Found in Translation: Co-design for Security Modelling

Albesë Demjaha[1,2], David Pym[1,3], and Tristan Caulfield[1]

[1] University College London
[2] The Alan Turing Institute
[3] The Institute of Philosophy, University of London
London, United Kingdom

Abstract. *Background.* In increasingly complex and dynamic environments, it is difficult to predict potential outcomes of security policies. Therefore, security managers (or other stakeholders) are often challenged with designing and implementing security policies without knowing the consequences for the organization. *Aim.* Modelling, as *a tool for thinking*, can help identify those consequences in advance as a way of managing decision-making risks and uncertainties. Our co-design approach aims to tackle the challenges of problem definition, data availability, and data collection associated with modelling behavioural and cultural aspects of security. *Method.* Our process of modelling co-design is a proposed solution to these challenges, in particular for models aiming to incorporate organizational security culture. We present a case study of a long-term study at Company A, where using the methods of participatory action research, humble inquiry, and thematic analysis, largely shaped our understanding of co-design. We reflect on the methodological advantages of co-design, as well as shortcomings. *Result.* Our methodology engages modellers and system stakeholders through a four-stage co-design process consisting of (1) observation and candidate data availability, (2) candidate model design, (3) interpretation of model consequences, and (4) interpretation of domain consequences. *Conclusion.* We have proposed a new methodology by integrating the concept of co-design into the classical modelling cycle and providing a rigorous methodology for the construction of models that captures the system and its behaviours accurately. We have also demonstrated what an attempt at co-design looks like in the real-world, and reflected upon necessary improvements.

Keywords: Security co-design · Security modelling · Security culture.

1 Introduction

Security managers are responsible for meeting the organization's security objectives. Most commonly, managers set a security policy as a way of clearly outlining these objectives and providing further guidance on how to follow them. While the security manager's primary concern is to keep the organization secure and ensure policy compliance, challenges arise from complex factors that may impede the effectiveness of the security policy. Factors obstructing compliance with security policy may include how the policy itself is written, the level of difficulty

associated with compliance, the organization's security culture (or lack thereof), or irrelevant threats represented in the policy. Unfortunately, these factors are often unknown at the time of policy design and security managers face the challenge of setting and championing a security policy that may have undesirable consequences for the organization. The inability to predict such consequences may create uncertainty and risk for the security manager. Modelling provides the opportunity to explore the consequences of a particular decision. Models can help system owners (in this case security managers) manage the complexity of their system by creating appropriate simplifications of the system and its components. In increasingly complex and dynamic environments, it is important to identify ways of exploring potential consequences of decisions before making decisions. Modelling, a 'tool for thinking', is a way of managing uncertainty and risk associated with decisions. By using a range of concepts from security (behavioural) economics as well as mathematical systems modelling, models can be built to make predictions about policy choices and aid security managers in future security decisions.

However, rigorous and useful modelling presents many challenges. Typically, on the one hand, the system's managers wish for it to be modelled in order to answer questions about its design or behaviour. They may be experts in the system's design, its behaviour, or its domain of application, but may have little or no knowledge of the languages, methodologies, or data-capture requirements of modelling. On the other hand, modellers, experts in the languages and methodologies of modelling, may have little understanding of many aspects of the behaviour of the system, the context within which the domain experts' questions are asked, and little knowledge of what data may be available to be collected.

It is, therefore, necessary that in order to construct models that capture the system and its behaviours accurately, capture the system's managers' questions adequately, and do so in such way that the required supporting data can be collected, it is necessary that the system's managers and the modellers cooperate in the construction of the model.

Our thesis is that this requirement can be addressed rigorously by introducing the concept of co-design into the classical modelling methodology, as depicted in Figure 3. We summarize here the necessary modifications, which are explored in detail in Section 4.

- We introduce — see Figure 2 in Section 4 — a translation zone in place of the simple 'induction' of models step.
- This translation zone is the space in which the stakeholders — system owners and users and modellers — interact in order to co-design an adequate model.
- The translation zone supports the development of shared understanding of the system, the questions about the system, the modelling methodology and its limitations, and the availability of relevant data.

Security provides a systems perspective that is both quite generic and for which co-design is particularly important. Although there is evidence to suggest that security culture drives policy compliance [8], cultural and behavioural aspects of security are not commonly considered when modelling security policy. The importance of culture in security has been highlighted long ago [20];

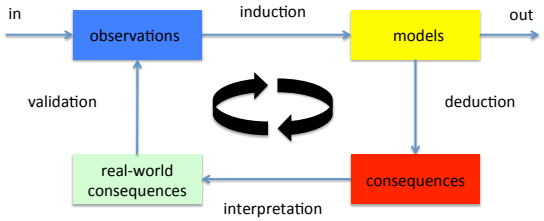

Fig. 1. The classical mathematical modelling cycle. (see, e.g., [21])

however, its representation is often oversimplified [24], or too complex to model usefully.

Modelling security culture through a co-design approach can help facilitate the required system and context knowledge to represent culture more accurately. Opportunities to capture observations of the cultural and behavioural aspects influencing security policy can be identified by engaging stakeholders from an early stage. Constructs from traditional and behavioural economics can then be used to characterize those observations in ways that are better suited for modelling by considering theories such as bounded rationality and herd behaviour [6].

1.1 Contributions and structure

Contributions:

- We identify challenges with modelling in general, and those of modelling behavioural and cultural aspects of security in particular.
- We introduce co-design into the classical modelling cycle and develop a methodology for security modelling that addresses the identified challenges. Our process of co-design facilitates collaboration and mutual learning between modellers and stakeholders towards achieving a mutually beneficial goal.
- We demonstrate how components of co-design translate into the real world by unpicking a case-study at Company A and reflecting on the advantages and disadvantages of the used methods as well as identifying opportunities for improvement.

