of work and age. We focus our analysis on business division, since the security mechanisms and rules that an employee interacts with vary with roles. Surveys were distributed to seven business divisions (where one was a group of smaller divisions) across a larger number of physical locations. The majority of responses originated from Sales & Services (292), followed by Operations (152). The number of responses was approximately proportional to the size of each of the divisions, but we were unable to further control the sampling within each division.

Demographic information (including business role) was captured at the start of the survey process and used to build a set of 3-4 scenario-based questions for each respondent based on their responses and split between attitude-level and behaviour-type questions.

We complement analysis of the combined attitude-level and behaviour-type with examination of the free-text responses. These responses also illustrate the kind of information that security managers could use in policy formulation should they involve employees — who may have differing relationships with organisation security — more directly in the process. This relies on security managers believing that employees may adopt a range of security behaviours in the workplace which are within and outside of policy, but that this may be done in response to practical challenges in fitting policy and other security mechanisms to the business more effectively (as with 'shadow security' behaviours [18]).

IV. Results — Culture Analysis

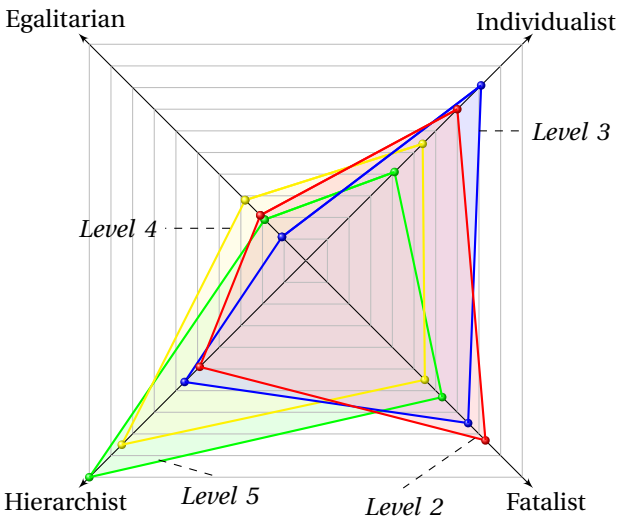

Fig. 1. Kiviat diagram of distributions of behaviour types for maturity level 2 (red), 3 (blue), 4 (yellow), 5 (green) for the entire organisation.

As described in Section III, we cross-analyse behaviour types with attitude levels for groups of employees. To

support analysis and to visualise the data, we employ Kiviat diagrams. Figure 1, for example, describes the distribution of behaviour types and attitude levels for the entire organisation. These diagrammatic representations expose the interplay between different behaviour types at varying levels of attitude toward policy, where together these varieties can help to strengthen the security posture of the organisation as a mapping of the reach and influence of policy. As we examine different subsets of the organisation, we can compare the security culture in each group to understand better how employees can be engaged to improve security effectiveness.

Figures 1 to 5 all have four tetragons plotted, one for each attitude level. The diagonal axes represent the fraction of participants that exhibit each personality type, with the centre of the diagram being 0%. To aid readability, Kiviat plots are scaled to fill the entire chart. Hence, each corner of the tetragon represents the fraction of participants of that attitude level that exhibit the behaviour type of that diagonal. As an example, for the case of Figure 1, the blue tetragon represents participants at attitude Level 3 ('Ad-hoc Knowledge and Application'). Of these, 4.5% (4 employees) exhibit as *Egalitarian*, 36% (29 employees) as *Individualist*, 34% (27 employees) as *Fatalist* and 26% (20 employees) as *Hierarchist* behaviour types. This distribution is very different to Level 5 attitude types, where 45% (212 employees) of participants belong to the *Hierarchist* group.

The quotients of participants labelled with each behaviour type and attitude level can be found in Table I. While only a minority of participants exhibit attitude Levels 2 and 3, the variations between different divisions remain strong enough for detailed analysis. The Kiviat diagrams illustrate the relationship that employees may be having with the IT-security infrastructure around them, knowingly or unknowingly, as part of their working lives. These interactions may be the result — or the root cause — of their behaviour type, where security-related skills are also a mediating factor.

