Journal of Cybersecurity, 2024, tyae007
https://doi.org/10.1093/cybsec/tyae007

Research paper

‘The trivial tickets build the trust’: a co-design approach to understanding security support interactions in a large university

Albesë Demjaha [1,2,*], David Pym [1,3,4], Tristan Caulfield [1], Simon Parkin [5]

[1]Department of Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom
[2]The Alan Turing Institute, 96 Euston Rd, London NW1 2DB, United Kingdom
[3]Department of Philosophy, University College London, Gower Street, London WC1E 6BT, United Kingdom
[4]Institute of Philosophy, University of London, Malet St, London WC1E 7HU, United Kingdom
[5]Faculty of Technology, Policy and Management, Delft University of Technology, Mekelweg 5, 2628 CD Delft, The Netherlands

*Corresponding author. Department of Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom. E-mail: albese.demjaha.16@alumni.ucl.ac.uk

Received 30 November 2022; revised 5 February 2024; accepted 7 May 2024

Abstract

Increasingly, organizations are acknowledging the importance of human factors in the management of security in workplaces. There are challenges in managing security infrastructures in which there may be centrally mandated and locally managed initiatives to promote secure behaviours. We apply a co-design methodology to harmonize employee behaviour and centralized security management in a large university. This involves iterative rounds of interviews connected by the co-design methodology: 14 employees working with high-value data with specific security needs; seven support staff across both local and central IT and IT-security support teams; and two senior security decision-makers in the organization. We find that employees prefer local support together with assurances that they are behaving securely, rather than precise instructions that lack local context. Trust in support teams that understand local needs also improves engagement, especially for employees who are unsure what to do. Policy is understood by employees through their interactions with support staff and when they see colleagues enacting secure behaviours in the workplace. The iterative co-design approach brings together the viewpoints of a range of employee groups and security decision-makers that capture key influences that drive secure working practices. We provide recommendations for improvements to workplace security, including recognizing that communication of the policy is as important as what is in the policy.

Keywords: security; users; policy; management; modelling; co-design; translation zone

Introduction

Organizations provide IT infrastructure for employees to use in their day-to-day work activities. This infrastructure includes security controls, which include policies and guidance to follow when interacting with digital assets, and controls on those assets that are to be used within regular, everyday tasks. Most recognizable of these would be managed account systems, which dictate access to IT systems, and associated account credentials, such as company usernames and passwords [1].

Making sure that humans can use security provisions is critical, especially where they are often supporting primary work activities. This is further complicated when considering that employees and teams can differ in their needs, especially in larger organizations. For over two decades, research into the human factors of security in organizations has highlighted impacts and frictions that are created when there is a bad fit of provisioned security with working practices (e.g. [1–3]). It remains the case that security managers continue to lack appropriate tools for understanding and addressing these challenges constructively [4], so that a rift between end-users and system managers persists [5]. Security managers are eager to engage with an understanding of human behaviours, provided that understanding is shown to relate directly to decisions they make around the security infrastructure that they manage [6,7].

We posit that directly relating security management decisions to employees' experience of security in the setting of a large organization can not only identify improvements, but specifically improvements that are feasible within that same infrastructure. That is, we aim to work with both employee groups and security decision-makers within an organization, towards identifying *more workable* security controls. Such an approach requires identifying the commonalities between end-user experiences and security controls; this is embodied in the infrastructure provided to users (as controls, policies, and so on), and the decisions made about that infrastructure.

In this work, we apply a co-design approach—grounded in modelling methodology—which we use to gather data from employee groups in the IT-security ecosystem, and construct models of the interaction of those employee groups with technological and policy infrastructure. In so doing, we seek to provide structured evidence to inform decision-making in the management and provisioning of employee-facing security measures. Prior work with organizations has provided valuable insights into the workings of security in organizations (e.g. [3, 8]). Here, we go further by engaging with the managers responsible for the security infrastructure in a large partner organization, relating their decisions to employee security practices. We gather evidence through qualitative research in the form of semistructured interviews with employees and IT/security support teams. Qualitative data is integrated into the structured model that underpins the co-design approach, such that successive rounds of data-collection build up conceptual models that detail how people interact with security provisions. The ultimate aim is to empower security managers with the systematically gathered evidence, so that they can relate human factors to their existing decision-making processes.

Our contributions are as described below.

- By framing the experiences of different groups through the lens of security management decisions, our iterative co-design approach surfaces connections between those groups.
- We structure engagement through a novel co-design approach, in this case executed with senior security managers at the centre, framed around their decision-making concerns and options (such as policy communications, and usability characteristics of provisioned security technologies). The approach is underpinned by rigorous modelling principles (see, e.g. [9–11]), while also incorporating a *translation zone* between researchers and security decision-makers. This serves to directly link the study of employees and support staff to security managers, to produce a multistakeholder view of the complexities of provisioned security in an organization [6]. By couching our security human factors findings in the capabilities of system (security) managers, we surface further avenues for improvement in complex organizational settings. For instance, the security manager(s) at our partner organization believe there are ways to improve the communication of security policies to employees, but are hesitant to overstep what they believe is a remit to support the working culture rather than directly influencing it.
- Engagement with distinct stakeholder groups within a large organization, namely employees, support teams, and security managers. Support teams especially have been rarely considered in research up to now, despite their role in resolving problems (such as with passwords, access cards, and so on) and ensuring access to provisioned IT. By analysing security use and support in the same organization according to our co-design approach, evidenced through direct qualitative engagement, we surface the complex and interconnected nature of supporting workable security practices by employees. Within the partner organization studied here, we found that employees appreciated explicit assurance that they were following guidance correctly; they also valued the qualities of local support in understanding their contextual needs, but also in accommodating employees *not being sure* and asking questions (as the nonexperts that organization security assumes them to be). This highlights new, informal dimensions to technical support [12] and support networks [13]; specifically, translating these processes to the setting of a workplace. Our findings surface the role of care in IT security [13], including the moralities around how to engage constructively with employees who are not sure how to exactly 'do the right thing' for security [14].

The paper is arranged as follows: an appraisal of organization security issues for employees is presented in the section 'Background and Related Work', including a review of prior attempts to reconcile use and provisioning of security in the workplace, and co-design approaches; details of our co-design and modelling methodology are found in the section 'Methodology'; this is followed by the conceptual model built from our engagement with employees, support teams, and security decision-makers in the section 'Results'; we close the paper with a 'Discussion' section that revisits our aims and distils recommendations, and a 'Conclusion' section that includes consideration of future work.

Background and related work

Through a review of related research, we set the scene for how security in organizations is experienced by employees, and how this sits relative to the view of security management in organizations. We then complement this by outlining how prior co-design approaches can inform how security human factors may be aligned to the decision-making processes of security managers in organizations.

Organizational security

Employees in organizations, especially larger organizations, will be working in an environment with provisioned IT-security measures that they will be expected to use. This typically includes corporate IT accounts, provisioned laptops, and smartphones, and so on. How to use these provisions, and which security-related behaviours to follow when interacting with digital assets, will often be defined as rules or advisories in one or more *security policies* (or as part of other IT-related policies).

Security rules and advice are not always workable in practice alongside productive tasks [14]; employees may adapt or circumvent proscribed security tasks and instead follow 'workarounds' of their own making. Employees might otherwise create their own 'shadow security' solutions [15], especially if there is a lack of visible support or understanding from the organization. In this sense, following the mandates of security managers and working securely are often assumed to be the same thing, but little attention is given to how best to design security rules so that employees can work both effectively and securely [5, 8]. Noncompliance with rules is not to say that in all cases the employee is working insecurely, such that there is often scope to design security policies that can be complied with, provide security, and which do not act as a burden that disrupts productive work tasks [1]. Security policies have been the subject of a great amount of research, as they are typically the main thread connecting security management decisions to employee activities and experience of security within organizations. As such, much effort has been invested in developing instruments to measure security behaviours and user compliance with policy, such as with the HAIS-Q behaviour measurement approach [16].

In terms of how to improve security and productivity in tandem, the foundational research of Adams and Sasse in 1999 [2] noted the need to consider the human aspects of security provisions in organizations, having exposed problems that employees had with provisioned credentials. The work highlighted that security managers did not understand their users, but also that there was no common ground between both sides or institutional means to reliably communicate issues from one side to the other. The work proposed a user-centric approach, whereas security provisioning to this day remains very much one-way, outwards from the security team to employees. We propose to address what we regard as the continued lack of both an understanding of the employee experience of security and a view of the organization environment, built from the perspectives of both decision-maker and employee.

A key aspect of improving the usability of security measures within organizations is the design of the security infrastructure [1]; this in essence comprises the 'hard' security controls [17]. Employees may also be subject to 'soft' controls such as regular online training courses, formal presentations (as during onboarding), and so on. [18]. There are various ways in which these initiatives can fail to resonate with employees [19], where communication is a key aspect in ensuring that employees are aware of (security) behaviours expected in the workplace [20].

Holistic views of organizational security

Through studies of security managers and support teams, recognition has been seen among practitioners of the need to consider employee needs [6, 21]. As found by Reinfelder *et al.* [7], security managers can often lack a view of the end-user experience, which only serves to perpetuate distance between them and the users they are meant to support. Ashenden and Sasse [22] noted that security managers can seem unsure of how to approach the human side of the organization, even while at the same time they are confident of their approach to managing security-related technologies. This then requires dedicated approaches to bringing together the views of both sides, as in the Security Dialogues work of Ashenden and Lawrence [5], which through focus groups explored a shift from unquestioned compliance with policy, towards security *concordance*: input from both sides can contribute to user-facing solutions which can effectively secure users' work and are doable at the same time. Here, we examine the threads that connect 'central' security policy-makers, via support teams, to employees who are using provisioned IT systems; i.e. the existing elements of an organization, which have the capacity to enable secure working if considered with the user in mind more than is done at present.

Many aspects of security managers' work demonstrate attention and care for how security is maintained [13], including where improvements can leave the security infrastructure in a temporarily weakened state as it 'oscillates'—is remade—into a new form. Adapting to users' needs while also securing the organization must then be done carefully, involving many such transitions between secure and nonsecure states. Solutions are ideally found which enable employees to go about their work, and be able to do so securely [8], but with care for how this can be maintained over time [15]. From a study of two organizations (including a university), Blythe *et al.* [3] stress the importance of focussing on building up specific workplace security behaviours, as do Pollini *et al.* [23], who engage with managers and employees to understand the differences in their knowledge about advocated security behaviours in the workplace. Regarding a university setting, Wang *et al.* [24] interviewed multiple types of university employee regarding account-sharing practices, noting the importance of making sure that security messaging resonates with employees.

Co-design of organizational security solutions

In an organizational setting, the aforementioned 'security dialogues' work of Ashenden and Lawrence [5] created dedicated focus groups for security staff and their users in the same organization. This then served as a space for the experiences of multiple groups to be shared, hearing out each other's perspectives on security. A disconnect was highlighted where, for one, neither side had the sense that their needs were being listened to by the other. Beautement *et al.* [8] demonstrate the importance of capturing data that represents a real-world environment and the workplace 'dilemmas' within; this data was ultimately communicated to security managers after analysis, resulting in targeted improvements to existing security-related infrastructure.

Heath *et al.* [25] utilized LEGO kits to support engagement between participants from different parts of the same organization, responding to a range of different security scenarios using a shared LEGO kit. This then informed each participant's knowledge of others' perspectives on what the larger 'whole' of the organization was and their involvement in it. The LEGO approach gives participants the constructs of a model (where each type of LEGO block had a particular meaning or purpose) and prompts them to develop a shared view, an instantiation of the model. Here, we address the development of a whole-system view by engaging with employee groups in their own terms through qualitative research, and deriving the constructs of the model from that data, through a translation zone that maps the end-user perspective to the constructs or artefacts in the translation zone, that represents decisions which can be explored in terms of the extent to which they can or cannot be enacted to directly improve the system in response.

Our approach has parallels with *participatory modelling* (PM), 'a purposeful learning process for action that engages the implicit and explicit knowledge of stakeholders to create formalized and shared representations of reality' [26, p.1]. Methods such as participatory and collaborative modelling have come into use because of an increased emphasis on stakeholder involvement, where the majority of PM work has been done in areas such as environment and planning, water resources management, and resource and environmental modelling [26–29]. To the best of our knowledge PM has not been applied in cybersecurity, yet we note here a comparable need to involve various stakeholders in complex environments and identify the best of the available choices to meet a broader need, in this case the provision of workable security measures in organizations.

PM aims to leverage the knowledge and experience that stakeholders can contribute, positing that policy compliance is more likely to emerge from engaging stakeholders in the process of developing those policies [29]. PM is also at times referred to as collaborative modelling or comodelling [27]. PM informs researchers in gathering evidence to direct long-term system improvements. Here, we focus on an approach that directly relates employee and support experiences to the security-related decisions that a system manager has immediately within their remit and capabilities.

Methodology

For this work, we use an overarching methodology that combines established methods in order to identify, relate, and meaningfully evidence employee-facing security management decisions in an organization setting. We apply an iterative *co-design modelling process*, generalizing the well-established modelling methodology as explained in, e.g. [10, 30] that aims to bring modellers and the decision makers of an organization together, adopted from [10, 30]. This approach guides the building of a model of the organization environment (as relates to security). Evidence of human-facing experiences and processes is then substantiated with evidence collected from qualitative research, in this case semistructured interviews; here we employ *humble inquiry* (HI) [31], whereas for interview analysis we refer to the widely used *thematic analysis* (TA) method [32].