Structure:

- In **Section 2**, we introduce the rôle of modelling in understanding and supporting policy-formulation and decision-making in security. We consider the challenges that can be observed in coordinating the identification and collection of relevant data and the design and construction of models.
- We explain the impact of culture and behaviour on security policy compliance in **Section 3**, and summarize why behavioural and cultural aspects should be captured when modelling security. We then observe the challenges that may arise when attempting to characterize culture less vaguely and model it in a way that is useful in practice.

- Before introducing our new methodology in **Section 4**, we first provide an overview of co-design and discuss existing co-design work in modelling and security. We introduce our approach in the form of a co-design methodology that is a modification of the classical modelling cycle.
- In **Section 5**, we present a case-study which largely shaped our understanding of co-design [10]. Through reflections, we discuss the methods and approaches that worked, as well as shortcomings. Finally, we summarize the contents of this paper in **Section 6**.

2 Modelling for security

Models play an important role in the way we understand, analyze, and make decisions about security. We can identify many types of models that arise in this setting. Here are a few key examples.

- Access control models: these are typically formulated using algebraic or logical methods. For example, Bell-LaPadula, Biba, and the many models they have inspired, use algebraic methods. An alternative approach is to use logical methods to specify access control rules. This too has been developed quite substantially in a large literature;
- Models of attack–defence strategies: these are typically game-theoretic, in which the game's players represent attackers and defenders with varying assumptions about the knowledge of the players and their levels of investment;
- Policy models: these illustrate the consequences of policy choices on, for example, trade-offs between performance and security attributes. Often these are simulation models, such as impulse–response models, which explore the response of a systems to attacks under varying policy régimes;
- Behavioural economics models: these illustrate behavioural choices within organizations. For example, the Compliance Budget [4], which can also be analysed logically [1], examines the trade-off between the commitment of individuals' (limited) resources to organizational operational objectives and those committed to compliance with organizational security policies;
- Penetration models: these may use, for example, stochastic processes to capture an attackers expected degree of of penetration a system with a given defensive posture.

In all these examples, albeit to differing extents, constructing the models adequately requires their co-design by the system's owners, users, and modellers.

2.1 Challenges of modelling

There are many problems that can arise when constructing models, and many of them have been described and explained in the work of Michael Pidd — see, for example, [22] and the many articles in [23]. For a more mathematical perspective, see [7] and for a 'systems thinking' perspective on engineering, see [18].

Challenges can arise during the initial phases of modelling, when the purpose and specification of the model is decided, during the construction of the model, and also during the eventual use of the model.

Before a model can be built, it is necessary to understand what its purpose is and what it should do. Beginning model construction or data collection before the purpose of a model has been identified can lead to a number of problems:

- Collecting data before determining the modelling approach to be used. The required data can vary significantly depending on the chosen modelling approach. By collecting the data in a silo, the data that has been collected may not be adequate for the modelling method in mind;
- Conducting large-scale data collection prior to determining the purpose of the model. When this occurs, the problem identification is driven and restricted by the data that has been already collected. Important contextual knowledge may be missing in the data-set because of the data collection happening prior to any careful objective identification;
- Neglecting communication with stakeholders (e.g., the system owner) at an early stage can lead to an incomplete identification of the problem to be modelled. The system owner is likely to hold critical information about the system and its issues, and can help with identifying modelling objectives.

Prior to model construction, it is essential to identify the data that are required and the limitations to what can be collected. Failure to do so can lead to the following problems:

- Deciding to model a system without considering the expert knowledge of the system stakeholders. Stakeholders might hold critical knowledge about whether constructing such a model is even a possibility given the limitations of data availability;
- Some models may require the understanding of processes for which data cannot be collected. The system stakeholders may have the required understanding of the processes even if data collection about those processes is not possible. This further emphasizes the importance of stakeholder involvement;
- The necessary data collection may be too expensive to conduct or require a long time to set up. This may mean that the data becomes unusable or irrelevant by the time it has been collected.

There are problems that can impact the eventual use of the model:

- Lack of stakeholder involvement may lead to a disconnect between the identified model objectives and the real world issues present in the system. If the the model objectives are not aligned with the real world problems, the model might end up being useless for the system stakeholders;
- When doing modelling as part of interdisciplinary work, there is a risk that domain experts will work in a disjoint manner. If the objectives of the expert collecting the data and the modeller are not aligned, the end result of the model might not be useful for either.

Finally, a few generic issues are always present: ‘the map is not the territory’ [16]; the level of detail/complexity of the model must be appropriate to address the problem — Einstein’s principle; the model should be available when needed — a less good model that is available when needed may be more useful than

a better model that is not; and cost-effectiveness — cost of creating the model should be justified by the benefits of having the model.

Looking carefully at these problems it is possible to see that they are in some sense circular: the data that needs to be collected depends on the purpose of the model and the modelling approach selected, but these choices are in turn constrained by the availability of data and affected by the modeller's understanding of the system. The challenge is to develop an approach to modelling that resolves this circular dependency; we propose to do this by involving modellers and stakeholders in an iterative process of co-design that creates a shared understanding of the system to be modelled, identifies the purpose of the model, and ensures that the specified model is aligned with the needs of the stakeholders and fits within the limitations created by data availability.

3 Modelling behavioural and cultural aspects of security

Compliance with security policy is largely affected by employee behaviour and the elements that influence these behaviours [4]. The behaviour and decision-making of people are already complex and can be further complicated by social, cultural, or other influencing factors in the organization.