It is interesting to note the difference in distributions of behaviour types for different attitude levels. *Individualists* have a larger proportion of lower attitude levels, and *Hierarchists* emerge at the highest level, Level 5 ('Active Approach to Security', as in Section III-B). Referring to the attitude levels, there is a disparity between Levels 2-3 and Levels 4-5, which immediately suggests not just that distinct approaches to employee engagement would be needed, but that the messaging would have to be crafted to match the relationship that employees have with security and security policy.

The strongest security attitude in the organisation overall (Figure 1) is portrayed predominantly by *Hierarchists* and *Fatalists*. The *Hierarchists* are akin to the idealised 'security champion' (as we identified in the literature review in Section II), someone who follows the rules and has security skills to support them (being mostly at attitude Levels 4 and 5). The limited representation of *Egalitarian* behaviours would suggest that individuals respond to security challenges in isolation (perhaps because of, or as the cause of, the aforementioned barrier to working with policy). The 'champions' the organisation may need most may then be team leaders or others who can bring people together and motivate them through social activities and interactions. These individuals do not need to have a high security attitude level — most employees are at a high attitude level already (Table I).

Behaviour type	Level 2	Level 3	Level 4	Level 5
Individualist	1.6%	4.8%	10.7%	14.1%
Egalitarian	0.5%	0.7%	5.6%	6.7%
Hierarchist	1.2%	3.3%	16.8%	34.9%
Fatalist	2.0%	4.4%	10.9%	21.9%

TABLE I. ABSOLUTE PERCENTAGES OF BEHAVIOUR TYPES COMPARED WITH ATTITUDE LEVELS

We also examine a number of specific business divisions/units in the organisation. This allows us to compare security practice in different working environments in a large and complex organisation.Business divisions in a large organisation may differ in security culture to the point where security champions need a different set of skills and strengths to support protection of the overall organisation.

Behaviour type	Level 2	Level 3	Level 4	Level 5	Total
Individualist	2.01%	8.72%	20.81%	25.50%	42.95%
Egalitarian	3.33%	0.00%	15.00%	26.67%	36.67%
Hierarchist	0.78%	1.17%	8.98%	20.70%	24.61%
Fatalist	2.48%	4.46%	10.40%	17.82%	32.18%

TABLE II. RESPONSE RATES TO FREE-TEXT RESPONSE QUESTIONS BY BEHAVIOUR TYPE AND ATTITUDE LEVELS

To support analysis, we also refer to free-text responses for the scenario-based questions (where this was optional for participants, as described in Section III-C). The response rates for optional comments are captured in Table II. We see that response rates generally increase with security attitude level for all behaviour types. That *Hierarchists* and *Fatalists* make fewer comments, which is in keeping with their behaviours — not questioning rules, either because they adhere strictly to the policies or because they consider security to be 'somebody else's job'. When discussing specific business divisions in the following sections, we refer to free-text responses that illustrate the qualities of different kinds of approaches to organisational security. Alongside each quote the participant's behaviour type and attitude level are included (as classified by their responses to scenario questions, see Section III-B). Quotations allude to aspects of security that already have their champion or heroic deeds which save an otherwise unworkable situation, in turn illustrating the benefits that employee input can bring to the security culture of the organisation.

To support analysis, we focus on the four largest divisions in the organisation: Sales and Services (292 participants, Figure 2), Operations (152, Figure 3), Business (33, Figure 4), and Finance & Professional services (47, Figure 5).

A. Analysis — Sales & Services division

Figure 2 shows the distribution of behaviour types for each attitude level in the Sales & Services division. The starkest difference compared to the organisation as a whole (see Figure 1) is that approximately 63% (248 employees)

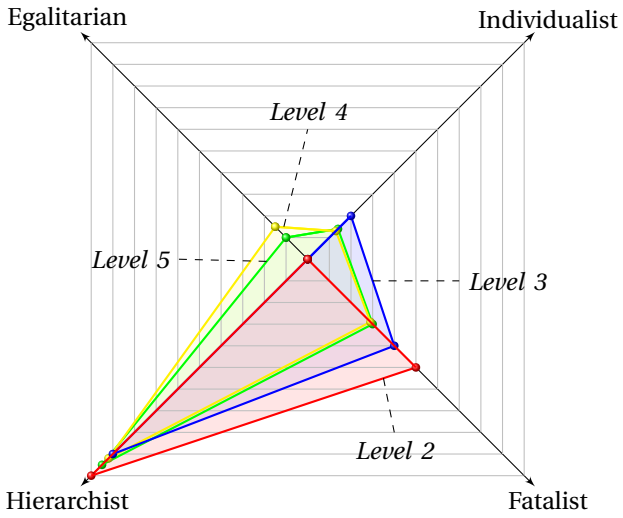

Fig. 2. Kiviat diagram of distributions of behaviour types for maturity level 2 (red), 3 (blue), 4 (yellow), 5 (green) for the Sales & Service division.