Co-design modelling process

Security managers are faced with the challenge of managing security apparatus within dynamic socio-technical environments. Yet, security managers must often take decisions in the interest of security that impact this complex environment, without always being aware of the potential outcomes. Modelling, whether conceptual or otherwise, can be used as a tool for managing uncertainty associated with security decisions (as with e.g. cybersecurity investments [33], or exploring physical access improvements [34]). Models enable a systematic understanding of problems and solutions and the process of constructing a model is in itself a valuable way of understanding and articulating a problem. There are, however, challenges with modelling in a useful and rigorous way in general, and modelling cultural and behavioural aspects of security in particular [35].

While the managers of an organization's security apparatus may have extensive knowledge of that apparatus and expertise in its domain of application, they may lack knowledge of the necessary methods and data collection requirements for modelling [36]. Modellers, on the other hand, experts in the latter, may have limited understanding of the system under observation, the available data to be collected, and the context of the domain. This can limit a modeller's capacity to model a system in a useful way that can arrive at actionable recommendations in practice.

In an effort to address these linked challenges, and facilitate better opportunities for capturing the behavioural and cultural aspects influencing security in organizations, we apply a co-design approach for security modelling. We define our co-design approach in the following way:

> 'Model co-design is a process that engages modellers and system stakeholders cooperatively in the acts of objective identification and model specification, design, and construction with the aims of aligning model objectives with the needs of the stakeholders, and designing a model that is feasible given the limits of data availability, which are discovered as part of the process.'[30, p.9]

Co-design modelling components

It is important to emphasise further the key differences as well as similarities between our understanding and definition of 'model co-design' and previously used methods such as participatory design (also referred to as co-design) [37] in the Human Computer Interaction (HCI) and design community, as well as PM [26].

Traditionally, participatory design has been used as a way of sharing knowledge between stakeholders of different disciplines, and often potential users of a product, with the aim of integrating this knowledge into a final product [38]. Similarly, PM engages in a process of learning from stakeholders—and integrating their knowledge into formalized representations of reality. Our approach focuses more heavily on a process of cocreation from the very beginning, including the problem identification, objective setting, and model design and construction.

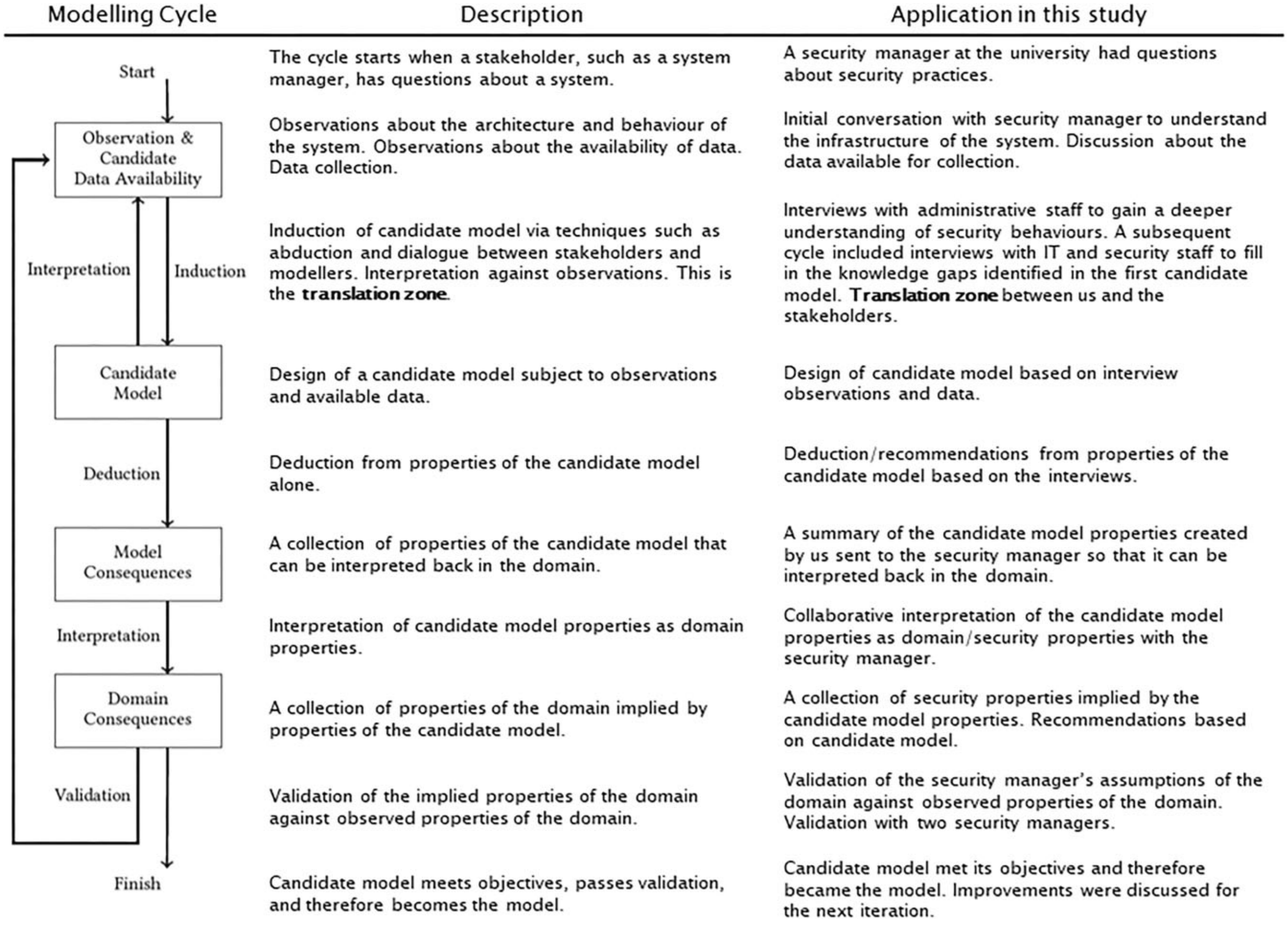
PM differentiates between three types of modelling method selection [26]: an 'expert approach' driven by the modellers' own preferences for tools and methods; an 'experimental approach' developed and piloted specifically within an engagement between modellers and stakeholders, and; a 'participatory approach', wherein all stakeholders, including modellers, decide about the modelling tools and methods to be used. The PM community then recommends an approach, which incorporates elements from all three types [26]. While the PM community considers the stakeholders' 'lack of (modelling) expertise' as a potential challenge when choosing tools and methods, our approach embraces the expertise of participating employee groups in their own domain of practice, as a strength.

We embrace qualities of the participatory approach of PM, but with a greater focus on co-design, rather than potential participation. In a way, our work has parallels with both co-design and PM, applied in the field of security, more specifically in the modelling of behavioural and cultural aspects of security in organizations. The focus of our approach is on representing decisions related to the management of employee-facing security, and how these relate to infrastructure, requiring a rigorous modelling approach with models constructed to inform decision-making, and how it feeds back into subsequent cycles—all in co-design with the expert stakeholder (here, the security manager in a participating university). Such an approach, iteratively collecting more evidence to reach more well-informed decisions that build on existing understanding of the system, can improve investments and cybersecurity risk management practices [36].

As seen in Fig. 1, the methodology provides a structured approach for modeller and decision-maker interaction through the key phases of model construction. The key phases are Observation and Candidate Data Availability, Candidate Model, Model Consequences, and Domain Consequences—and their implementation is carried out through the processes of *interpretation*, *induction*, *deduction*, and *validation*. We create a subloop between the first two phases which represents the *translation zone* between the modellers and the security decision-maker(s) [9]. Below we explain how we applied the different stages of the co-design process in this particular study, emphasising the importance of the translation zone.

The goal of each part of the framework (Fig. 1) is as follows:

- Observation and candidate data availability: identify mutually beneficial objectives, which can be pursued, and explore the data collection opportunities in the real environment.
- Translation zone: engage in an iterative process of mutual learning, where we as modellers learn about the system from the decision-maker stakeholders, and the decision-maker stakeholders learn from us about the nature and bounds of our research (in this case, sociotechnical security) and the required data and information to substantiate the model.
- Candidate model: construct an initial candidate model based on the collected data (here, qualitative data from interviews) and information.
- Model consequences: deduct preliminary consequences from the candidate model, which resonate with the decision-maker stakeholders.



Modelling Cycle	Description	Application in this study
Start	The cycle starts when a stakeholder, such as a system manager, has questions about a system.	A security manager at the university had questions about security practices.
Observation & Candidate Data Availability	Observations about the architecture and behaviour of the system. Observations about the availability of data. Data collection.	Initial conversation with security manager to understand the infrastructure of the system. Discussion about the data available for collection.
Interpretation Induction	Induction of candidate model via techniques such as abduction and dialogue between stakeholders and modellers. Interpretation against observations. This is the **translation zone**.	Interviews with administrative staff to gain a deeper understanding of security behaviours. A subsequent cycle included interviews with IT and security staff to fill in the knowledge gaps identified in the first candidate model. **Translation zone** between us and the stakeholders.
Candidate Model	Design of a candidate model subject to observations and available data.	Design of candidate model based on interview observations and data.
Deduction	Deduction from properties of the candidate model alone.	Deduction/recommendations from properties of the candidate model based on the interviews.
Model Consequences	A collection of properties of the candidate model that can be interpreted back in the domain.	A summary of the candidate model properties created by us sent to the security manager so that it can be interpreted back in the domain.
Interpretation	Interpretation of candidate model properties as domain properties.	Collaborative interpretation of the candidate model properties as domain/security properties with the security manager.
Domain Consequences	A collection of properties of the domain implied by properties of the candidate model.	A collection of security properties implied by the candidate model properties. Recommendations based on candidate model.
Validation	Validation of the implied properties of the domain against observed properties of the domain.	Validation of the security manager's assumptions of the domain against observed properties of the domain. Validation with two security managers.
Finish	Candidate model meets objectives, passes validation, and therefore becomes the model.	Candidate model met its objectives and therefore became the model. Improvements were discussed for the next iteration.

Figure 1. The co-design process applied in this study (adapted from [10, 30]).

- Domain consequences: interpret the domain properties that are implied by the properties of the model (consequences relating to the real-world environment).
- Validation: validate the domain properties that are implied by the model against the observed properties of the domain.

The framework described above can be used to develop all of the key types of model—mathematical, computational, and conceptual (e.g. [10]). In the case of the work reported here, we are constructing a conceptual model, and the components of our conceptual model (represented in Fig. 3) are the following:

- An in-depth understanding of the system.
- An understanding of the interaction between different employee groups and decision-makers in the organization.
- Knowledge of the organizational structure and policies intended to be applied to the system.

We demonstrate how to use this conceptual model to extract recommendations that can inform security policy design, communication, and decision-making.

Supporting security management decision-making

We engaged with the acting security manager—Chief Information Security Officer (CISO)—at a participating university, applying our approach in the process. The overall aim was to support decisions about how to manage and invest in cybersecurity infrastructure, which is a common challenge [36]. Here, we specifically examined the management of employee-facing security, where our examination of Related Work has detailed the additional complexities here, as well as reasons why it is critical to anticipate and avoid problematic security provisions. A capacity to model a system and to some extent forecast the outcomes of decisions then have additional importance.

In the initial engagement with the security manager, the manager had made some assumptions about the security behaviours and practices at the university but had, at the same time, a lot of questions, believing that knowing more about working practices in the organization would better inform decisions around investments in employee-facing controls and improvements. That is, there were elements of the workings of the organization—around employee activity—that the security manager believed they: (i) did not understand because they were not observable as part of their existing (technical) infrastructure, and (ii) did not have the methods or capacity to measure. This naturally led to opportunities for human factors research to gather and structure information from the environment. We, as researchers working in the spirit of the Related Work discussed earlier, were interested in examining the role of behavioural aspects in organizational security, towards finding ways to reach workable security solutions in practice.

These challenges were complicated further by the decentralized nature of the university infrastructure (with some user support and IT decisions happening within faculties or departments); the security manager had a less detailed overview of the system than if all infrastructure was directly under their control (as in a completely central-

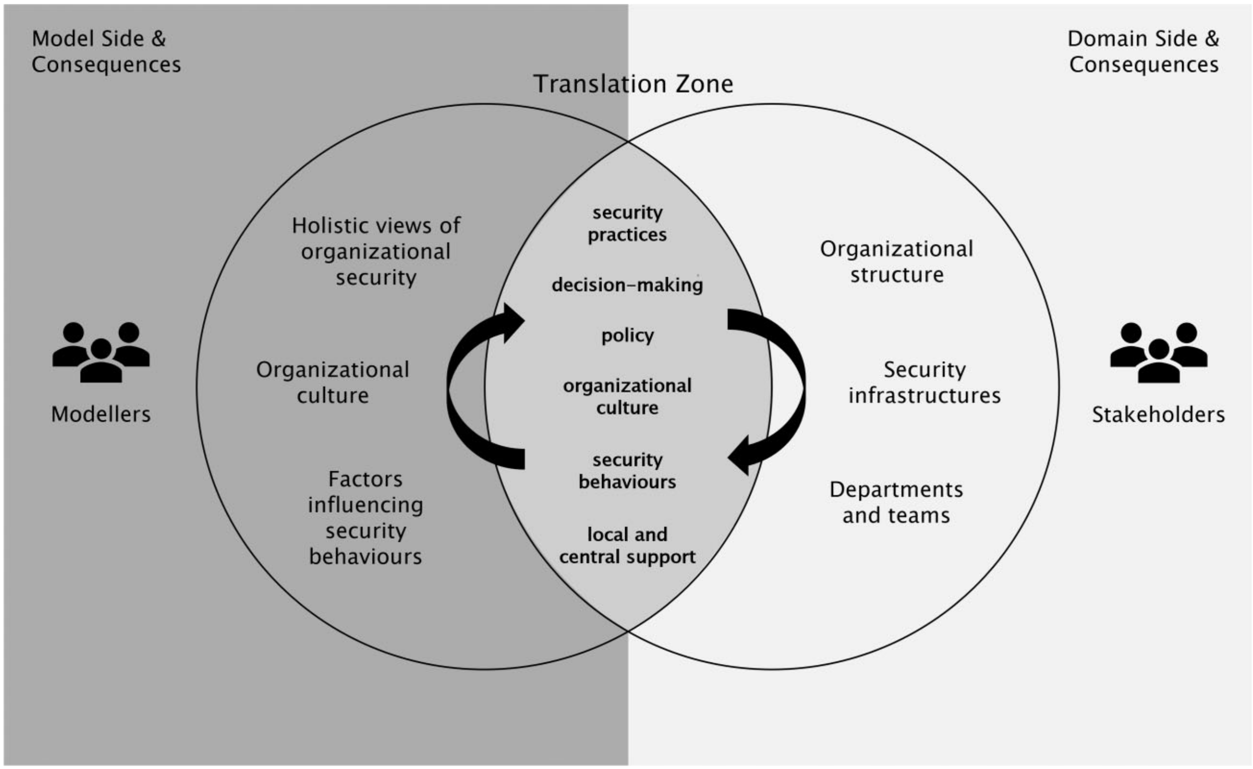


Figure 2. Exchangeable artefacts between modellers and decision-maker stakeholders in the translation zone.

ized environment), and was thus unable to support these assumptions or explore them further from their ‘central’ position.