Insights from behavioural economics can aid the understanding of people's decision-making and interaction with the system, which subsequently help better modelling of such behaviour [6]. Simplified abstractions of complex phenomena such as security culture may particularly benefit security managers and other system owners tasked with the management of security behaviours in ever-changing ecosystems. Modelling certain dimensions of security culture, or groups interacting within that culture, may help characterize security culture in a more meaningful and practical way for system stakeholders.

3.1 Challenges of modelling behavioural and cultural aspects

The complexity of security culture creates certain challenges when trying to model it. The following are some examples of such challenges:

- The concept of culture is complex and difficult to articulate in a tangible manner [11]. Although culture has been studied for a very long time and is a widely used concept, its meaning is often portrayed in an intangible way. When modelling culture, there is a need to focus on tangible components of culture, which can be used to establish cultural and behavioural parameters [11];
- There is no accepted and practical definition of security culture [19]. Originating from organizational culture, the concept of security culture has received a lot of attention in security research and the literature has been expanding rapidly. However, work on security culture rarely provides a more in-depth explanation about how the adapted model of organizational culture translates to the context of security [24]. This further complicates modelling cultural aspects of security;
- Culture is a dynamic phenomenon, often impacted by unexpected change or turbulence [25]. Culture may have stable components, but it is dynamic

in nature and continuously changing. While it may be a more difficult and lengthier process, the stable components of culture may change as well under unexpected and extreme circumstances [25]. When modelling culture, it may be difficult to anticipate such extreme circumstances, which could significantly impact the cultural parameters in the model;
- Representing culture in a model could introduce a two-fold risk. The first would be ending up with a reductionist view — taking an approach that is too simplistic in representing the influence of culture on behaviour. This would produce yet another insufficiently detailed representation of security culture. The second would be that of over-elaboration — creating an overly complex representation of culture, perhaps rendering the model unusable in a real-world context [11].

The complex nature of culture in general — and that of security culture in particular — is what makes the opportunity to model culture appealing. The ability to represent culture more practically — in a model — has the potential of becoming a useful tool for system owners challenged with the task of managing security behaviours in a complex and dynamic ecosystem. A possible representation of culture could be in the form of cultural and behavioural parameters derived from moving components of culture, or by categorizing system stakeholders into distinct behaviour groups.

While the benefits to modelling culture in a practical manner may be obvious, there are inhibitors — similar to the modelling challenges above — that may limit the ability to do so. In order to represent cultural components or behaviour groups adequately and accurately, there is a necessity for real-life observations of that very culture. In addition to the observations of culture, there is a requirement for an in-depth understanding of the ecosystem. The availability of such knowledge is often limited, whereas the collectability of such data is sometimes not a possibility for various reasons.

System owners and other stakeholders hold critical knowledge about the ecosystem and the moving components of that system. The experience, knowledge, and information of the stakeholders about the system as well as culture to be modelled complement the expertise of the modeller. By involving stakeholders from the stage of problem identification, and receiving their willingness to participate, much more accurate representations of culture and system components can be created for the model. The complexity of a system — and culture — can be captured more correctly through a process of mutual learning between the system stakeholders and the modeller.

4 Co-design for security modelling

4.1 What is co-design?

Co-design is normally associated with user-centred design and participatory design [9]. As it is largely influenced by the latter, co-design is often considered to be an updated term for participatory design [9]. The core principle of co-design is that it encourages *collaboration* between all stakeholders in the design process. A useful definition that thoroughly captures the process of co-design is that by Kleinsmann and Valkenburg [15, p.2–3]:

> 'Co-design is the process in which actors from different disciplines share their knowledge about both the design process and the design content. They do that in order to create shared understanding on both aspects, to be able to integrate and explore their knowledge and to achieve the larger common objective: the new product to be designed.'

Benefits such as improved creativity and idea generation as well as better knowledge and cooperation between stakeholders have been associated with co-design [28]. Steen [27], argues that co-design can be viewed as a process of *abduction*. Dorst [12] provides a similar perspective by arguing that abduction is fundamental to design thinking. When using abduction as a technique in co-design, problems and potential solutions are explored in an iterative process whereby *problem and solution co-evolve* [27, p.18].

4.2 Co-design and modelling

The closest representation of co-design in modelling work can be found in *participatory modelling* (PM) which can be defined as 'a purposeful learning process for action that engages the implicit and explicit knowledge of stakeholders to create formalized and shared representations of reality' [30, p.1]. PM emerged as a result of the realization that stakeholders can contribute useful knowledge, experience, and skills — and that stakeholders are more likely to comply with policies if they are engaged in the process of developing those policies [31].

Participatory modelling is sometimes referred to as collaborative modelling or co-modelling, terms which are often used interchangeably as there are no clear distinctions between them [2]. Basco-Carrera et al. [2] attempt such a distinction and associate collaborative modelling more strongly with co-design as it is better suited for contexts with high cooperation. PM, on the other hand, involves a lower level of cooperation.

Methods such as participatory and collaborative modelling have come into use because of an increased emphasis on stakeholder involvement in fields such as water resources management. In fact, the majority of PM work has been done in areas such as environment and planning, water resources management, and resource and environmental modelling [17, 2, 31, 30].

An ideal approach to PM would be to involve stakeholders in most (if not all) stages of modelling [31]. However, this is not always the case, and there are different 'ladders' of stakeholder participation which distinguish between different levels of involvement [2]. In contrast to PM, co-design focusses more strongly on high participation, which suits our methodological approach.

4.3 Co-design and security

To the best of our knowledge, there is a scarcity of works in security research that focus on participatory modelling or co-design. Ionita et al. [14] implement participatory modelling principles to evaluate whether such a collaborative approach would improve the quality of the final models. They tested their approach in the context of risk assessment and got favourable results from the participatory modelling. Beautement et al. [3] demonstrate the importance of capturing

data that represents a real-world environment. To achieve this, they propose a methodology consisting of passive and active data collection cycles — meant to collect accurate data about security behaviours and attitudes in organizations [3]. Heath, Hall, and Coles-Kemp [13] focus on the security design of a home banking system by intersecting aspects of co-design and participatory physical modelling. More specifically, participants interact with different security scenarios by using LEGO kits and achieve positive insights by doing so.