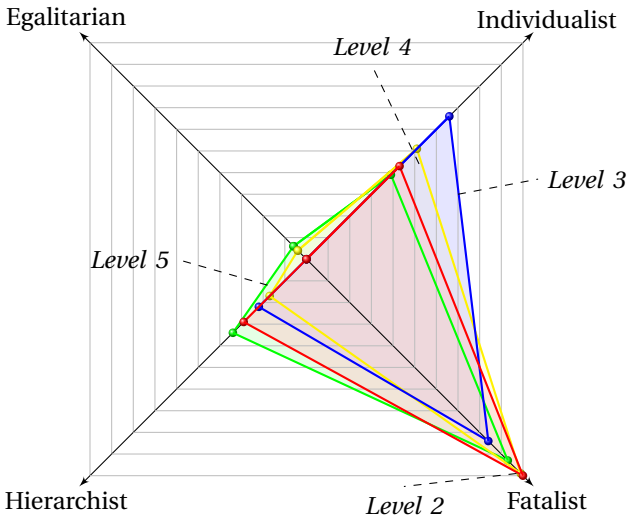

Fig. 3. Kiviat diagram of distributions of behaviour types for maturity level 2 (red), 3 (blue), 4 (yellow), 5 (green) for the Operations division.

of all participants from this department exhibit as *Hierarchists* (vs. 40% for the whole organisation, statistically significant with Fisher's exact test with $p < 0.01$). The free-text responses for this group included additional comments regarding a scenario where — due to IT limitations — the scenario's protagonist is unable to securely send data to a client. As an example:

> *"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')

Here the employee weighs up options, leaning toward adherence to policy without compromising security. A *Hierarchist* approach is for the most part the standard security behaviour in this division. The second largest group represented at attitude Level 5 ('Active Approach') are *Fatalists*, with a share of 20% (52 employees), with little *Individualist* behaviour.

Considering the high representation of *Hierarchists* in this division, it may be that prescribed security behaviours may align with the context in this division, in that it has the most outward-facing customer interaction of all of the divisions, and predictable processes may be beneficial for managing those interactions. There is an extremely low representation of *Egalitarians* and *Individualists* in this division; for one this means that we cannot be sure whether security rules can be followed without impacting business opportunities. Missed business opportunities are noted elsewhere as a potential cost of being constrained by organisational security controls [5]. *Egalitarians* and *Individualists* may adapt security procedures in such situations so as not to impact service.

B. Analysis — Operations division

A contrasting picture is found in the Operations division, as shown in Figure 3. Here 55% (65 employees) of the employees at attitude Level 5 are *Fatalists*. If *Fatalists* see their own actions as irrelevant to the preservation of security, it may be that there is a separation from the larger organisation's security function. This may be a perceived separation, or that employees perceive security as being addressed elsewhere by someone else. That these employees are at Level 5 ('Active Approach') implies that their security understanding — which may or may not stand alongside *policy-compliant* security — is superb. The high proportion of *Fatalists* implies a disconnect; either the role of security policy in the activities of the division is not clear and visible, or there are insufficient efforts by the security function to engage employees. The following quote, although referring to policy, also mentions 'best practice', which is how IT operates in reality:

> *"This question needs to be contextualised around how important the information is and how important the consequent information security policy/policy level applied is. [...] Existing best practice for teams [is] to share logins to certain systems precisely because individual logins might not be working. [...] I'm not sure what significance [a] Password Manager has, because I'm not aware of anyone in [Operations] using that facility. Most of the tools are not even [tested and approved for internal use], much less supported by something as silly as a Password Manager."* (*Fatalist*, Level 3 / 'Ad-hoc')

The individual is resigned to working with an IT system that does not support business processes. The idea that a password manager could be beneficial to the efficiency of an employee is considered laughable, because of the perceived state of the organisation's systems. The employee's comments are useful to security managers simply for referring to IT as a larger element of the organisation, which security ought to be aligned with. Similarly, the *Fatalists* in this division may have 'seen it all', and accepted that personal involvement in maintaining secure operations can in some instances prove futile. This is emphasised by the

high attitude Levels of *Fatalists* here — these employees understand the consequences of their actions, and conclude that even the most effective approaches to security still have the capacity to fail in practice.