The interaction began by exploring the opportunity for collaboration. Initially, we, as modellers, and the security manager as a decision-maker stakeholder, each had our own representation of reality, which was, for the purposes of this research, regarded as being each side’s candidate model of the system and its socio-technical interactions. These models were predominantly characterized by our areas of expertise. For example, we brought in knowledge about the human factors of security, and questions to be asked about security culture and practices. The security manager, on the other hand, brought in observations of the system, and different elements of infrastructure relevant for the security behaviours at the university. As shown in Fig. 2, while we each had our own understanding of the system, and areas of expertise, we identified exchangeable artefacts, which facilitated the translation zone.

The concept of the translation zone stems from that of trading zones [39], which was introduced to bridge the communication gap between sciences. The purpose of a translation zone is to identify a shared language between communities in order to facilitate conversation and collaboration in specific contexts [40]. Having been previously proposed to solve a range of challenges in the security community (e.g. [9, 10, 40]), we similarly adopted the concept of the translation zone and exchangeable artefacts, to establish a meaningful conversation with the security manager. This exchange would be meaningful insofar as the researchers gathering human factors data within the organization in a targeted fashion, and constructing a model of the environment, i.e. then discussed with the security manager. By identifying these artefacts, we were able to interact within the translation zone through commonly understood concepts, which are outlined in the intersection of the union in Fig. 2. As can be seen in Appendix A, the artefacts identified within the initial engagement became the basis for the basic structure of interviews conducted with employees as part of later evidence-gathering activities.

Interview study (substantiating the model)

Interview structure

In total, we conducted 21 semistructured interviews with employees, the design of which was guided by HI—an approach which facilitates relationships based on interest and curiosity, and focuses on asking instead of telling [31]. HI goes beyond traditional interviewing and aims to create an atmosphere of trust and empathy. It is also guided by similar principles to our own methodology, such as truly learning what the other person knows and thinks and why—making it an adequate choice for this study. By using HI, we were able to have open and honest conversations with our participants, and learn more about the context of their work in relation to security practices. Rather than merely following structured questions, we focused on constructing open-ended questions, and prompts, to facilitate an interactive and honest conversation with our participants, while acting to build implicit trust. On average, the interviews lasted for ∼55 min.

Opening questions aimed to understand employee experiences through organizational culture and ‘how we do things around here’ [41]. A definition of ‘security culture’ is also useful for scoping what we explored, as the ‘attitudes, assumptions, beliefs, values and knowledge’ of employees and their interactions ‘with the organization’s systems and procedures’ that result in security-related behaviours [42]. However, we note that rather than there being ‘a collection of people’ to define organizational culture, the words *community*, *group*, or *team* are better suited to indicate some level of culture formulation [43]. Informed by existing studies of security in organizations, the interviews also explored interaction with security policies and training, and how employees manage primary work tasks alongside security expectations (as in Appendix A). The interviews with support staff were informed by the interviews with administrative employees and further explored security practices and interactions at the university, including the ticketing system, which is a way of managing user queries at the university (Appendix B).

Participants and recruitment

Interviews were conducted with employees holding active roles in the partner university. The interviews were anticipated to provide a foundational understanding of security-related practices among administrative as well as IT and security support staff at the university, while being a large enough cohort to characterize issues relevant to particular security processes and technologies. Considering that we aimed to interview several hard-to-recruit participant groups, the total participant number depended on their availability (a challenge noted in other studies with active professionals [7]). We interviewed 14 administrative staff and seven IT and security support staff, as well as engaging in iterative discussions with two security managers responsible for cybersecurity strategy.

The first group of participants that we interviewed are administrative staff who work across departments and faculties at the university, in a wide range of services such as finance, HR, and communication. The second group of participants—which we refer to as IT and security support—consists of staff in the central university helpdesk, security group, and local/departmental IT teams. Overall, the participants that we recruited represent—a variety of roles, departmental as well as central functions, and level of seniority (ranging from administrator to manager level). The participants' job positions, departments, and duration of working at the university were discussed informally in the interviews, but these were not collected as part of demographics data. These factors were considered during the TA and noted where they impacted people's security behaviours but no direct connection was identified in the interviews.

The two security managers, which we interacted with are a part of the security group which governs the security of the entire university. They are responsible for managing different functions within the group, such as awareness, incidents, and governance, which support both staff and students in their daily management of information security. Interactions were mainly with one of the security managers—both were involved in the last discussion, primarily as the second manager was taking over duties from the first. Both, however, had years of experience as a CISO.

Senior managers in administrative services were asked to promote the study as a normal part of communications with teams, where care was taken to ensure that any such communication is framed in a welcoming manner for the good of the organization, removing any sense of pressure to participate. In addition to this channel of promotion, the interview study was promoted via the university newsletter, using a combination of brief study recruitment text and advance sight of the participant Information Sheet, to provide potential participants with information about the study and its aims, so that they could make an informed decision whether to participate. There was a focus on speaking to administrative staff in this engagement as they work with important data assets. Security managers suggested to focus in this area first.

Research ethics and Covid-19 measures

The study was approved through the university ethics committee review process. We followed the principles on the Menlo Report [44]: *Respect for Persons* through anonymization, right to retract from interview, conducting interviews online, and so on; *Beneficence* through anonymity, and so on; *Justice* by hearing both sides, and so on; and *Respect for Law and Public Interest* by respecting the policies of the organization during the study. All interviews were recorded and transcribed by one of the researchers and transcripts were redacted to remove any identifying information.

Because of changes to research conduct during Covid-related 'lockdown' restrictions over the course of the study, it was necessary to conduct human-subjects research online. The interviews were conducted between April of 2020 and November 2021. Because of the changes and uncertainty in the way of working following Covid, the recruitment and interviewing cycle lasted longer than expected. This means that we were able to capture experiences at different points during the pandemic. Having remote as well as hybrid working conditions may have impacted the responses of participants. Recent studies [45, 46] have reported on the impact that the pandemic has had on employees and their working practices. In particular, Kaur *et al.* [45] focus on how system administration work was affected. Their findings largely align with ours, in that, e.g. many system administrators did not experience the shift to remote working to be a significant change in terms of carrying out tasks, but they did experience longer working hours. Many of them communicated with users via e-mail or phone prior to the pandemic, and this type of communication continued during remote working. Coordination with colleagues, especially new joiners, proved to be more challenging during remote working, as even small exchanges had to be done via the phone or MS Teams. This also impacted the ability to provide or receive help from other colleagues or teams. Lastly, a notable difference was the decrease in human interaction, both with colleagues and users, where particularly in our case, this was more visible for local administrators who were used to walk-ins and informal interactions with users.

Data analysis

We transcribed the employee group interviews verbatim and analysed them using a process of TA [32, 47]. Here, we adopted a hybrid approach of *reflexive* and *codebook* TA. We focused mostly on reflexive TA, an open coding approach, where themes are the final outcome of an iterative theme development and coding process [32]. Additionally, we developed a codebook during the coding process to document our analysis. Unlike other approaches to TA, neither codebook nor reflexive TA use inter-rater reliability as a measure of quality [32].

We constructed two separate codebooks, one for each of the two main participant groups.

Through a process of refinement and regular coding discussions, the final codebook for administrative staff consists of 73 codes, whereas the one for IT and security staff consists of 56 codes.

Regarding the interactions with the security manager (and later, two security managers, with one transitioning into the role), one researcher managed the conversation while the other took written notes.

Based on groupings of the codes, we identified several themes for both user groups: five themes from the interviews with administrative staff, and four themes from the interviews with IT and security support. The themes for both groups are summarized in Table 1, and the outcomes of our interviews in the next section are arranged according to these themes and demonstrated in a conceptual model (Fig. 3).

Qualitative data collection and the modelling framework

We relate the interview activities and qualitative research to our framework (Fig. 1) in the following ways:

Table 1. Themes identified during TA.

Administrative staff	IT and security support
T1A: behaviour is not guided by policy directly	T6S: local support teams build relationships
T2A: central mandates, made actionable locally	T7S: giving assurance rather than guidance
T3A: personal relationships with IT and security support build trust	T8S: ssking for security advice is common
T4A: relating security to every day tasks	T9S: security of behaviours varies between Individuals and groups
T5A: impact of GDPR on security awareness	

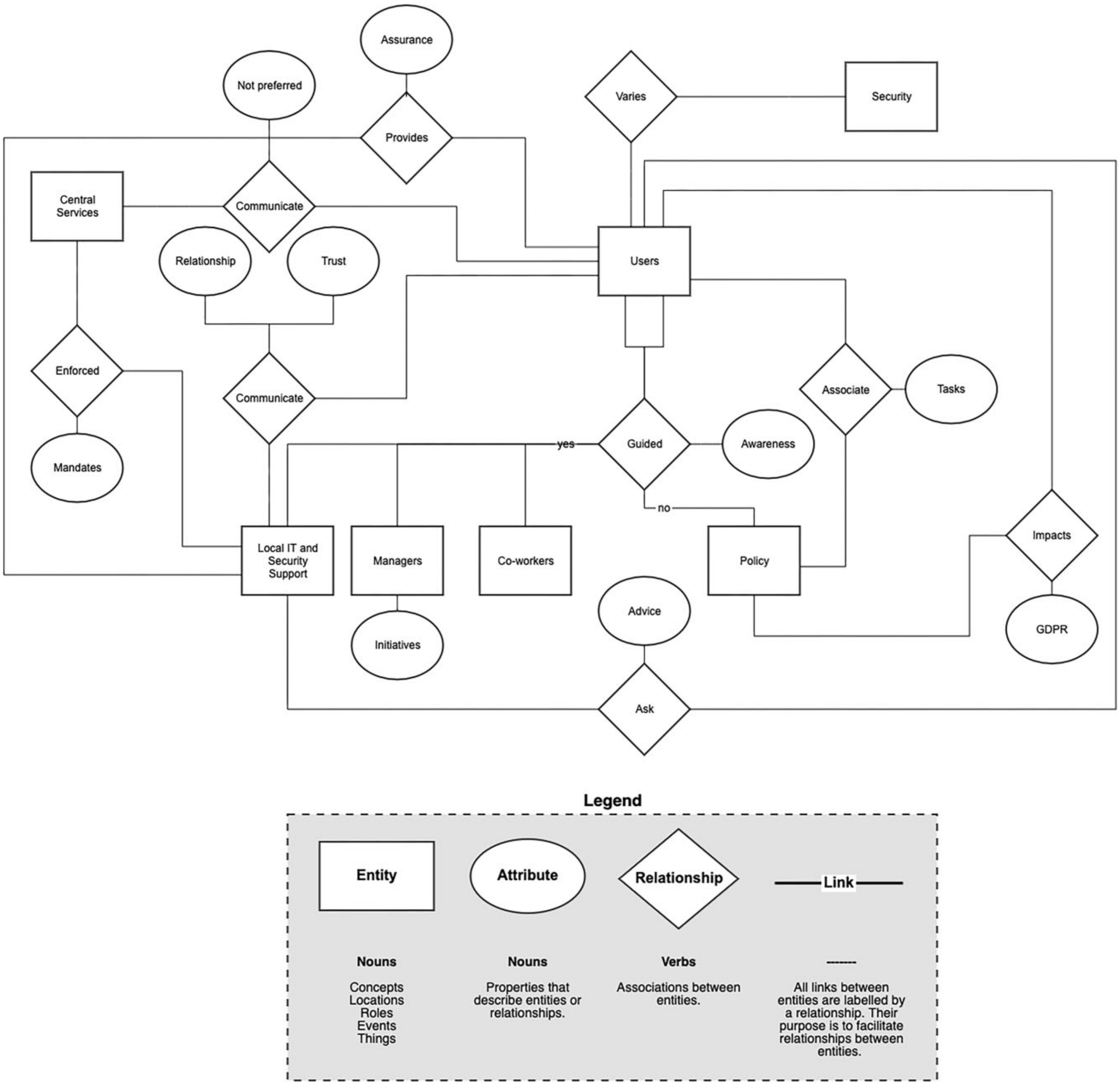


Figure 3. The conceptual model in the form of an entity-relationship (ER) model representing the interview themes.

- Observation and candidate data availability: the observation phase started with preliminary conversations with the security manager to capture their perception of how the existing IT/security systems were being used by employees and other users, and their questions about how human factors research—and research techniques—could be helpful to inform management decisions. This centred around understanding better which potential changes, and in turn decisions, could encourage engagement with security provisions, and how to avoid deploying controls which frustrate—and not support—users. During this conversation, we discussed what we would like to achieve with the modelling process and agreed on the objectives for the work. Opportunities for data collection were also discussed, and the security manager helped us identify relevant employee groups from which we could gain a realistic picture of the system, as well as brokering contact with specific teams.