While the above examples demonstrate co-design thinking [3] — and attempts to create an interaction between co-design and modelling [13] — no comprehensive methodology has been proposed for co-designing security modelling, at least not one that reflects *our* understanding of co-design. Our approach focusses on a deeper involvement of stakeholders, by ensuring mutual objectives from early on, and continued participation — but also co-creation — throughout the entire co-design process.

4.4 Our new methodology

In order to build a model, the modeller has three requirements: an understanding of the modelling objectives, an understanding of the system to be modelled, and the knowledge or data about the system required to construct the model. In order for a model to be useful for a system manager (the model user or 'customer'), the modelling objective must be aligned with the manager's desired analysis. The modeller and the manager must have a shared understanding of the model objectives. The model must also fit within the limitations of what information the modeller can learn and collect about the system. A well-specified model with a shared understanding between modeller and manager is useless if the modeller has no access to the information required to build it.

These limitations on data collection come in two forms. First, there is information that is impossible to collect; this is a hard limit — perhaps because of time, monetary, or physical limitations that cannot be overcome. Second, there are limitations imposed by the willingness of system stakeholders to participate in the modelling process. In large socio-technical ecosystems, as frequently found in the security domain, there are many sources of data and many stakeholders, without whose cooperation it can be challenging to gain access to their knowledge of the systems of which they are a part.

We propose a process of model co-design that aims to facilitate the construction of models that meet these criteria. We start by giving a definition:

> 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.

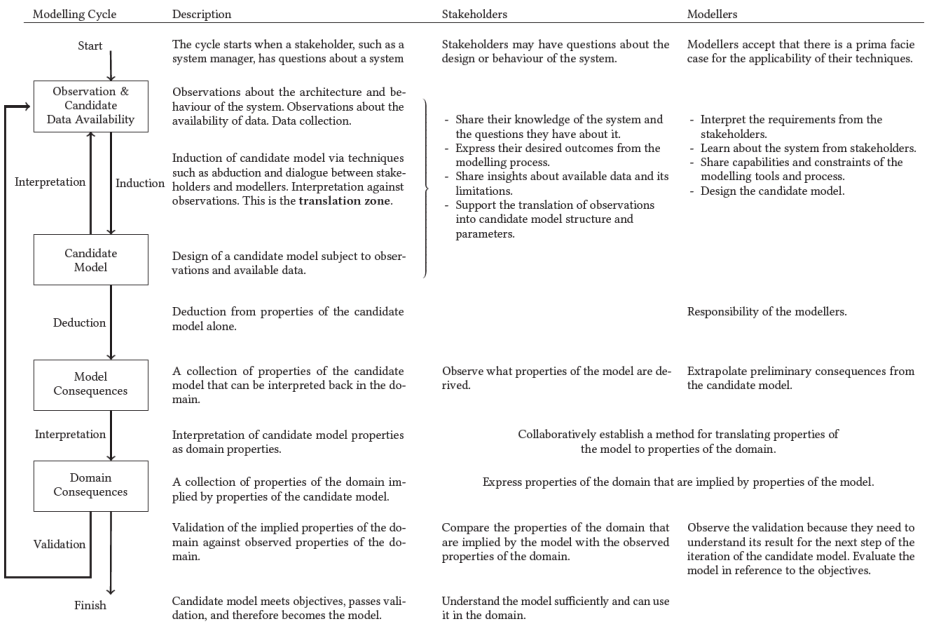

Fig. 2. Modelling cycle, translation zone, and co-design.

We can express this process as a modification of the classic modelling cycle, which is shown in Figure 3. The classic modelling cycle starts at the point of observation — it assumes the objectives of the model are already specified — and moves in a cycle. Observations of the system are made and a candidate model is constructed; the consequences of the model are interpreted as real-world (or domain) consequences and then validated against observations of the real system. If the model does not match the real system, the candidate model is refined and the process repeats. When the modeller is satisfied that the model performs appropriately the cycle is finished. The perspective of this classic cycle is very modelling- and modeller-centric.

In our conception of co-design, modellers and stakeholders work together to determine the objectives of the model, which are refined based on observations of the system, the data required to produce a model, and the limits of data availability. Figure 2 presents our *co-design cycle*.

The co-design cycle starts when a stakeholder, such as a system manager, wants to understand something about the system. This may, for example, be due to a desire to understand an aspect of observed system behaviour, or a question about policy choices or system management. The stakeholder then begins to work with a modeller, if the modeller believes their techniques are applicable. The modeller can be a person or team, and possibly be unfamiliar with the system of interest.

Next come the main elements of the co-design cycle: observation of the system and candidate data availability, which leads to the construction of a candidate

model. In a change to the classic modelling cycle, we create a sub-loop between these two stages, and it is this sub-loop that forms the *translation zone* in the modelling co-design process. Here, system stakeholders work with modellers to

1. make observations about the architecture and behaviour of the system,
2. make observations about the availability of data,
3. perform data collection,
4. refine the goals of the model based on these observations, data, and data availability,
5. design (or induce) a candidate model, and
6. interpret the candidate model against observations — returning to (1).