Another employee voices their opinion in a less exasperated manner, when considering the expectation of having to share passwords:

> *"Assuming he can change the password straight after - that's not too bad."* (scores equally as an *Individualist* & *Fatalist*, Level 4 / 'Policy Compliant')

This *Individualist*/*Fatalist* may not necessarily be considering policy, but nonetheless they are attempting to maintain some level of security. That *Individualists* also have a sizable representation in this division, albeit at the lower levels, further implies that the division's internal security culture is driven by the role of security in highly-skilled technology-related roles. *Individualists* and *Fatalists* who fit security to their role may be more naturally able to articulate the relevance of security to the goals they are trying to achieve. Where there is a lack of *Egalitarians*, the security function may compensate by talking to staff in the division, arranging security surgeries etc., to learn from the collective experiences of employees.

C. Analysis — Business division

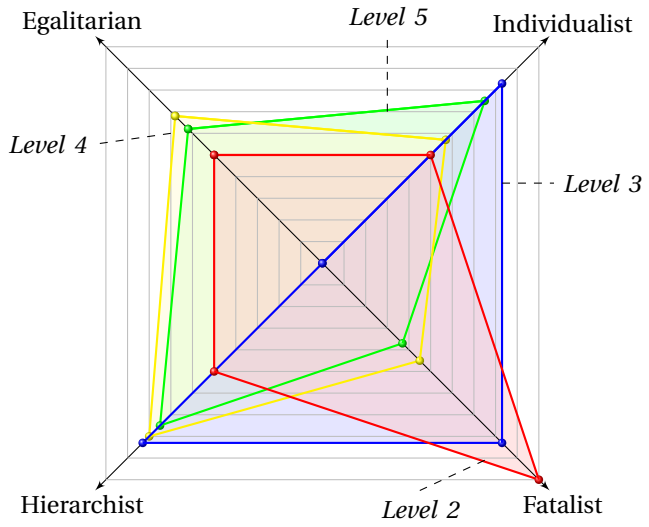

Fig. 4. Kiviat diagram of distributions of behaviour types for maturity level 2 (red), 3 (blue), 4 (yellow), 5 (green) for the Business division.

A more diverse security culture can be seen in the Business division. There is an approximately equal mix of *Egalitarians*, *Hierarchists* and *Individualists* present here. This alone suggests that a 'one-size-fits-all' approach to engaging with employees would not reach everyone in the division. The existence of diverse organisational (sub)cultures can conversely be a source of resilience during times of change [25]; this division may have valuable insights to offer security managers through open dialogue, rather than needing their guidance.

The division may have a good security posture that accounts for new and unexpected security dilemmas — if they can be addressed in a timely way. The free-text responses from this division were varied, showing security compromise as well as policy enforcement. When faced with the prospect of having to share credentials in order to get work done, one respondent comments:

> *"Assuming the colleagues are from the same team and have the same clearance then they are equally trustworthy."* (*Fatalist*, Level 2 / 'Technically Controlled')

Another respondent stands up for the policy, declaring that the actions offered to address the survey question's dilemma are not sufficient. When faced with the prospect of transferring data over an insecure connection, s/he states:

> *"Would liked to have seen this option as a choice: [additional option] Report the [connection] problem and sit back until its fixed. Ignoring the fact that the work is crucial."* (*Fatalist*, Level 4 / 'Policy Compliant')

Individualist responses to such a query are more balanced. When faced with insecure choices for transferring restricted data, one respondent shows a highly mature attitude to policy (as on the maturity scale) while at the same time risking actions that may be judged negatively by security managers:

> *"It depends on the level of security on the [bring your own device] laptop - if it's password protected and has encryption that is more acceptable. Online services such as Dropbox should not generally be used for confidential information, particularly if not [approved for use]."* (*Individualist*, Level 4 / 'Policy Compliant')