- Translation zone: the translation zone depicts instances of interaction between researchers and the security manager, which occurred several times throughout the co-design process. The placement of the translation zone relative to the traditional modelling process [10] is summarized in the left-hand side of Fig. 1. The artefacts of the translation zone are represented in the centre of Fig. 2, in respect of the consequences of the model and domain sides of the translation zone.
- Candidate model: after consultation with the security manager, we conducted our first round of interviews with administrative staff who were able to provide an in-depth account of security interactions at the university, as an employee group which both (i) made direct use of provisioned IT systems, and (ii) worked with sensitive data (such as student records), and so ought to have secure systems at their disposal. Administrative staff engagement acted as the first iteration of the translation zone that supported the fuller approach. The knowledge that we gained from this interaction allowed us to construct the first candidate model, based on the analysis of the interviews. When going back to the decision-maker stakeholder—the security manager—we identified gaps and areas of interest from the interviews. In further conversation with the security manager, we were able to identify the next group of employees to engage, specifically the IT and security support staff. This demonstrates the subloop between the *translation zone* and the *candidate model*, as seen in Fig. 1. The candidate model was updated in light of new knowledge emerging from the second phase of interviews.
- Model consequences: the analysis of both sets of interviews allowed us to extract potential recommendations from the candidate model that could be applicable in the domain (of managing IT-security in a university).
- Domain consequences: during our interactions with the security manager, we went through the properties of the candidate model and collaboratively translated them into domain properties. In more concrete terms, we discussed the method of translating the findings into appropriate and useful recommendations that could inform future security decision-making in the university (the 'domain'). Once we had discussed how to translate the properties from model to domain, we were able to instantiate the main findings stemming from the candidate model. We were cautious about formulating recommendations in a silo, as the purpose of the co-design process was intended to be mutually beneficial. Therefore, the final formulation of the recommendations was shaped towards the end of the co-design process, in interaction with the main decision-maker stakeholders (in this case, the security manager we engaged with during most of the study, who handed over to the new security manager, who also participated as part of a transition), and based on existing constraints (e.g. budget) and realistic opportunities.
- Validation: in the final stage of the co-design, we were able to interact with another security manager in addition to the one we had interacted with from the very start. The second security manager had recently joined the university and was interested in gaining insights that would inform future security initiatives and decisions. Both security managers confirmed that the findings from our candidate model were in line with their own assumptions. They were also positive about the knowledge sharing that had occurred as a result of the co-design process and were keen to use the recommendations extracted from the candidate model. Although we completed two cycles of our framework, the engagements with the security managers pointed to other groups to engage with should further cycles be possible (as reported on later in our 'Results' section).

Results

Here, we present the outcomes of our interviews with employees working in administrative teams (PE##, Administrative employees subsection), and IT and security support staff (PS##, IT and security support subsection). The outcomes contribute to a conceptual model (Fig. 3), which supported the interactions with security decision makers, and which here acts as an overview of the identified entities, attributes, and relationships in the organization which are relevant to the security practices at the collaborating university.

The model comprises nine themes in total, which are also summarized in Table 1. The sections detailing the use of technology and the role of security provide background and context, to support the nine themes which are then discussed. As the legend depicts, the model consists of four different shapes, which portray the entities, attributes, relationships and links in the model. For example, the link from the entity Users to the entity Central Services facilitates the relationship Communicate, and Not Preferred is an attribute of that relationship. We describe the conceptual model below through each individual theme and reflect on its evolution throughout the next sections. Section 4.3 then summarizes the closing discussion with security managers, incorporating paraphrased statements from that interaction.

Administrative employees

Use of technology

Most of the administrative participants see technology as a fundamental part of their daily work. They mention the importance of technology when communicating with others, such as through e-mail or Microsoft Teams, the use of content creation tools, as well as several university systems used for administrative purposes. Administrative staff provide a nuanced view of their experience with technology, with examples of advantages—where using a tool enables more effective work—but also barriers that may be introduced when using IT systems and services. For example, participant PE1 explains that they must often rely on colleagues for getting access to certain reports, because of restricted access as a temporary employee. PE3, on the other hand, appreciates the physical presence of the security guards, when 'the technology sometimes does not work' and she is unable to use her access card.

The topic of change is also present in the conversation about technology. Some participants observe that there are people in the university who are sceptical towards change, and meet technology advancements with strong feelings of resistance. Such people usually need longer time and additional support to adapt to the use of new technologies and ways of working. The 'four rooms' concept refers to a similar phenomena [48], where employees may not be as willing to change if they are content with how their workplace is currently established.

Role of security

Most participants seem to believe that their current workplace is secure. This includes an implicit trust that the university's own systems are secure, and in turn that this trust extends to the external systems used by the university, that '*the university have put their trust in the*

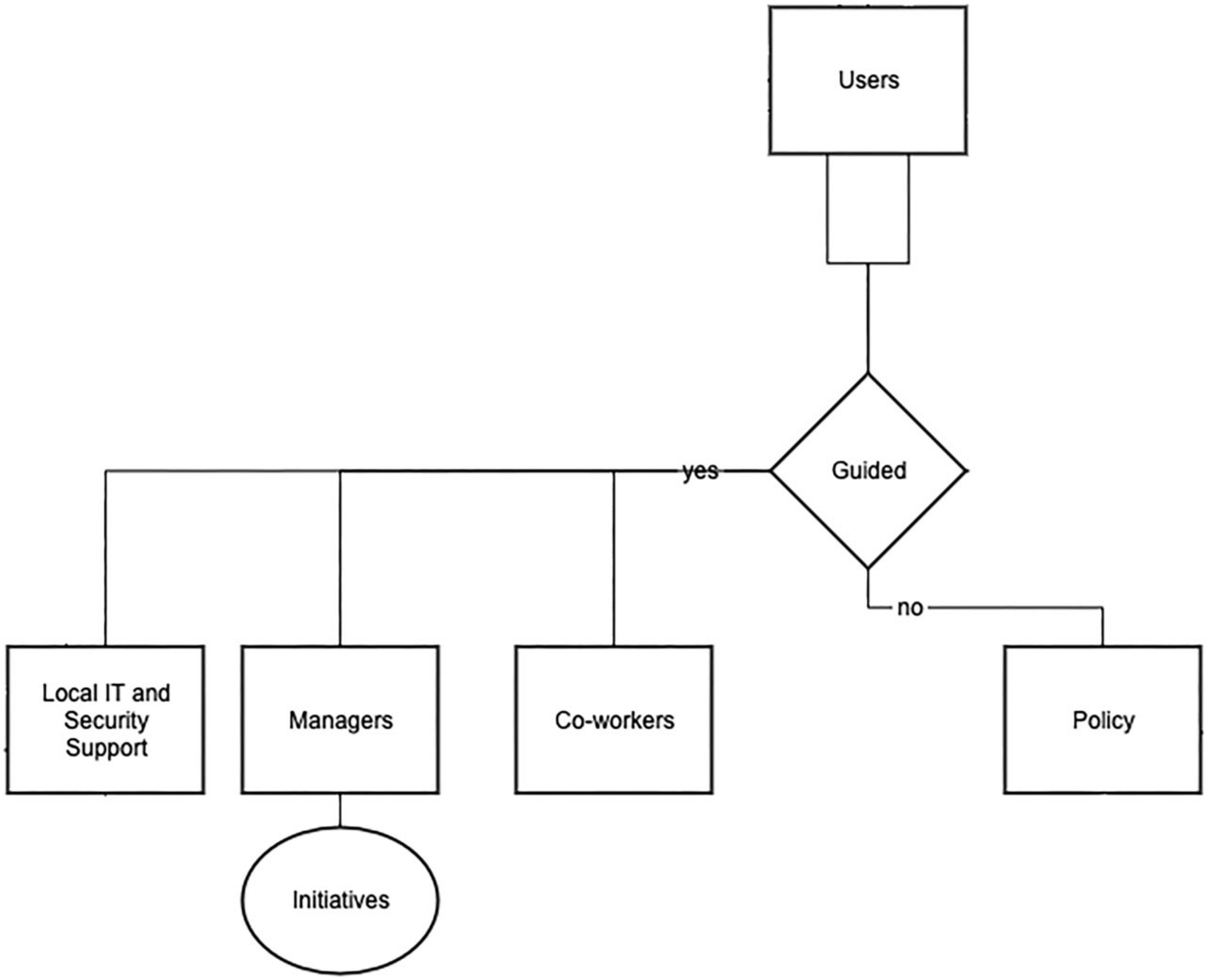


Figure 4. Entity-relationship diagram for theme T1A: 'Behaviour is not guided by policy directly'.

software'—PE13. Participants are not able to articulate thoroughly what they mean by 'secure', but some associate a state of security with the lack of experiencing a compromise. This is in contrast to the notion of 'counterfactuals' in security, as 'what-if' scenarios [49]; i.e. if there is no experience of compromise, then what is being done currently must be secure.

In addition to placing trust in the organization's security provisions, participants are also generally understanding towards its limited IT and security resources. Although it may often be inconvenient to experience a long waiting time (e.g. to regain access to a locked device or account), participants are aware of the university's limited resources and, in turn, their propensity to prioritize certain tickets over others. One participant summarizes this sentiment: '*When I have tried with [central helpdesk], it's been a very mixed bag. Sometimes, if it's something very specific, you can solve it over phone but if you turn it into an e-mail ticket it can take a while. [...] But at the same time, it's nothing that I hold a grudge about, [...] it's not a big department and these are the less urgent things.*'—PE6.

T1A: behaviour is not guided by policy directly

Representation in the conceptual model (Fig. 4). The link between the entity *Users* and the entity *Policy* denotes the relationship *Guided*, which in this case is a negative relationship, as the link states. The link from the entity *Users* to the entities *Local IT and Security Support*, *Managers*, and *Coworkers* facilitates the *Guided* relationship, only this time it is a positive relationship. For example, *Initiatives* is an attribute of the entity *Managers*, and users are guided by manager initiatives. In addition, there is a recursive relationship between users, meaning that users are also guided by their own awareness.

Participants' security behaviours and practices are generally not guided by a specific policy but rather by other factors such as personal security awareness, coworker behaviours, manager initiatives, or guidance from local IT and security support. The overwhelming majority of participants are not explicitly aware of a security policy. There was, however, some mention of awareness of policies relating to physical security, data retention, health and safety, as well as data protection. No direct connection was made between such policies and cybersecurity. After direct prompting, participants acknowledged that there is likely a security policy in place, but almost none claimed to have seen it or have substantial knowledge of it. These findings then represent knowledge derived from the working environment that the security manager would benefit from, as employee experiences are disconnected from some of the tools they control, such as security policies.

Instead of a specific policy, several other sources of guidance emerged. For instance, when asked about the source of their security behaviours and practices, PE13 noted that '*it's also from talking to colleagues, like my manager, who is also knowledgeable about*

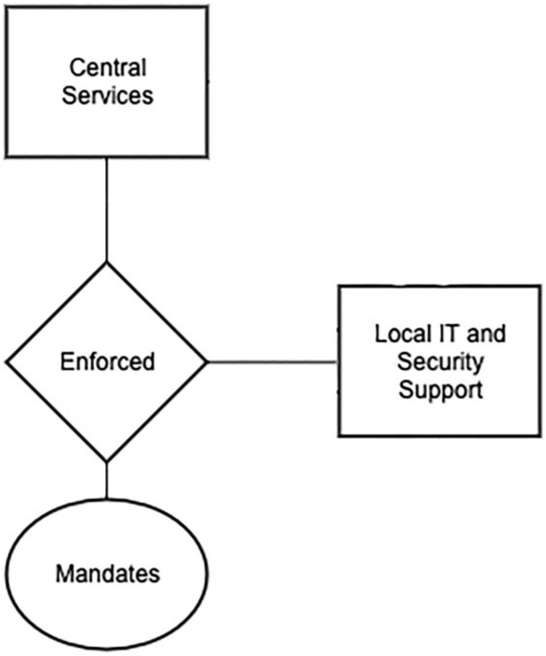


Figure 5. Entity-relationship diagram for theme T2A: ‘Central mandates, made actionable locally’.

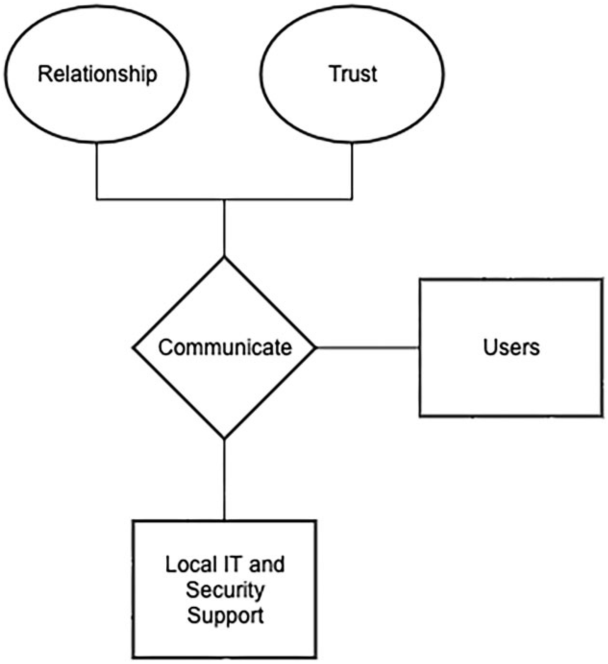


Figure 6. Entity-relationship diagram for theme T3A: ‘Personal relationships with IT and security support build trust’.

these sorts of things, as well. So, it’s probably come from a mixture of experience, my own practical experience and learning from reading’. Kirlappos *et al.* [15] noted the role of middle managers in communicating security behaviours, and Blythe *et al.* [3] have noted the potential of security culture to act as ‘the way we do things here’.