We define this as the translation zone because of the interactions and cooperation of the modellers and stakeholders during this sub-loop. The stakeholders share their knowledge of the system with the modeller; the modellers learn about the system from the stakeholders. Modellers express their requirements for information and data; the stakeholders share their insights about data availability and limitations. The stakeholders share the questions they have about the system and express their desired outcomes from the modelling process; the modellers interpret these requirements as a specification. The modellers share the capabilities and constraints of the modelling tools and process; the stakeholders refine their requirements based on this understanding of what can be modelled. The modellers design the candidate model; the stakeholders support the translation of observations into model structure and parameters.

The candidate model is then interpreted by stakeholders and modellers against observations, and the cycle repeats. This is an iterative dialogue between stakeholders and modellers that seeks to converge on a shared understanding of the system, of the data available, and of the objectives and capabilities of the model.

The rest of the co-design cycle closely follows the classic modelling cycle, but we define the rôles that stakeholders and modellers play during these parts of the process, as shown in Figure 2. The modellers deduce the model-consequences from the candidate model, while the stakeholders observe this step to learn more about the operation of the model. These are consequences *in terms of the model*, not in terms of the system itself, so they must be interpreted. The modellers and the stakeholders collaboratively establish a method for translating properties of the model to properties of the domain; the result are the domain properties that are implied by the properties of the model.

Next comes validation. Here, the stakeholders must compare these model-implied domain properties to the observed properties of the model. The modellers observe this because understanding validation failures — where model-implied properties and observed properties do not match — is important for the construction of a new candidate model in the next iteration. If validation is successful, the candidate model is accepted and the cycle is complete.

What the co-design cycle achieves. We described above a number of challenges that often arise during modelling. This co-design approach has the potential to help modellers and stakeholders to overcome some of these challenges. Many of the challenges arise because of of uncertainty on the part of the modeller: about which data should be collected, what data is available, and even what problem

should be modelled. Other challenges arise because of the stakeholders' lack of involvement: stakeholders may ask an initial question, but it might not be the right question to arrive at answers that will be useful to them, or they may have necessary insights into the system that get ignored because they are never asked. For security problems, organizational culture is often a very important factor (for example, in the way policy decisions will play out); without the engagement of stakeholders, it may be impossible to capture the culture sufficiently well enough to make a good model.

A co-design modelling process will bring both modellers and stakeholders together in a cooperative process to produce a model that deepens the understanding of all stakeholders involved; it helps understand the system and helps make better decisions about it. Part of the value of building models of things is that it enforces a careful consideration of the thing itself — it actually forces one to think about what it is, in ways that are perhaps more rigorously characterized than they would be otherwise. This careful consideration also applies to the formulation of questions about the system of interest: it will encourage a more rigorous, more precise, more reflected formulation of questions. Co-creating the questions (or problem) is just as important as co-creating the model. Better questions allow for a better understanding of what a model needs to do, and what data is needed for it.

Co-design also makes it more likely that more data will be available to the modellers: stakeholders may have a great deal of knowledge about the system, and in the case of modelling culture, the stakeholders' behaviour *is* the data that is needed. A process that creates an understanding of why data is needed, through a shared understanding of the model and its purpose, can help gain access to the stakeholders who have this information, as we show below.

5 Case study: Reflections

To demonstrate how an attempt to co-design looks like in a real-world context, as well as reflect on potential improvements, we present an in-depth case-study of a single company, previously published in [10].

5.1 The organization

Here we provide a brief profile of Company A, focussing on the historical security context of the organization as well as their current security structure, policies, and processes. A more detailed description of the company can be found in [10].

Profile: The company — hereafter referred to as *Company A* — is a medium-large sized company operating within the finance and technology sector. Company A is based in the United Kingdom and specializes in financial forecasting. The company has grown significantly over the last few years — the start-up mentality it had in the beginning has slowly shifted to a more corporate one. Starting at around two hundred employees about two decades ago, it now has close to a thousand employees.

So far, Company A has been incredibly successful in the work that it does. In order to protect the work that it produces, the company also places great value

on its information assets by investing heavily on security measures. They have developed their security expertise throughout the years — so much so that — it is mistaken for a security company rather than a finance and technology one.

Security context: Company A's security measures were almost non-existent in the beginning. The company had a much more informal attitude towards security and only basic controls. Then, Company A suffered an information security breach in the form of an insider attack [10]. This breach seriously threatened the company's financial and reputational stability and could have potentially ended the business. Fortunately they were able to predominantly contain the breach and the damage. However, this particular experience emphasized the necessity for a better security strategy and more mature processes.

Fast forwarding some years after the incident — Company A resembles almost a completely different organization. It has a post-shock organizational security structure. This means that the security structure was created as a result of a *shock*, that being the breach in this particular case. To ensure that a similar breach does not occur again, Company A invested significantly in security technology and staff. The security increase is also noticeable when entering the premises of the organization as there are multiple CCTV cameras and physical barriers to control movement in different areas.

Structure, policies, and processes: The security division comprises around ten percent of Company A. The increase in size changes the security communication and impacts the processes and policies. After the incident, several security policies were created — some of them are redundant, some are jargon-heavy, some contradict others, and most are located inconsistently. Security rules are also outlined in the Staff Handbook, to which all newcomers and existing employees are contractually bound.

According to the policies, non-compliance with security leads to disciplinary action, but Company A has no formal and systematized way of tracking non-compliance — some incidents may go unnoticed, while others receive unexpected disciplinary action. An inconsistent approach to disciplining non-compliance may negatively impact the legitimacy of the policies and, in turn, lead to increased workarounds. In addition, having a set of scattered policies rather than a single central policy can further complicate employees' ability to comply with security. Given these observations, there has been an initiative at Company A to centralize the security policy in order to achieve consistency.