Egalitarians are by default social creatures; they thrive in groups to solve problems. This division stands out as it contains the highest proportion of *Egalitarians* from all divisions considered. Their social leaning may well help to engage others. A typical comment from an *Egalitarian* person, when encountering an unlocked and unattended workstation, is:

> *"[I would] send an email from the user of the unlocked machine to the team, offering to buy ice creams for everyone."* (*Egalitarian*, Level 5 / 'Active Approach')

Although there is a lot of variation in behaviour types in this division, it could be useful to engage employees here in a number of different ways to capture all of their experiences (as demonstrated by the quotes above), certainly *before* any attempts to reinforce policy from the top down. The large percentage of attitude Level 2 and 3 *Fatalists* may however benefit from having a clear, workable process that employees can follow; those at higher levels can inform how that can be achieved in a way that does not hinder reaching business goals.

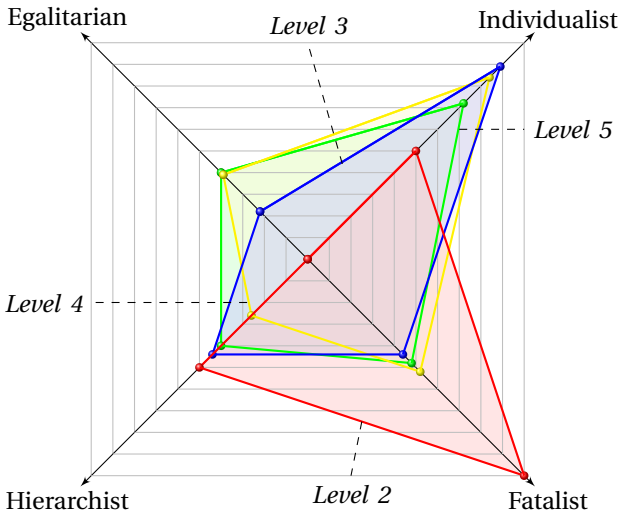

Fig. 5. Kiviat diagram of distributions of behaviour types for maturity level 2 (red), 3 (blue), 4 (yellow), 5 (green) for the Finance & Prof. Services division.

D. Analysis — Finance & Professional Services division

Considering the Finance & Professional Services division, the data shown in Figure 5 illustrates that the predominant behaviour type is *Individualist*: approximately 40% (26 employees) of attitude Levels 3, 4 and 5 display this type. In this division, there is a discrete switch from *Fatalist* to *Individualist* from attitude Level 3 ('Ad-hoc Knowledge and Application') upwards — this is statistically significant, with Pearson's $r = -0.91$, $n = 45$, $p < 0.01$. Both approaches are *individualised*, but differ in that the former experience prescribed "Inequality" and the latter act toward "Equality" [1]. It might be that those employees whose jobs are constrained by IT are relying on the organisation to ensure security for all, whereas those with an understanding of policy feel that they own how it is applied.

A top-down, prescriptive approach to engaging employees may fail to achieve results here, where *Individualists* at higher attitude levels may have an increasingly clearer understanding of how security policy fits with business goals. Indeed, communicating more security-related information to those at lower levels of security attitude may set employees up for *cognitive overload* and *embarrassment* [5].

V. Discussion and Limitations

To revisit the research challenges outlined in Section II-B, we found that separate divisions of the organisation exhibited different distributions of both behaviour type and attitude level, immediately indicating that a "one size fits all" approach to messaging around security would achieve mixed results. By combining behaviour types and attitude levels (as defined in the maturity model summarised in Section III-B), we were able to reason about differences in the security experiences of distinct groups as well as the dynamic between employees and the security provisions available to them.

Similarly, employees' free-text responses indicate that they can offer insights about the security challenges they face and how to craft solutions for their working environment — 'champions' who can improve security can then be found in different places. For example, staff in the Operations division tended toward *Fatalist* behaviour, where security would be something taken care of 'by somebody else'. Given that this included *Fatalists* with high attitude levels, any enhancements to security here may look at ensuring timely support from IT security representatives to leverage the high *risk understanding* seen in the division to spot risks as they arise and mobilise support. Conversely, in the Finance & Professional Services division more *Hierarchists* would be desired to improve the understanding of policy. Security improvement must leverage the *existing* security culture; the recruitment of security champions needs to be tailored to specific groups and divisions.