T2A: central mandates, made actionable locally

Representation in the conceptual model (Fig. 5). The link from the entity *Central Services* to the entity *Local IT and Security Support* facilitates the relationship *Enforced*, and *Mandates* is an attribute of that relationship.

How security is managed centrally or locally relates to a broader issue within the university, distinguishing between preparation and action. Participants mention several IT and security initiatives that were mandated and communicated centrally in the past, such as the implementation of the General Data Protection Regulation (GDPR) or the introduction of Microsoft Teams. Several participants frame rules as becoming ingrained once they are related to local context, such as PE9:

> ‘*It’s that combination of the things we all sort of vaguely know we should do because the people at the top have sent out these messages like [...] change your passwords, etc. But then when it is sort of talked about and enforced locally, then it becomes more of a culture, and it becomes more obvious how it affects your work and the work of the people around you.*’—PE9.

Some participants imply centrally communicated security rules and recommendations may be ignored or remain unclear, until they are taken a step further by local managers, and linked to the local work context at the level of a team. These findings identify a potential ‘local’ point of action for centralized policies, in local managers. This again reflects previous findings [15] relating to how security-related practices are informed by managers, but also relates to conversations around the role of ‘security champions’ within companies [50].

T3A: personal relationships with IT and security support build trust

Representation in the conceptual model (Fig. 6). The link from the entity *Users* to the entity *Local IT and Security Support* facilitates the relationship *Communicate*, and *Relationship* and *Trust* are attributes of that relationship.

Participants mentioned that they may avoid communication with central services if it is seen as involving a longer waiting time. Also, the majority of participants believe that it is important to have more of a personal relationship with IT and security staff, in order to build trust and effective communication. The participants that do have a local IT person or a departmental IT team report a more frequent and positive interaction, in comparison to the participants whose only recourse would be to contact the central service desk. For example, PE13 explains the difference in behaviour when interacting with local vs. central support:

> ‘*We had our own IT team and the benefits of that are, you know the guys, you know they’re just down the corridor from you. You know those IT guys well and you trust them. What used to happen, when I was based there, [...] if I saw an e-mail that I thought looked like a phishing attack, I would forward the e-mail to them and then say, flag it as this looks dodgy, to them. And then they would deal with it. They would make people aware you know be careful [...] But, now that [central help-desk] is a bit more remote [...] I mean they’re not physically down the corridor from me and I don’t really know those people face to face.*’—PE13.

When participants were asked whether they would prefer asking for help locally or from central services, most of them preferred a local alternative, unless they needed help with something quite specific, as ‘*the local IT manager is maybe more pertinent to me because I know the person, [they are] a colleague of mine.*’ (PE11). Crucially, several participants mention that they feel more comfortable and potentially less embarrassed to get help from somebody they feel they know or somebody who is physically located closer to their office. A preference for seeking IT help from someone who is seen as hav-

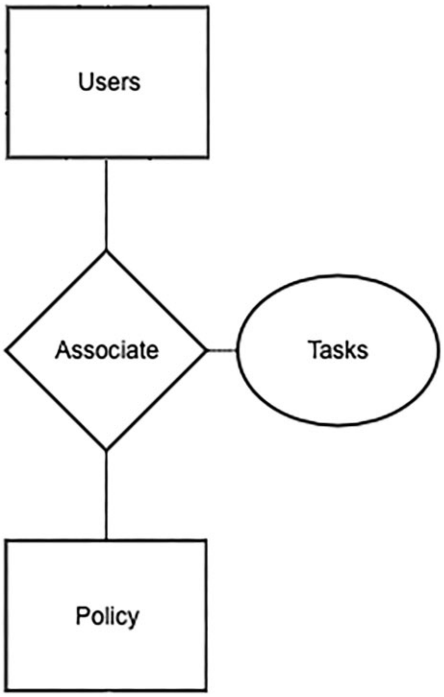


Figure 7. Entity-relationship diagram for theme T4A: 'Relating security to everyday tasks'.

ing an existing understanding of personal IT needs has been noted for home users [12, 51]. Kirlappos and Sasse [52] noted that trust between employees can clash with the trust promoted by following top-level policies (e.g. if a policy requires screen-locking even in the midst of colleagues); here, we find that support teams serve a purpose as a mediator between the two.

One participant specifically mentioned an approach called 'management by walking', suggesting someone from central help-desk could walk around and introduce themselves to staff. The participant believes this would make the experience more human and future interactions more approachable. The work of Harvey Molotch in assessing, e.g. airport and subway safety advocates such an approach also for understanding how infrastructure is experienced 'on the ground' by those who must use it [53].

T4A: relating security to everyday tasks

Representation in the conceptual model (Fig. 7). The link from the entity *Users* to the entity *Policy* represents the relationship *Associate*, and *Tasks* is an attribute of that relationship, meaning that users associate security policy with their tasks.

An immediate takeaway from the interview results is that participants associate security with various terms and concepts, most frequently with tasks familiar and relevant to them personally. When first asked about security, most participants mention data privacy or data protection as well as physical campus security. Almost reflexively, they then link these concepts to their daily work and give examples of tasks they usually complete to stay 'secure' in the workplace, e.g. '*I guess the only security part of it is monitoring visitor access cards.*'—PE3.

Although many participants do not immediately mention security tasks, most appear familiar with security when prompted further. Overall, any lack of knowledge or awareness about security practices cannot be attributed to a lack of interest or awareness about the importance of security. On the contrary, the majority of participants acknowledge the importance of being secure at the workplace and do not object to the additional effort that may be necessary. However, a difficulty conveyed by participants was in mapping security to concrete tasks. This appeared to stem from participants' lack of knowing all the ways in which security was involved in their daily tasks.

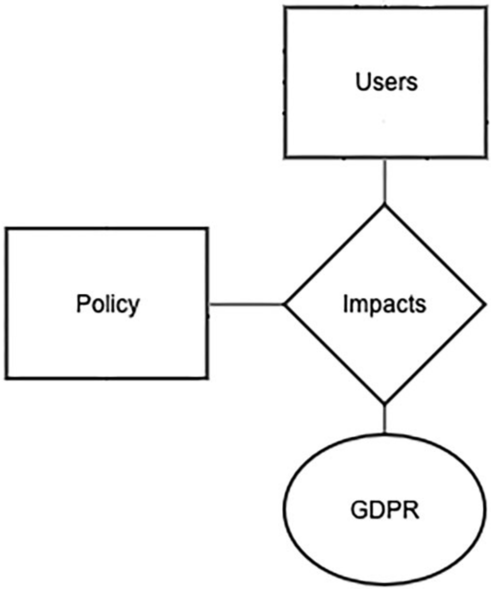


Figure 8. Entity-relationship diagram for theme T5A: 'The impact of GDPR on security awareness'.

As a constructive example, many participants mentioned GDPR when the topic of information security was brought up, e.g. PE5, '*we are being very careful about GDPR and [...] try not to leave anything on our desks.*', and '*Security fits into my day because, as you might expect, I see quite a lot of confidential information. So, on the most basic level [including payment details] that's GDPR level of personal information.*'—PE10. These excerpts demonstrate where participants saw a direct relation between a tangible workplace behaviour and a set of rules issued by the organization. Participants took the opportunity to suggest ways to make these connections more often, such as through scenario-based content, tailored messages, and real-world examples. Another suggestion is to provide easy checklists, or 'golden rules' to follow, with very clear messaging, but, crucially, so that less is left up to the reader's interpretation.

T5A: the impact of GDPR on security awareness

Representation in the conceptual model (Fig. 8). The link from the entity *Users* to the entity *Policy* facilitates the relationship *Impacts*, and *GDPR* is an attribute of that relationship.

Awareness of GDPR among participants was strong, with this being attributed to a clear organization-wide buy-in, and the link to everyday tasks seeming to be clear: '*Everyone's thinking quite a lot about GDPR, [...] that message has come down very strongly. [...] Because a lot of people in our office work with student records [...] people are fairly cognisant of the need to be sensitive with data and things like that.*'—PE9.

Moreover, the introduction of GDPR practices appears to have had an influence on security practices as well. For instance, some of the GDPR training materials helped to clarify the motivation behind using certain security controls, such as a Virtual Private Network

(VPN): '*I think probably GDPR did a lot in terms of information security because it spread the awareness of the few basic principles of you know, who is this information related to, who needs to see it and what level of access I give to people.*'—PE7.

Generally across our participants, there was an association of security tasks and policies with data protection, as most participants are obliged to comply with GDPR as part of their job. In contrast, those who did recall receiving security training almost exclusively related this to their induction when joining the university: '*with GDPR it kind of clarified what [current workplace] systems were because I was a bit confused with the Sharepoint, OneDrive, VPN, Dropbox, all these things. So, this tutorial, [current workplace] mandatory training was very beneficial in explaining different systems and why they needed to be used.*'—PE11.

When asked whether security comes up in conversations with coworkers, the association with GDPR would often surface again, as for PE8: '*It does come up, particularly in HR areas and sort of GDPR areas, for want of a better term. So, it's like we can do this, we can't do this because of GDPR. And I know it's not exactly the same as information security, but it makes you think about what information you can and can't pass down and how secure information is. [...] I think will I put this on an e-mail, will I put it on the Dropbox [...] what is the most secure way of putting that information which is confidential so that only certain people can access it?*'—PE8.

Summary

The themes presented in Section 4.1, namely, Behaviour is not guided by policy directly (T1A), Central mandates made actionable locally (T2A), Personal relationships with IT and security support build trust (T3A), Relating security to every day tasks (T4A), and Impact of GDPR on security awareness (T5A), were produced in the first iteration of the translation zone cycle.

We aimed to distil the overall themes from the qualitative work as—or related to—exchangeable artefacts. For example, in the theme *Behaviour is not guided by policy directly*, behaviour was our side of the translation zone, and policy was on the decision-maker stakeholder's side, whereas guidance was the exchangeable artefact in the translation zone. We communicated to the security manager that local understanding was important to employees, as was being able to put security advice into context; this highlighted the role of managers ahead of policy in communicating security, for instance.

Another example is the theme *Relating security to everyday tasks*, where the decision-maker stakeholder had knowledge of security practices at the university. We modelled the everyday tasks through the interviews, and discussed the relationship between the two in the translation zone. We took these themes into the next discussion with the decision-maker stakeholder and agreed that more information was necessary. The next important cycle would be to conduct interviews with IT and security support: although managers were guiding employees' security behaviours locally, where a relationship with 'central' security policy was missing there was instead a reliance on IT support teams to provide relevant security-related guidance. What we saw in practice with administrative employees was in essence along the same lines of a a primary recommendation in earlier research of 'Shadow Security' behaviours [15], informing locally derived working practices with security knowledge, rather than supplanting those behaviours entirely with security-focused behaviours, which dismiss the need to maintain productivity and applicability to local context.

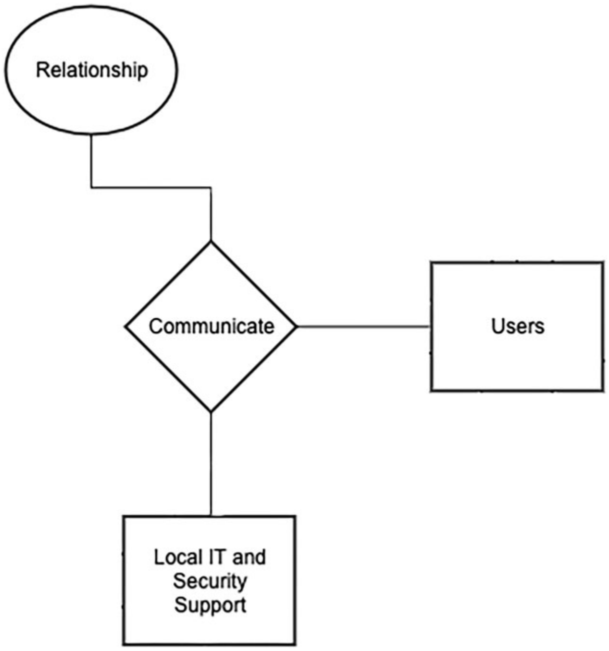


Figure 9. Entity-relationship diagram for theme T6S: 'Local support teams build relationships'.

IT and security support

T6S: local support teams build relationships

Representation in the conceptual model (Fig. 9). The link from the entity *Local IT and Security Support* to the entity *Users* represents the relationship *Communicate*, and *Relationship* is an attribute of that relationship.

Local support teams have the opportunity to build a relationship with their users. They are 'just down the corridor', and as PS5 put it, they are: '*friendly, local, and quick*'. According to IT and security support, users prefer to approach someone they know and trust, rather than a stranger who has no understanding of their history (as noted elsewhere in discussion of 'informal' technical support [12]). In terms of employees adopting secure behaviours, users are seen as often feeling embarrassed about asking 'stupid questions', and a choice to talk to local support is in part due to feeling that they will not be judged, and '*Yeah, we are not exactly going to broadcast it, what comes to us stays with us.*'—PS7.

Local support staff such as PS7 would make an effort to get to know their users, learning about their way of working, and thus providing a more personalized experience: '*there is that connection. There is not this nameless faceless person, who doesn't maybe know my history or even just [that] the way I work is quirky or different.*'—PS7.

The 'lockdown' restrictions related to the Covid-19 pandemic have made it difficult to maintain the same type of in-person communication. While most local teams usually have an 'open-door' policy, Covid-19 'lockdown' practices have limited users' opportunity to pass by with queries in an *ad hoc* manner (as noted in research with system administrators in the immediate aftermath of the pandemic [45]). Local support staff expressed that they continue to maintain interactions, either through the phone or via Teams, and still try to accommodate physical appointments when possible and in accordance with the restrictions (for instance, knowing when employees will be at the office, to then also be there if support might be needed).