5.2 Methodology

The engagement with the organization started when the Chief Information Security Officer (CISO) of Company A had made certain observations about the security division and had questions about the impact of security on the company's business processes. The CISO and one of the authors had been discussing the questions about Company A's security function. As a result of mutual interest in the topic — as well as the author's capabilities to capture the factors they had discussed — they decided to research the questions by constructing a conceptual model of Company A's security processes, policies, and behaviours, focussing on the following objectives: (1) to explore and evaluate the daily security processes in the company, (2) to identify potential friction, (3) to explore

the meaning and role of security culture in general and within the organization, and (4) to identify potential improvements.

The research for this case-study was led by one of our researchers, embedded in Company A for a period of 6 months. By working at the security division, the researcher was able to immerse in the role of a security employee and simultaneously conduct research. The methods used were guided by our engagement with Company A and the context of the organization [10]. While the case-study was conducted during the early stages of our understanding and development of co-design, we recognized the importance of focussing on the engagement and participation of stakeholders and adopted existing methods to achieve this.

The study: The case-study at Company A consists of long-term diary entries and semi-structured interviews with security staff. We used the following methods during the research: *participatory action research* (PAR) [29], *humble inquiry* [26], and *thematic analysis* (TA) [5]. The diary entries served primarily as a process of familiarization with Company A and its processes, and as a way to contextualize the findings. Semi-structured interviews with fifteen security managers at Company A were conducted focussing on the objectives that were agreed on with the CISO. The interview questions were guided by regular discussions with the CISO as well as the researcher's independent observations.

Participatory action research, humble inquiry, thematic analysis: Participatory action research is an approach to action research that focusses predominantly on the action and participation of stakeholders impacted by the research [29]. In exploring issues and questions that are significant to stakeholders, PAR emphasizes their role as co-researchers in the process of inquiry and research. PAR encourages the understanding of factors such as: what people do, how they interact with the world and others, what they value, and the discourses through which people understand and interpret their world [29]. These factors are much akin to those required to understand the culture of an organization.

At Company A, the researcher had the opportunity to observe the employees on a daily basis — absorbing a detailed account of their actions, values, and interaction with the world. The PAR factors above — in line with the model objectives — were additionally explored during the interviews with the security managers. Other principles of participatory action research further guided the case-study at Company A — PAR is a process that is *social, participatory, practical and collaborative, emancipatory, critical, reflexive,* and *transformative.* An account of applying these principles in practice can be found in [10].

As we developed our understanding of co-design, the researcher used Schein's method method of *humble inquiry* [26], which encourages effective communication and positive relationships with participants, to conduct interviews. It treats participants as *co-researchers* rather than as interviewees. Interviews conducted in this way are meant to benefit both parties by having a conversation based on curiosity and honesty.

We used *thematic analysis* — a widely used method for analysing qualitative data — to analyse the interviews with the security managers. The purpose of TA is to identify patterns in the data by creating codes that are later on grouped into relevant themes. The method consists of several steps such as data familiarization, the generation of the initial codes, the search and revision of themes, up to the naming of the final themes [5]. The field researcher had detailed knowledge

of the data and thus conducted the primary coding, which was then reviewed by one of the other researchers [10]. We agreed on the final themes jointly.

5.3 Main findings

We produced eight themes from the thematic analysis of the interviews. The themes relate to Company A's overall approach to security and the employees' perceptions and attitudes towards security. The main findings from [10] are briefly summarized in Table 1.

Table 1. Themes from thematic analysis.

Theme and Description
Post-shock security The impact of the information security breach is reflected in the security structure and practices of Company A.
Security theatre undermines policy The heavy implementation of visible security controls for the sake of *appearing* secure undermines the legitimacy of the security policies at the company.
Security is like detention Non-security staff are treated as *enemies* when not complying with security, which leads to a blame culture in the company.
Security is a blocker The productivity of non-security staff often suffers because of restrictions imposed by security controls.
Lack of effective communication The justification behind implementing such strict security controls is not adequately communicated across the organization.
Zero-risk appetite The tolerance for taking security risks is almost non-existent in Company A, which often compromises productivity.
Sensible security is likely to work The security division believes that less strict but better suited security controls are likely to increase compliance with security policies.
Behaviour change is required Unlearning of old behaviours and behaviour change is required in order to create better security habits over time.

5.4 Reflections

We designed and conducted the Company A case-study while we were at the beginning of developing a co-design methodology for security modelling. The study was preliminary, aimed at developing a conceptual model, and meant to be followed up by larger-scale research, which might have involved more mathematical types of modelling. Unfortunately, because of organizational restructuring, the co-design with Company A ended earlier than expected.

Important lessons, which significantly shaped our understanding of co-design, emerged from conducting this case-study. The individual methods that we implemented, such as participatory action research and humble inquiry, helped us learn which aspects of co-design would work and which should be improved. The work we did with Company A provided an interesting perspective and valuable reflections, which significantly influenced the co-design work presented here.

We summarize our reflections below.

Co-creating objectives: The research objectives for the Company A case-study were jointly created between us and the CISO. We wanted to ensure that the questions the CISO wanted to explore were aligned with our research goals and vice-versa. These aligned objectives were stated early on in the field researcher's job description and the methods were then adapted based on the context and other organizational factors. For example, one factor that impacted the method of the research was the availability of the security managers. Compromises were made jointly to ensure that the objectives were followed and that the research was beneficial for all actively involved stakeholders. We encountered a limitation in our attempt to co-create the objectives. Although there was initial buy-in for the research from the senior executives, we did not agree on the long-term objectives with them as we did with the CISO. This led to misalignment of goals later on and influenced the continuation of the co-design.

Involvement in research: The collaboration with the CISO and other relevant stakeholders was present throughout the research. Continuous discussions with the CISO helped shape the design of the interviews and encouraged the managers' willingness to participate. The interview study was approved as well as championed by the CISO of Company A. This simplified the arrangement of the interviews with the participants and set a positive tone for the conversations during the interviews. Furthermore, the involvement of the security managers in the research carried on as they were keen to contribute to the research and be informed of the outcomes.