The sample of the workforce studied here has few *Egalitarians* (see Table I) — it implies that there are few opportunities or little interest in socialising security. Developing a two-way *security dialogue* between security managers and employees can promote the alignment of security policy and process with the working environment [3]. Identifying individual and team trust dynamics could identify the most effective ways to engage in that dialogue, as security challenges may be resolved at a local team level as much as by following prescribed policy directives [19]. The organisation studied here is a large organisation with thousands of staff; having a distinct security function in a large, complex work environment may indirectly result in a *Fatalist* approach of security being 'not my job' (as hinted at for the Operations division), so there would be value in examining diverse organisations to determine the effect of organisation size and the viability of engagement activities.

A limitation of the analysis conducted here is that the data collected is a *snapshot* of the security experience at one point in time, and does not account for how security processes have developed over time up to that point, or any disruptive events which may have occurred within the organisation (such as a merger, change in applicable regulations, large-scale IT renewal, etc.). However, if events were disruptive enough to result in a change in the experience of security (e.g., adoption of another company's policies), employees may be inclined to comment on the change from their perspective when engaged in an activity such as the survey described here. Similarly, collection of survey responses over time can build a picture of security culture development, not least to understand the impact of security awareness initiatives.

VI. Recommendations for Practitioners and Researchers

For the policy owner, our work reaffirms the need for security policy to be relevant to work activities and for employees to understand the risks that relate directly to those activities. Furthermore, policy should not be seen as an immovable object; when circumstances in the organisation change, the security policy should be revisited. The best sources of information for the policy owner are the employees: regular, direct, two-way interaction with individuals from all departments will enable policy to remain aligned with reality. The correct policy might not be known, but

colleagues can be engaged to identify where it falls short and identify the underlying causes of non-compliance. A policy is only workable if employees are involved in shaping it, and employees can accept that they have to 'do the right thing'.

Our recommendation to security awareness professionals and researchers is to target awareness content to specific security behaviour-types and attitude-levels. Any one mode of engagement will resonate best with a different portion of the employee population. Encouraging meaningful responses from employees may require a combination of different approaches, such as surveys, workshops, and individual interactions. The tailoring of advice does not need to be guesswork — engaging with groups of employees in the right way can immediately inform a picture of the security culture across the organisation. Ultimately, an understanding of relevant risks and work-related motivations could make *targeted* interventions much more successful. If security doesn't work for people, it doesn't work.

VII. Conclusion

Here we have analysed 608 employee responses to a security behaviour survey deployed in a large partner organisation. The survey captured attitude to security policy on a scale of maturity, and based on answer choices would assign one of four behaviour types as an indicator of the individual's approach to managing security in the workplace. Responses were analysed and four business divisions were examined in detail, including Operations and Business divisions. We found that by combining these two dimensions we can characterise the quality of security policy for groups of employees. Analysis of 189 optional free-text comments linked to the survey further suggests that those who follow policy can contribute to effective security, but so can those who question policy, socialise solutions, or would otherwise expect security to be part of their productive work if it was important. These various security cultures all have the potential to help improve security for the whole organisation, where here we have identified a range of security heroes for security managers to engage.

The ideal type of security hero engagement for the organisation studied here would be a composite of different approaches: it cannot be identified by one specific set of traits, but rather is entirely dependent on the social context it manifests in. Individuals may act alone or together, with policy in mind or in isolation from it. The methodology presented here, combining security attitude and security behaviour, is a useful tool for investigating the interplay between policy and action. Attempting to narrowly define and promote the characteristics of a security champion is counterproductive, as it simplifies the challenge of involving employees in the process of improving organisational security.

Future work will see the survey exercise repeated with more organisations over time, across sectors. This will further inform the understanding of how employees as a group or workforce respond to security policy and its implementation. With that, work will also look to identify interventions based upon user feedback, to determine if improvements to security can effect lasting behaviour change. It may be that survey can be designed in such a way as to elicit information about not only generally secure behaviours and behaviours which align with policy, but also those behaviours which are acceptably secure given limiting restrictions in the particular work environment being assessed.