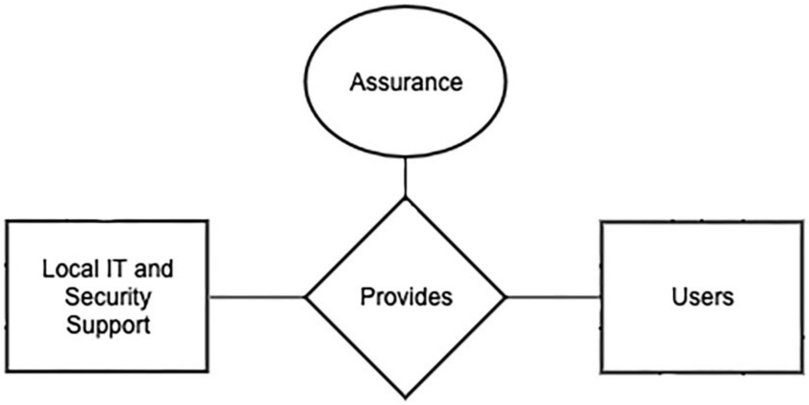


Figure 10. Entity-relationship diagram for theme T7S: 'Giving assurance rather than guidance'.

T7S: giving assurance rather than guidance

Representation in the conceptual model (Fig. 10). The link from the entity *Local IT and Security Support* to the entity *Users* facilitates the relationship *Provides*, and *Assurance* is an attribute of that relationship.

Support participants stated that there is guidance for a variety of topics, which has been made accessible, either on the central university website, on local sites or forums, or via e-mail correspondence. However, these materials were seen as lacking a level of assurance. Users prefer to get confirmation from a person that what they are doing is correct, rather than interpreting the guidance themselves. This was represented in that there may be many tickets about topics for which there is already guidance available, and the tickets would often be seen as trivial to solve, from an IT and security perspective; this was in essence laying the groundwork of a safe space for users, so that they would reach out if faced with something more serious later. One participant elaborates this further:

> '*Without the trivial engagement, when someone is new and you've given them their password, or their new laptop, [...] it's what creates community, and it's what gives that person the understanding that they can come to us down the line that's going to be more beneficial for them. But, having engaged with us on the trivial, I think makes them more likely to come to us with the more complex stuff where we can actually help them where they couldn't help themselves.*'—PS3.

Although there is value in trying to make guidance more appropriate and engaging for users, IT and security support believe that sometimes even if guidance is available in abundance, there are users who need human interaction and *assurance*. When they are unsure of how to do something securely, it helps to receive some type of approval from the experts whom they trust:

> '*Absolutely, yeah there are some people that just want to make sure because when they read that information, they are not confident enough to make a decision. So, maybe they just need some approval or confirmation that okay you're doing the right thing [...] they'll tell you oh I just wanted to make sure.*'—PS2.

Blythe *et al*. [3] note that *response efficacy* was an issue for their participants, as to whether individuals behaviours were believed to be effective; here we find instead that there is hesitancy about knowing what the approved behaviours are. Blythe *et al*. [3] mention the importance of feedback as of further interest, where here we find an existing interaction point for this in workplaces; i.e. support teams. We then find evidence that *self-efficacy* and the belief a person has that they can enact a behaviour can be encouraged by leveraging existing (local and informal [12]) processes. Similarly, where Das *et al*. [54] have explored the *socialization* of security, and learning through communication with others, here we see that within that communication, there can be a purpose in explicitly legitimizing or approving a learned behaviour as secure.

T8S: asking for security advice is common

Representation in the conceptual model (Fig. 11). The link from the entity *Users* to the entity *Local IT and Security Support* denotes the relationship *Ask*, and *Advice* is an attribute of that relationship.

In line with the theme above, almost all participants reported that one of the most frequent security queries or tickets that they receive is users seeking advice. They often walk into the local office—e.g. to ask the local IT and security support for any advice on working securely abroad when they are travelling to another country. Others may send an e-mail when they are about to procure a new piece of software asking which one is the most secure one.

On the other hand, IT and security support also make recommendations proactively and advise users on whether they should stop or start doing something in order to be secure. One participant working in local capacity says:

> '*People will often ask us for advice, they'll say look I know what to do but I just want to check. And that's because of that culture that we've put in, ask us, we're busy, but ask as anyway, we'd rather you get it right than get it wrong. And I'd say probably 25% of the time we do pick up on something and advise somebody and say that was a good point, but actually, did you know you could do it better*'—PS5.

This proactive dispensing of advice where it is known it will be relevant is again similar to findings from 'informal' technical support for members of the public [12].

T9S: security of behaviours varies between individuals and groups

Representation in the conceptual model (Fig. 12). The link from the entity *Users* to the entity *Security* facilitates the relationship *Varies*, meaning that the security behaviours of users vary.

There is an overall view that users differ in terms of there being those who would immediately contact IT and security support regardless of the issue, and those who will take a few steps on their own first before deciding to contact support. The people in the second category might first try to search online for information about an issue, or ask their colleagues, consult their manager, and so on. Several participants elaborate on this, for example:

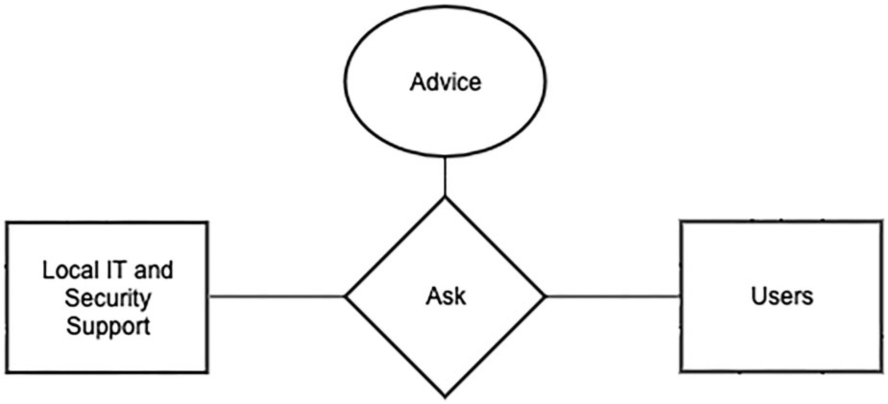


Figure 11. Entity-relationship diagram for theme T8S: 'Asking for security advice is common'.

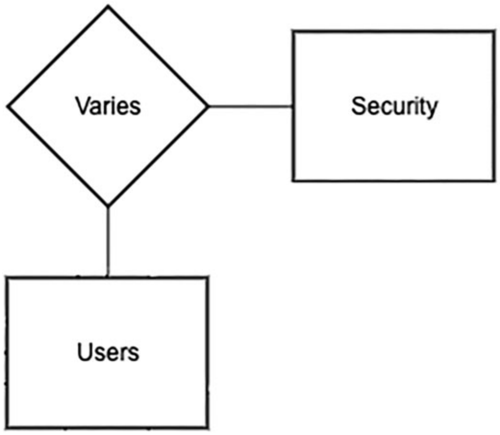


Figure 12. Entity-relationship diagram for theme T9S: 'Security of behaviours varies between individuals and groups'.

> '*It's not just security related, but it's sort of evidenced in security matters, there's one sort of person that gets in touch at the first sign of needing to, or there being any IT issue. And there's another sort of person who leaves it and tries to figure stuff out and only gets in touch when it becomes an actual problem. And, I think, for the security type stuff, probably people in the second groups, means we don't actually see everything that's going on.*'—PS3.

That some users may prefer to take matters into their own hand, and try to resolve or abandon the issue rather than contact support, may then mean that IT and security support do not always have oversight over nonsecure behaviours. A reluctance to reach out to support or even report something may sometimes be due to long-term aspects of workplace culture '*that we've always done it this way*'—PS2, where '*It's not easy to change those individuals to adapt to better ways of doing things [...] Especially if they feel like it's always been working for them*'—PS2.

PS3 summarized a general order of how queries may reach them, where '*they'd rather talk to each other, and then they'd rather talk to local IT support, then they might talk to central, but they might not*'—PS3.

Summary

Similarly to the previous cycle with administrative staff, we analysed the interviews with support staff, adding further detail to themes developed for the translation zone with security management staff. The availability/visibility of support staff T6S) and role of assurance T7S) were key findings from this round of interviews.

We then took the themes back into another discussion with the decision-maker stakeholder, as well as an additional decision-maker stakeholder transitioning into a similar role as security manager to take over those duties. All themes were part of that discussion, having been enriched by a second iteration of the translation zone.

Reflection by policy decision-makers

The two security managers, responsible for higher-level security strategy such as security policies and procurement decisions, reflected upon the themes from the interviews (Sections 4.1 and 4.2), as presented to them.

Discussion with security managers was guided by the overall themes as in Table 1. The conceptual model (Fig. 3 was then useful for the discussion—the translation zone—as it allowed us to 'zoom in' on specific elements within the themes when the security managers explored the meaning and available next steps in response to individual themes. This is reflected in the expansion of each theme in individual subsections of our interview Results.

It was noted that IT cannot drive a change of culture alone, and that IT teams '*do not have the tools to achieve the change*', with this being about remit rather than power. The managers spoke instead of supporting the mission of the organization, that security is not the primary purpose of the organization, and although '*security is important*', this is because of what the rest of the organization is doing that their teams are supporting (where this broadened the themes around providing support). This in turn pointed to the alignment of security messaging with the organization's strategic direction, to values in terms of enabling people to do their job safer or in a more compliant way, or as an improvement; e.g. being able to send data in a safer way (relating to the specific theme of GDPR as having a lot of attention—Theme T5A).

An additional area of focus was on rolling out secure technologies, 'to be more secure from the outset', and 'if something goes wrong we can stop and help', rather than security being everybody's responsibility. This relates to the distinctions made by Pallas [17] on organizational security provisioning, between large one-time investments in security technologies, and lower-cost user-level activities such as training, where the latter can nonetheless involve higher costs due to the need to proactively manage for noncompliant behaviours. Regarding employees generally, it was seen as '*its about how we get the same message to people in a way that is relevant to them*', in terms of understanding local risks; Beris *et al*. [55] make a distinction between sentiment toward security apparatus, and ability to recognize risks in the workplace which then activate interaction with security controls.

When considering our study as a first step in a continuous process of using models to empower security management, the security managers suggested to look externally in further work, and involve security solution vendors. Specifically, vendors may argue that deciding how much security to have is an organization's choice as a consumer; however, the argument was made here that '*security should not be a bolt-on any more; allow choice with a baseline*'. That is, ensure that a reasonable level of security is provided by default, *then* allow additional options on top of that.

In line with the support staff interviews (Section 4.2), the managers stressed the importance of '*removing the stigma of raising questions about security*', and employees reaching '*a comfort level to be able to ask when they don't know*', signalling the cultural aspects of having approachable, local IT support. The managers believed this relied also on engagement from their side, and '*becoming a visible business partner*'. The managers also discussed the role of policy in light of our findings; i.e. that '*policy is for taking someone to task; even if people ask for an exception to do things in a better way*'. The key point in this is to drive engagement and find workable solutions. This is in line with existing research [4, 8]. However, here it is noted that support staff also may have questions about how things work, so it is necessary to provide support outwards from the security experts to support teams as well as employees.

The managers noted that our co-design methodology '*confirmed their intuition*', but that the *evidence* was useful for them, for informing and bolstering decision-making in the company of other decision-maker stakeholders beyond security. The managers would have the cocreation process go into generating more information, i.e. of practical use; e.g. '*how do we resolve some of this?*' or '*how do we test whether we're doing it right?*'. This points to a further element of our approach; research producing scientific evidence, but also evidence that can inform real-world security decisions, where the two are not necessarily synonymous without an integrated approach that considers the working 'model' of decision-maker stakeholders responsible for managing the systems that are being researched. We consider further, targeted data collection in the Limitations and Recommendations in the next section towards future work, especially towards reducing workplace security dilemmas for employees.

The security managers we were working with had some initial sense 'from afar' about what was going on but wanted to get a better sense of it directly from source. Themes were not completely unknown or surprising, but the model and interview outcomes helped to confirm existing assumptions and explore the connection to decisions within the managers' remit. This then prompted the discussion of the limits to their capabilities as relate to policies and external suppliers.

Discussion

Reflecting upon the interviews with employees (Section 4.1), participants noted security as important, but it was often discussed relative to daily tasks and terms relating to data privacy and protection rather than security details directly. The majority of participants implied that they had limited recollection of security policy and security training, but that experience and intuition played a role in guiding their security behaviours. Sources of guidance linked more closely to how they worked had the greatest utility, such as help from coworkers and managers (where the latter may include arranging training), the local IT person/team or potentially a mixture of all of these.

Several participants also noted their own initiatives and security practices in the organization as well as how they help coworkers with security. Ultimately, security behaviours are not embodied in one policy document alone, but are a sum of guidance material, help from others who understand personal working practices and needs (be they colleagues or recognized IT support staff), and a kind of 'oscillation' [13] between being nonsecure and secure, of signalling when not sure of how to do something, and being guided towards how to work securely in what may be an unfamiliar situation or one that implies caution should be taken. Such a view, of care for the security-related norms and values in an organization, goes beyond present references to the concept of a 'security culture' as being 'how we do things around here', by exploring how users are guided to 'do things' in a secure way.