Building relationships: In addition to the CISO's involvement and support, something else that positively impacted the experience was the researcher's opportunity to build relationships with the employees of Company A, including the security managers. The ability to work alongside the participants for months before interviewing them meant that the researcher could build a relationship based on trust and mutual goals. Building such relationships also influenced the authenticity of the researcher's cultural and behavioural observations and the possibility to make such observations in the first place.

Mutual learning: When embedded in the company, the researcher worked on several projects and tasks that were not directly related to the research. This was an opportunity to work together with many employees from the security division as well as other departments. During these collaborations, there were many instances of mutual learning. The security division were able to learn about

the behavioural and cultural aspects of security from the researcher, while the researcher learned a lot about how the security systems and processes worked in practice. This process of mutual learning created a space for symmetric relationships functioning through translation zones between both technical and human-centred security — as well as between security research and application. A shortcoming of the mutual learning process was the lack of formalization during the initial phases of learning while the researcher was getting familiar with the systems and processes. More structuring and documentation of the knowledge exchange between the system owners and the researcher would have benefited the construction of the conceptual model.

Mapping case-study reflections to our co-design process: Our co-design methodology was directly informed by the methodological principles and reflections at Company A. Below we map the components from the case-study to the corresponding components in our methodology.

1. The process of *co-creating the objectives* with the CISO of Company A, as well as the inability to co-create the objectives with the rest of the senior executives, emphasizes the importance of clarifying the mutual objectives from the very beginning. This maps to the first stage in the modelling cycle — *Observation and Candidate Data Availability*. Here the observations or questions about the system originating from stakeholders, are communicated to modellers to explore collaboration opportunities. If there is alignment between the questions the stakeholder wants to ask and the modelling techniques the modeller aims to apply, they co-create the objectives towards a mutually beneficial aim.
2. In between the first and second stage of the modelling cycle, lies the *translation zone* between the stakeholders and the modellers. This space of the co-design methodology corresponds to the multiple levels of *mutual learning* at Company A. In the translation zone, stakeholders and modellers exchange knowledge and experiences.
3. The reflections on *involvement in research* and *building relationships* highlight the significance of involving stakeholders in the research end-to-end. An extended interaction creates opportunities to build relationships and trust, as was the case with the researcher and the employees of Company A. Strong relationships create better collaboration opportunities while the involvement of stakeholders throughout the entire process improves the feasibility and quality of the research. As such, these two components correspond to *all the stages in the co-design process.*

Summary: Even though some of our reflections suggest that there is space for improvement, the experience at Company A has been largely positive. It gave us the opportunity to trial a set of methods, the principles of which closely relate to our understanding of co-design, that further emphasize the necessity for stakeholder involvement. The engagement of stakeholders at Company A was worthwhile as it enabled observations and data collection from a wide range of people and significantly aided our understanding of the system. As a result of this early co-design process, we were successfully able to draw mutual conclusions — from the observations and conceptual modelling — summarized in Section 5.3.

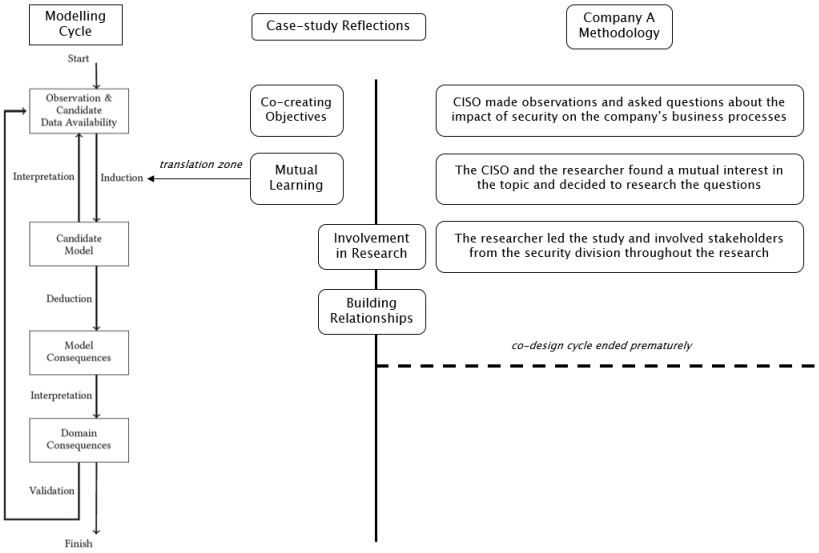

Fig. 3. The mapping of the case-study components to the co-design modelling cycle.

The biggest shortcoming was the inability to continue the co-design process, which stopped at the stage of designing a conceptual *candidate model*. The later stages of the co-design process, such as developing a more accurate model as well as validating it are missing from the current case-study. Another study must be repeated in the future in order to apply all the stages of our co-design process.

6 Conclusion

In this paper, we have proposed a new methodology by integrating the concept of co-design into the classical modelling cycle and providing a rigorous methodology for the construction of models that capture the system and its behaviours accurately. Our definition of co-design focusses on the ongoing *engagement between modellers and stakeholders* in the process of *objective identification and model specification, design, and construction* with the goal of achieving *alignment* between the model objectives and the needs of the stakeholders, and designing *a feasible model* given the constraints of data availability, which are explored as part of the co-design process.

We have presented an in-depth case-study of Company A, marking the beginning of our understanding and development of co-design. We reflect on the methods used in the case-study that shaped our co-design methodology by extracting positive experiences and shortcomings from approaches such as *co-creating objectives*, *involvement in research*, *building relationships*, and *mutual learning*.