Acknowledgments

The authors would like to thank the participating organisation for their assistance. We would also like to thank the reviewers for their comments and suggestions. The authors were supported in part by UK EPSRC grants, no. EP/G037264/1 and no. EP/K006517/1.

References

[1] J. Adams, "Risk and morality: three framing devices," *Risk and morality*, pp. 87–106, 2003.

[2] E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," *Computers & Security*, vol. 28, no. 6, pp. 476–490, 2009.

[3] D. Ashenden and D. Lawrence, "Security dialogues: Building better relationships between security and business," *IEEE Security & Privacy*, vol. 14, no. 3, pp. 82–87, 2016.

[4] A. Beautement, I. Becker, S. Parkin, K. Krol, and A. Sasse, "Productive security: A scalable methodology for analysing employee security behaviours," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, 2016, pp. 253–270.

[5] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 workshop on New security paradigms*. ACM, 2009, pp. 47–58.

[6] O. Beris, A. Beautement, and M. A. Sasse, "Employee rule breakers, excuse makers and security champions:: Mapping the risk perceptions and emotions that drive security behaviors," in *Proceedings of the 2015 New Security Paradigms Workshop*. ACM, 2015, pp. 73–84.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: an empirical investigation," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–7.

[8] L. Connolly, M. Lang, and J. D. Tygar, "Investigation of employee security behaviour: A grounded theory approach," in *IFIP International Information Security Conference*. Springer, 2015, pp. 283–296.

[9] N. Conway and R. B. Briner, *Understanding psychological contracts at work: A critical evaluation of theory and research*. Oxford University Press, 2005.

[10] S. Dekker, *The field guide to understanding 'human error'*. Ashgate Publishing, Ltd., 2014.

[11] S. Furnell and A. Rajendran, "Understanding the influences on information security behaviour," *Computer Fraud & Security*, vol. 2012, no. 3, pp. 12–15, 2012.

[12] T. Gabriel and S. Furnell, "Selecting security champions," *Computer Fraud & Security*, vol. 2011, no. 8, pp. 8–12, 2011.

[13] J. Haidt, "The righteous mind: Why good people are divided by religion and politics," *Pantheon, New York*, 2012.

[14] J. S.-C. Hsu, S.-P. Shih, Y. W. Hung, and P. B. Lowry, "The role of extra-role behaviors and social controls in information security policy effectiveness," *Information Systems Research*, vol. 26, no. 2, pp. 282–300, 2015.

[15] A. C. Johnston, M. Warkentin, M. McBride, and L. Carter, "Dispositional and situational factors: influences on information security policy violations," *European Journal of Information Systems*, vol. 25, no. 3, pp. 231–251, 2016.

[16] I. Kirlappos, A. Beautement, and M. A. Sasse, "'comply or die' is dead: Long live security-aware principal agents," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 70–82.

[17] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from "shadow security": Why understanding non-compliance provides the basis for effective security," 2014.

[18] ——, "Shadow security as a tool for the learning organization," *ACM SIGCAS Computers and Society*, vol. 45, no. 1, pp. 29–37, 2015.

[19] I. Kirlappos and M. A. Sasse, "Fixing security together," 2015.

[20] S. L. Pfleeger, M. A. Sasse, and A. Furnham, "From weakest link to security hero: Transforming staff security behavior," *Journal of Homeland Security and Emergency Management*, vol. 11, no. 4, pp. 489–510, 2014.

[21] D. H. Pink, *Drive: The surprising truth about what motivates us*. Penguin, 2011.

[22] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, "Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," *Information & management*, vol. 51, no. 5, pp. 551–567, 2014.

[23] J. T. Reason, *The human contribution: unsafe acts, accidents and heroic recoveries*. Ashgate Publishing, Ltd., 2008.

[24] M. A. Sasse, M. Smith, C. Herley, H. Lipford, and K. Vaniea, "Debunking security-usability tradeoff myths," *IEEE Security & Privacy*, vol. 14, no. 5, pp. 33–39, 2016.

[25] E. H. Schein, *Organizational culture and leadership*. John Wiley & Sons, 2010, vol. 2.

[26] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: a systematic review of quantitative studies," *Information Management & Computer Security*, vol. 22, no. 1, pp. 42–75, 2014.