When in need, participants will call upon local IT support where it is available. In general, most participants are more likely to ask for help from someone they already know (Themes T3A and T8S), such as their manager or a tech-savvy coworker, rather than approach a relative stranger at the service desk—somebody who understands something of their work and goals (Themes T2A, T3A, T4A, and Themes T6S and T9S). As noted in our interviews with both employee groups, this has parallels with informal technical support for individual members of the public [12]. Here, this support is attributed to the opportunities for building relationships with 'local' people in general. More specifically, there is a mutual understanding between the users and the local IT and security support that their relationship is built on openness and trust (Themes T3A, T6S, and T7S). These types of interactions with local support may positively influence users' willingness to ask for security advice, or even to get in contact when something goes wrong. If support is not actionable or not visible, employees may develop their own 'shadow security' approaches to working securely [15].

When discussing the availability and adequacy of guidance with IT and security support, there seemed to be a shift throughout the conversation; although they saw value in tailoring guidance to users, as well as making it more practical, they also highlighted the importance of giving assurance to users (Theme T7S). Local support staff claimed that many queries and tickets are trivial to solve from their perspective, but although the guidance is predominantly available, and often fit for purpose, many users require a level of confirmation *that what they are doing is what was intended*. They prefer to be reassured that their behaviour or practices are secure rather than having to make that judgement about themselves, upon themselves. This relates to contradictions in how security is typically managed in organizations, deciding that employees need to be trained, but that they know security well enough to adopt secure practices with incomplete information as if they are experts [56] (we see this in Fig. 3) where the employees in Local IT Teams enforce rules, but also provide guidance and assurance to users).

In the shift to remote working, there is less visibility of security practices as well as perceived barriers to communication [45]. When the 'lockdown' was introduced, administrative staff worried about how they would get anything done, as collaboration with others was part of their way of working. An important part of that collaboration is the ability to communicate effectively. One participant reflected on how '*you could normally raise your head above the screen and ask a question*' (PE7), whereas during the 'lockdown' they became more reluctant to reach out to each other remotely to avoid being bothersome. While technology has enabled communication during Covid-

19 in one way, it has also hindered it in another way, by reducing opportunistic communication.

In terms of IT and security support, remote working seems to have impacted interactions between users and local services more than those between users and central services. This may be due to the differences in communication style to begin with, with local support always keeping their door open for physical interactions, and central services communicating remotely most of the time. Local staff continue to make efforts in accommodating their users, where a big part of this accommodation is in facilitating in-person support every now and then, in line with Covid-19 restrictions and recommendations.

Previous research indicates that when there is a need for IT or security support, people may also choose to ask their friends or family for advice [12]. During the interviews, administrative staff acknowledged that they often observe the behaviours of others, be it family, or coworkers, and sometimes learn about security through these observations (Theme T4A). This further emphasizes the importance of visibility in security support, and the championing of secure behaviours in the organization.

Limitations

It was made clear to all participants that we would be communicating summary themes to the security management decision-makers, under conditions of anonymity. There is potential for this to have acted as a barrier to engagement by employees, but our participants nonetheless voiced concerns and offered alternatives to the existing security provisions. Similarly, support staff often talked positively about how they support employees, which may have indicated a bias in praising their own work, but they also provided concrete examples of positive engagements and of where negative outcomes could arise. They were also able to relate their experiences as reasoning to explain phenomena seen in, e.g. the ticketing system (such as why there would be a great number of seemingly trivial tickets for issues where guidance was already provided, as a signal that direct assurance was amiss).

To consider this engagement as a specific case study [57], here we have focused on a large university; it has many thousands of active users, like other large organizations, but is decentralized and not necessarily governed by one centralized IT system, much like smaller businesses [58]. In consultation with the security managers, we knowingly selected employee participant groups based on their use of managed infrastructure, where most organizations will have teams dedicated to working with sensitive or high-value information. With this, there may also be limitations to how well the model developed here would apply to other organizations—the model, for instance, presumes the presence of 'local' IT teams. However, many larger organizations will have centralized IT teams, GDPR compliance expectations, and materials guiding users on how to secure their work (as are also here). Future work will examine the capacity to reuse or combine regularly found elements of models created in the same manner across organizations. In this way, continued interview phases would add to the model, limited to the infrastructure that a security manager can make decisions about; a model such as this also demonstrates its usefulness if it can be used to support a dialogue with employees [5, 40].

Recommendations and future work

Below are recommendations which emerged from the research study, which can be regarded as interrelated.

- Leverage local expertise to communicate security policy: security policy is a useful tool for articulating compliance expectations, but is not the way employees 'live' security. Communication efforts can support the intentions of policy, where this can include supporting IT and security teams in ways to be more personable. Although local IT teams are referred to in terms of their proximity to employees' work, our interviews surfaced that what was of great value was the *approachability* that this engendered. Local representatives are a conduit for two-way communication of security concerns, but also for validating behaviours and *legitimizing* security behaviours for nonexpert employees when they have learned them, providing a highly valued confirmation that a behaviour is correct. We saw that support staff would provide a *prompt* [59] to employees that they are 'correct' and have approval to activate their existing motivation and ability, so that employees actively practice the behaviour. This represents 'knowing I'm doing the thing right', as opposed to only 'knowing the right thing to do'. This builds on the behaviour dimension of *actionability* as described by Redmiles *et al.* [60], by activating actionable behaviour through assurance from someone who understands the person's existing behaviours [12] and has the expertise to 'approve' the behaviour. It would then be necessary to dedicate resource to allow support staff the capacity to engage in these currently invisible conversations with employees about how to enact security behaviours correctly (as has also been seen elsewhere in research with system administrators [45]).
- Maintain an awareness of the wider security ecosystem and related infrastructure decisions: the co-design process followed during this work helped us create a conceptual model of the organization, which captured the entities, attributes, and relationships of the system. This approach, including the translation zone, led both researchers and decision-maker stakeholders to a more systematic understanding of the organization, including the effectiveness of policies, how groups within the organization interact, and where changes and improvements can feasibly be made, i.e. the decision points in the system. Maintaining such a systematic understanding—in this case via a conceptual model—then informs how an organization designs future (security) policy changes effectively. When researchers study users in a managed environment, it is then useful to have a model—with qualities similar to the one described here—to engage the security manager/decision-maker. Fundamentally, where there are points where user experience could be improved, it is useful to pinpoint these and convey them to the decision-maker, to explore what their options are within their resources and remit.
- Explore the role of stories and structured vignettes: the model captures the experiences of employees; TA identified themes across the interviews, and codifying the elements of the themes allowed for connections to be made between employee groups, and with some elements of the organization's security infrastructure (as relate to the security manager, as the decision-maker who interacted with the model). Leveraging qualitative data to build models can also extend existing work, such as the survey-building approach in the Productive Security work [8] (where interviews were used to build scenarios). In such a way, stories—or vignettes—from employees can be codified, as with Productive Security, and encoded in an ontology not dissimilar from the entity-relationship diagrams here. For instance, Parkin *et al.* [40] proposed an ontology to capture news stories, to facilitate discussion between a small business leader and their IT provider, with common elements to allow for reasoning from both sides. Where Productive Security [8] used interview themes to build scenarios, vignettes can be developed and encoded in a model to convey

employee 'dilemmas' to security decision-makers. A similar approach has been used to consider the role of smart device manufacturers when device users face security dilemmas, for instance [61].

Conclusion

Acknowledging the complex, multistakeholder nature of security in organizations, we have introduced a modelling methodology based on co-design principles that incorporates qualitative, user-centred research. This methodology enriches existing modelling approaches by introducing a 'translation zone' within which successive iterations and interactions between modellers and decision-maker stakeholders are used to construct candidate models. These candidate models are further refined, in the usual way, by comparison with observations of the domain. The components of the conceptual model we have developed are the following: an in-depth understanding of the system; an understanding of the interaction between different employee groups and decision-maker stakeholders in the organization; and knowledge of the organizational structure and policies intended to be applied to the system.

We have demonstrated how to use this conceptual model to bring out recommendations that can inform security policy design, communication, and decision-making. The outcome of this study has been a range of coexplored recommendations for improving security decisions, policy design, and communication in the organization. The recommendations include the following:

- Leveraging the expertise of local staff and their approachability to communicate security policy.
- Applying a co-design approach to understand better the context of the system.
- Explore encoding of identifiable workplace 'dilemmas' in a structured model, to support manager decisions.

Through this novel co-design-based modelling methodology, applied in collaboration with administrative staff at a large university with a high number of employees, our work has informed the conversation around 'security culture' and its relationship with skills and expectations associated with other nonsecurity behaviours in the workplace. Future work will explore the involvement of a wider range of stakeholder groups in the iterative co-design modelling process, which will include further engagement across and external to organizations.

Acknowledgements

The authors wish to thank the interview participants and the organization's security managers for their contributions to the study, including their time, and their feedback.

Author contributions

Albesë Demjaha (Conceptualization, Data curation, Methodology, Project administration, Resources, Validation, Visualization, Writing – original draft, Writing – review & editing), David Pym (Conceptualization, Methodology, Project administration, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing), Tristan Caulfield (Conceptualization, Methodology, Visualization, Writing – original draft), and Simon Parkin (Conceptualization, Methodology, Project administration, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing)

Conflict of interest: None declared.

Funding

None declared.

Appendix A: employee interview questions

Introductory questions:

(1) What do you do here?
(2) How long have you been working here?
    (a) Have you worked anywhere else that compares (or not) in some way?
(3) Can you describe your typical working day at the university?
(4) Where does your way of working come from?
    (a) The way things have been done?
    (b) A policy you know about or have read?
    (c) Security awareness/training you have done?
    (d) What is it that makes a behaviour adoptable?
    (e) What would have to happen outside of that behaviour that would help you learn it?

Security practices:

(1) How does technology factor in your work?
    (a) Does it help in any ways?
    (b) Does it get in the way of your work in any ways?
(2) How does security fit in to your day?
    (a) Are there particular tasks you do in your work, which are related to information security?/how often?
    (b) Probe: sensitive data/information, clear desk policy and sharing workspaces, physical security/tailgating, passwords, sharing data/USB sticks and sharing by emails, phishing.

Decision-making and policies:

(1) Is there a security policy within the organization?
    (a) Is this a departmental one or university-wide? (for people not in central services)
(2) How much would you say you know about the content?
(3) What security training, if any, have you received to date?
(4) Have you ever received any security communication?
(5) How effective was it in your view?
(6) What do you see as the pros and cons of security policies?
(7) Do the rules you follow work well?
    (a) If so, in what ways?
    (b) If not, what do you think should change, and in what way?
(8) How often do you think people generally follow the policy rules?
(9) If you see people behaving securely—how do you feel about that?
    (a) Good, bad, or waste of time.
(10) Is it clear from the policy what noncompliance is?
(11) Does the policy say anything about reporting an incident?
(12) How does the culture compare to health and safety and physical security?
(13) What risks do you think failing to comply with security policy poses to the org?

Organizational culture:

(General probe: (if applicable) how does this compare to other places you have worked at?)

(1) How would you describe the working culture around here?
    (a) What is important in that culture?
    (b) What is recognized and rewarded?
    (c) Do you see staff here pushing themselves in any way to meet those expectations?
(2) How do you usually do things around here? (further probe—do you do them as you're told, as others do them, or in your own way?)
    (a) Probe: shared beliefs/values
    (b) Probe: shared norms (ways of doing things)
    (c) Who are these approaches shared with (certain colleagues, an entire team, or the university)?

(d) How are these approaches shared? (e-mail, conversation, and so on)

(3) Could you talk through an example of the way you work with others to get things done?

(a) Do they need to be done this way for a reason?

(4) (If previous answers indicate they are a ‘new’ employee) Can you give examples of behaviours you are expected to adopt in order to fit in?

(a) Do you adopt these behaviours and why?

Appendix B: support staff interview questions

Contextual questions:

(1) How long have you worked here?

(2) Could you describe an hour of your working day? (focus: processes, way of working, and routines)

(3) How many people are there in your division/department? (e.g. central helpdesk vs. security helpdesk)

(4) How many people are there in your team?

Ticketing system:

(1) How many users do you have?

(2) How are tickets assigned?

(3) What are the different ways people can contact you with a query? (e.g. phone, e-mail, online form/another tool, dropping in, and so on)

(4) Which is the most common way to submit a query/ticket?

(5) Are all queries logged as tickets?

(a) If not (or if queries are logged informally), why/when does that happen?

(6) Do users rank tickets by severity? (e.g. urgent or medium)

(a) If not, how are tickets prioritized?

Security tickets:

(1) How much of the tickets that you get are security tickets?

(2) What kind of security tickets do you get?

(3) How many security tickets per day do you/your team receive on average?

(4) How many security tickets per day do you solve on average?

(5) How long does it take on average to resolve a security ticket?

(6) Do you get certain security queries more than others?

(a) If yes, which are the 3–5 most common?

(7) Do you often get security queries that are meant for another team/department?

(a) If yes, what is the process of handling such queries? (e.g. reject, help anyway, delegate, or reject and redirect)

(b) Are there certain queries that you get by mistake more frequently? Why do you think that is?

(8) Are security tickets prioritized over nonsecurity tickets by default?

(9) Do you ever notice an unusually low number of tickets?

(a) If yes, do you follow-up on that?

(10) Do you feel that you ever have time to proactively support people? (i.e. without them having to log tickets)

(11) Based on the things you just said, how would it affect your work if any of them went up or down?

Security behaviours:

(1) Do you have any sense of what happens before people decide to contact you regarding a query?

(2) Do you think they first attempt to solve it themselves?

(3) Do you think they try to find help/guidance on your website?

(4) Do you think they ask someone in their team before coming to you?

(5) How frequently do people log issues that there is already guidance for?

(6) Do you think...

(a) There are queries that would be trivial to solve if people have access to the right information?

(b) That there is guidance available, but they cannot find it?

(c) That there is guidance available, but they cannot understand it?

(d) That there is guidance available, they are able to resolve the issue, but prefer assistance?