Our co-design approach aims to tackle the challenges of problem definition, data availability, and data collection associated with modelling behavioural and cultural aspects of security. It does so by capturing the system's managers' questions adequately, in such a way that the required supporting data can be collected, and the managers and modellers can cooperate in the construction of the model. Co-designing a security model in such a way focusses on more accurate and practical representation of behavioural and cultural aspects of security, which can help security managers with their policy decisions.

In future work, we intend to further validate our co-design methodology by going through all the stages of the cycle with system stakeholders in an organization.

References

1. Anderson, G., McCusker, G., Pym, D.: A logic for the compliance budget. *Proc. GameSec 2016*. LNCS **9966**, 370–381 (2016), proc. GameSec 2016
2. Basco-Carrera, L., Warren, A., van Beek, E., Jonoski, A., Giardino, A.: Collaborative modelling or participatory modelling? a framework for water resources management. Environmental Modelling & Software **91**, 95–110 (2017)
3. Beautement, A., Becker, I., Parkin, S., Krol, K., Sasse, A.: Productive security: A scalable methodology for analysing employee security behaviours. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). pp. 253–270. USENIX Association, Denver, CO (Jun 2016), https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement
4. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 New Security Paradigms Workshop. pp. 47–58 (2008)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
6. Caulfield, T., Baddeley, M., Pym, D.: Social learning in systems security modelling. constructions **14**(15), 3
7. Collinson, M., Monahan, B., Pym, D.: A Discipline of Mathematical Systems Modelling. College Publications (2012)
8. D'Arcy, J., Greene, G.: Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security (2014)
9. David, S., Sabiescu, A.G., Cantoni, L.: Co-design with communities. a reflection on the literature. In: Proceedings of the 7th International Development Informatics Association Conference. pp. 152–166. IDIA Pretoria, South Africa (2013)
10. Demjaha, A., Caulfield, T., Sasse, M.A., Pym, D.: 2 fast 2 secure: A case study of post-breach security changes. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 192–201. IEEE (2019)
11. Dignum, V., Dignum, F.: Perspectives on Culture and Agent-based Simulations, vol. 3. Springer (2014)
12. Dorst, K.: The core of 'design thinking'and its application. Design studies **32**(6), 521–532 (2011)
13. Heath, C., Hall, P., Coles-Kemp, L.: Holding on to dissensus: Participatory interactions in security design. Strategic Design Research Journal **11**(2), 65–78 (2018). https://doi.org/10.4013/sdrj.2018.112.03

14. Ionita, D., Wieringa, R., Bullee, J.W., Vasenev, A.: Investigating the usability and utility of tangible modelling of socio-technical architectures. No. TR-CTIT-15-03 in CTIT Technical Report Series, Centre for Telematics and Information Technology (CTIT), Netherlands (May 2015), foreground = 100Type of activity = technical report; Main leader = UT; Type of audience = scientific community; Size of audience = n.a.; Countries addressed = international;
15. Kleinsmann, M., Valkenburg, R.: Barriers and enablers for creating shared understanding in co-design projects. Design studies **29**(4), 369–386 (2008)
16. Korzybski, A.: Science and sanity: An introduction to non-Aristotelian systems and general semantics. Institute of GS (1958)
17. Landström, C., Whatmore, S.J., Lane, S.N., Odoni, N.A., Ward, N., Bradley, S.: Coproducing flood risk knowledge: redistributing expertise in critical 'participatory modelling'. Environment and Planning A **43**(7), 1617–1633 (2011)
18. Lawson, H.B.: A Journey Through the Systems Landscape. College Publications (2010)
19. Malcolmson, J.: What is security culture? does it differ in content from general organisational culture? In: 43rd Annual 2009 international Carnahan conference on security technology. pp. 361–366. IEEE (2009)
20. Martins, A., Elofe, J.: Information security culture. In: Security in the information society, pp. 203–214. Springer (2002)
21. McColl, J.: Probability. Elsevier: Butterworth–Heinemann (1995)
22. Pidd, M.: Tools for thinking—modelling in management science. Journal of the Operational Research Society **48**(11), 1150–1150 (1997)
23. Pidd, M.: Systems modelling: Theory and practice (2004)
24. Reid, R., Van Niekerk, J., Renaud, K.: Information security culture: A general living systems theory perspective. In: 2014 Information Security for South Africa. pp. 1–8. IEEE (2014)
25. Schein, E.H.: Organizational culture and leadership, vol. 2. John Wiley & Sons (2010)
26. Schein, E.H., Schein, P.A.: Humble inquiry: The gentle art of asking instead of telling. Berrett-Koehler Publishers (2021)
27. Steen, M.: Co-design as a process of joint inquiry and imagination. Design Issues **29**(2), 16–28 (2013)
28. Steen, M., Manschot, M., De Koning, N.: Benefits of co-design in service design projects. International Journal of Design **5**(2) (2011)
29. Stephen, K., Robin, M., Denzin, N., Lincoln, Y.: Participatory action research: Communicative action and the public sphere. Norman K; Denzin and Yvonna S. Lincoln (editors), The Sage handbook of qualitative research, United Kingdom: Sage Publications pp. 559–604 (2000)
30. Voinov, A., Jenni, K., Gray, S., Kolagani, N., Glynn, P.D., Bommel, P., Prell, C., Zellner, M., Paolisso, M., Jordan, R., et al.: Tools and methods in participatory modeling: Selecting the right tool for the job. Environmental Modelling & Software **109**, 232–255 (2018)
31. Voinov, A., Kolagani, N., McCall, M.K., Glynn, P.D., Kragt, M.E., Ostermann, F.O., Pierce, S.A., Ramu, P.: Modelling with stakeholders–next generation. Environmental Modelling & Software **77**, 196–220 (2016)