(7) Are there queries that would be trivial to solve but for which there is no available guidance?

(8) How would it affect your work if they were able to find the guidance?

(9) How often do people come back with the same problem? (e.g. a ticket that has already been resolved)

(10) What would you say a ‘good’ number of queries/tickets would look like?

(11) On a percentage scale, how secure would you say most behaviours are?

(12) Are there certain behaviours which are followed in a more/less secure way than others?

(13) Do people ever log a ticket to seek advice (about how to do something securely) rather than to resolve a particular issue?

(14) Do people ever log a security problem after it has broken their computer and they are terrified?

Remote working:

(1) What has changed the most about your way of working since ‘lockdown’?

(2) Do people come to you as much as before the ‘lockdown’?

(3) With the new policy, have you seen people come to you with questions?

Additional group specific questions:
Central support staff:
(after remote working questions)

(1) How was the policy launched and communicated to people?

(2) Do you think it’s useful to have local IT teams/person?

(a) Why yes/no?

(3) Have you noticed any key differences between departments that have vs. departments that do not have a local IT team/person?

Security support staff:

(1) Are there any queries that can only be solved by the security helpdesk?

(2) Do you think people fully understand when they should explicitly come to you?

Local IT:
(after remote working questions)

(1) Were you already guiding people on that?

(2) Did you notice people coming to you more when the e-mail was sent out?

(3) Have you noticed a lot of people having the same questions about it?

(4) When a new policy is introduced, do you get a sense that it takes time to adapt to new practices?

(5) Do you feel that people in the department trust you and feel comfortable coming to you with queries?

(6) If yes, why do you think that is?

(7) Do you think they prefer coming to you vs. central helpdesk and why?

(8) What fraction of queries are you able to solve without escalating to central IT?

(9) What type of queries are most likely to be escalated to central IT and why?

(10) Is there a local system of tracking queries?

(11) What is the local culture like in terms of people asking for help?

(12) Do you think that people ask each other what to do before calling someone?

(13) Have you noticed specific groups that behave differently in this respect? (e.g. managers vs. other employees)

References

1. Beautement A, Sasse MA, Wonham M. The compliance budget: managing security behaviour in organisations. In: *Proceedings of the 2008 New Security Paradigms Workshop*. New York: ACM, 2008, 47–58.

2. Adams A, Sasse MA. Users are not the enemy. *Commun ACM* 1999;**42**:40–6. https://doi.org/10.1145/322796.322806.

3. Blythe JM, Coventry L, Little L. Unpacking security policy compliance: the motivators and barriers of employees’ security behaviors. In: *Proceed-*

ings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). Berkeley: USENIX Association, 2015, 103–22.

4. Zimmermann V, Renaud K. Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *Int J Hum Comput Stud* 2019;**131**:169–87. https://doi.org/10.1016/j.ijhcs.2019.05.005.
5. Ashenden D, Lawrence D. Security dialogues: building better relationships between security and business. *IEEE Secur Priv* 2016;**14**:82–7. https://doi.org/10.1109/MSP.2016.57.
6. Parkin S, Van Moorsel A, Inglesant P,. *et al.* A stealth approach to usable security: helping IT security managers to identify workable security solutions. In: *Proceedings of the 2010 New Security Paradigms Workshop*. New York: ACM, 2010, 33–50.
7. Reinfelder L, Landwirth R, Benenson Z. Security managers are not the enemy either. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York: ACM, 2019, 1–7.
8. Beautement A, Becker I, Parkin S,. *et al.* Productive security: a scalable methodology for analysing employee security behaviours. In: *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Berkley: USENIX Association, 2016, 253–70.
9. Spring JM, Moore T, Pym D. Practicing a science of security: a philosophy of science perspective. In: *Proceedings of the 2017 New Security Paradigms Workshop*. New York: ACM, 2017, 1–18.
10. Caulfield T, Ilau MC, Pym D. Meta-modelling for ecosystems security. In: *Proceedings of the International Conference on Simulation Tools and Techniques*. Berlin: Springer, 2022, 259–83.
11. Caulfield T, Ilau MC, Pym D. Engineering ecosystem models: semantics and pragmatics. In: D Jiang, H Song, (eds), *Simulation Tools and Techniques*. Cham: Springer International Publishing, 2022, 236–58.
12. Poole ES, Chetty M, Morgan T,. *et al.* Computer help at home: methods and motivations for informal technical support. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM, 2009, 739–48.
13. Kocksch L, Korn M, Poller A,. *et al.* Caring for IT security: accountabilities, moralities, and oscillations in IT security practices. *Proc ACM Hum Comput Inter* 2018;**2**:1–20. https://doi.org/10.1145/3274361.
14. Kirlappos I, Beautement A, Sasse MA. 'Comply or Die' is dead: long live security-aware principal agents. In: *Proceedings of the International Conference on Financial Cryptography and Data Security*. Berlin: Springer, 2013, 70–82.
15. Kirlappos I, Parkin S, Sasse MA. Learning from 'Shadow Security': Why understanding non-compliance provides the basis for effective security. In: *Workshop on Usable Security (USEC) 2014*. San Diego: NDSS, 2014.
16. Parsons K, Calic D, Pattinson M,. *et al.* The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Comput Secur* 2017;**66**:40–51. https://doi.org/10.1016/j.cose.2017.01.004.
17. Pallas F. Information Security Inside Organizations-A Positive Model and Some Normative Arguments Based on New Institutional Economics. *TU Berlin Inf Syst Eng* 2009.
18. Bauer S, Bernroider EW, Chudzikowski K. End user information security awareness programs for improving information security in banking organizations: preliminary results from an exploratory study. In: *Proceedings of the AIS SIGSEC Workshop on Information Security and Privacy (WISP 2013), Milano*. Atlanta: Association for Information Systems, 2013.
19. Bada M, Sasse AM, Nurse JR. Cyber security awareness campaigns: Why do they fail to change behaviour?. In: *Proceedings of the International Conference on Cyber Security for Sustainable Society*. Coventry: Sustainable Society Network, 2019.
20. Beyer M, Ahmed S, Doerlemann K,. *et al.* Awareness is only the first step: a framework for progressive engagement of staff in cyber security. Business white paper. Palo Alto: Hewlett Packard, 2016.
21. Brostoff A. *Improving Password System Effectiveness*. London: University College London, University of London, 2005.
22. Ashenden D, Sasse A. CISOs and organisational culture: their own worst enemy?. *Comput Secur* 2013;**39**:396–405. https://doi.org/10.1016/j.cose.2013.09.004.
23. Pollini A, Callari TC, Tedeschi A,. *et al.* Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn Technol Work* 2021;**24**:1–20.
24. Wang S, Faklaris C, Lin J,. *et al.* 'It's Problematic but I'm not concerned': university perspectives on account sharing. In: *Proceedings of the CSCW 2022*. New York: ACM, 2022.
25. Heath C, Hall P, Coles-Kemp L. Holding on to dissensus: participatory interactions in security design. *Strateg Design Res J* 2018;**11**:65–78. https://doi.org/10.4013/sdrj.2018.112.03.
26. Voinov A, Jenni K, Gray S,. *et al.* Tools and methods in participatory modeling: selecting the right tool for the job. *Environ Model Softw* 2018;**109**:232–55. https://doi.org/10.1016/j.envsoft.2018.08.028.
27. Basco-Carrera L, Warren A, van Beek E,. *et al.* Collaborative modelling or participatory modelling? A framework for water resources management. *Environ Model Softw* 2017;**91**:95–110. https://doi.org/10.1016/j.envsoft.2017.01.014.
28. Landström C, Whatmore SJ, Lane SN,. *et al.* Coproducing flood risk knowledge: redistributing expertise in critical 'participatory modelling'. *Environ Plan A* 2011;**43**:1617–33. https://doi.org/10.1068/a43482.
29. Voinov A, Kolagani N, McCall MK,. *et al.* Modelling with stakeholders–next generation. *Environ Model Softw* 2016;**77**:196–220. https://doi.org/10.1016/j.envsoft.2015.11.016.
30. Demjaha A, Pym D, Caulfield T. Found in translation: co-design for security modelling. In: *Proceedings of the 11th Workshop of Socio Technical Aspects of Security (STAST)*. Berlin: Springer, 2022.
31. Schein EH, Schein PA. *Humble Inquiry: The Gentle Art of Asking Instead of Telling*. Oakland: Berrett-Koehler Publishers, 2021.
32. Braun V, Clarke V. One size fits all? What counts as quality practice in (reflexive) thematic analysis?. *Qual Res Psychol* 2020;**18**:1–25.
33. Fielder A, Panaousis E, Malacaria P,. *et al.* Decision support approaches for cyber security investment. *Decis Support Syst* 2016;**86**:13–23. https://doi.org/10.1016/j.dss.2016.02.012.
34. Caulfield T, Parkin S. Case study: predicting the impact of a physical access control intervention. In: *Proceedings of the Sixth Workshop on Socio-Technical Aspects in Security and Trust*. New York: ACM, 2016, 37–46.
35. Woods DW, Böhme R. SoK: quantifying cyber risk. In: *Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP)*. New York: IEEE, 2021, 211–28.
36. Hubbard DW, Seiersen R. *How To Measure Anything In Cybersecurity Risk*. Hoboken: John Wiley and Sons, 2016.
37. David S, Sabiescu AG, Cantoni L. Co-design with communities. A reflection on the literature. In: *Proceedings of the Seventh International Development Informatics Association Conference*. Pretoria: IDIA, 2013, 152–66.
38. Kleinsmann M, Valkenburg R. Barriers and enablers for creating shared understanding in co-design projects. *Design Stud* 2008;**29**:369–86. https://doi.org/10.1016/j.destud.2008.03.003.
39. Galison P. Trading with the enemy. In: *Trading Zones and Interactional Expertise: Creating New Kinds of Collaboration*. Vol. **25**. Cambridge: MIT Press, 2010, 52.
40. Parkin S, Arnell S, Ward J. Change that respects business expertise: stories as prompts for a conversation about organisation security. In: *Proceedings of the New Security Paradigms Workshop*. New York: ACM, 2021, 28–42.
41. Deal TE, Kennedy AA. *Corporate Cultures: The Rites and Rituals of Organizational Life*. Vol. **2**. Boston: Addison-Wesley, 1982, 98–103.
42. Da Veiga A,. *et al. Cultivating and assessing information security culture*. Ph.D. Thesis, University of Pretoria, 2008.
43. Schein EH. *Organizational Culture and Leadership*. Vol. **2**. Hoboken: John Wiley and Sons, 2010.
44. Kenneally E, Dittrich D. The Menlo Report: ethical principles guiding information and communication technology research. Washington: U.S. Department of Homeland Security Scienceand Technology, 2012.
45. Kaur M, Parkin S, Janssen M,. *et al.* "I needed to solve their overwhelmness": How system administration work was affected by COVID-19. In: *Proceedings of the 25th ACM Conference on Computer-Supported Cooperative Work and Social Computing*. New York: ACM, 2022.
46. Delfino GF, van der Kolk B. Remote working, management control changes and employee responses during the COVID-19 crisis. *Ac-*

count Audit Accoun J 2021;**34**:1376–87. https://doi.org/10.1108/AAAJ-06-2020-4657.

47. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol* 2006;**3**:77–101. https://doi.org/10.1191/1478088706qp063oa.
48. Weisbord MR. *Productive Workplaces Revisited: Dignity, Meaning, and Community in the 21st Century*. Hoboken: John Wiley and Sons, 2004.
49. Herley C, Pieters W. "If you were attacked, you'd be sorry" Counterfactuals as security arguments. In: *Proceedings of the 2015 New Security Paradigms Workshop*. New York: ACM, 2015, 112–23.
50. Becker I, Parkin S, Sasse MA. Finding security champions in blends of organisational culture. In: *Proceedings of the Workshop on Usable Security (USEC) 2017*. San Diego: NDSS, 2017.
51. Nthala N, Flechais I. Informal support networks: an investigation into home data security practices. In: *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Berkeley: USENIX Association, 2018, 63–82.
52. Kirlappos I, Sasse MA. What usable security really means: Trusting and engaging users. In: *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*. Berlin: Springer, 2014, 69–78.
53. Molotch H. Everyday security: default to decency. *IEEE Secur Priv* 2013;**11**:84–7. https://doi.org/10.1109/MSP.2013.142.
54. Das S, Dabbish LA, Hong JI. A typology of perceived triggers for {End-User} security and privacy behaviors. In: *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Berkeley: USENIX Association, 2019, 97–115.
55. Beris O, Beautement A, Sasse MA. 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*. New York: ACM, 2015, 73–84.
56. Demjaha A, Parkin S, Pym D. The boundedly rational employee: security economics for behaviour intervention support in organizations. *J Comput Secur* 2022;**30**:1–30.
57. Morgan MS. Resituating knowledge: generic strategies and case studies. *Philos Sci* 2014;**81**:1012–24. https://doi.org/10.1086/677888.
58. Parkin S, Fielder A, Ashby A. Pragmatic security: modelling it security management responsibilities for SME archetypes. In: *Proceedings of the Eighth ACM CCS International Workshop on Managing Insider Security Threats*. New York: ACM, 2016, 69–80.
59. Fogg BJ. *Tiny Habits: The Small Changes that Change Everything*. Eugene: Harvest, 2019.
60. Redmiles EM, Warford N, Jayanti A,. *et al*. A comprehensive quality evaluation of security and privacy advice on the web. In: *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*. Berkeley: USENIX Association, 2020, 89–108.
61. Kustosch L, Gañán C, Van't Schip M,. *et al*. Measuring up to (reasonable) consumer expectations: providing an empirical basis for holding {IoT} manufacturers legally responsible. In: *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*. Berkeley: USENIX Association, 2023, 1487–504.