Information security culture as socio-technical negotiation*

Guro Bråten Olsborg*[1]

[1] *Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Teknologivegen 22, 2815 Gjøvik, Norway*

Abstract

I argue that prevailing models of information security culture (ISC) and cybersecurity culture rest on two assumptions, that culture is a property of people and that technology belongs to a separate domain. In this idea paper, I problematise these assumptions and ask how ISC can be understood and studied in a way that centres the everyday information security practices of people in organisations and the technologies they involve. Drawing on organisational culture studies, the socio-technical tradition and science and technology studies as analytical vocabularies, I propose an understanding of ISC as the meanings of security that take shape in everyday sociomaterial practice. Security is then an ongoing negotiation. Two conceptual examples, research-data practice and a move towards Zero Trust, show how this negotiation could be studied empirically. The paper argues that governance, risk management and compliance (GRC) that recognises these negotiations can complement awareness work, and take part in the ongoing, everyday processes through which information security culture changes.

Keywords

Information security culture, cybersecurity culture, socio-technical systems, science and technology studies, sociomateriality, actor-network theory

1. Introduction

In this idea paper, I examine the concept of information security culture (ISC), and the closely related concept of cybersecurity culture (CSC), from a socio-technical perspective. I ask: *How can information security culture be understood and studied in a way that centres the everyday information security practices of people in organisations and the technologies they involve?*

Rather than identifying a gap in existing research, I problematise the assumptions it rests on [1]. Alvesson and Sandberg distinguish such problematisation from gap-spotting, which does not deliberately identify and challenge what existing literature takes for granted [1, p. 252]. Problematisation fits the aim here, since the question is not what ISC research has yet to study, but how it conceives of culture and of the relation between the human and the technical. Their own examples include challenges to the image of organisational culture as a unitary set of shared values, and to a dualist ontology that separates the person from the work [1, p. 255]. I

*The 12th International Conference on Socio-Technical Perspectives in IS (STPIS'26), September 16–17, 2026, L'Aquila, Italy.

* Corresponding author.

guro.b.olsborg@ntnu.no (G. B. Olsborg)

0009-0004-1228-7229 (G. B. Olsborg)

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-4334/paper19.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-19

identify two assumptions of this kind that underlie prevailing models of ISC and CSC, and draw on theories from other traditions to propose alternatives. In Jaakkola's terms, the paper is a theory adaptation, in which theories from other traditions are used to revise a concept within a field [2, pp. 22–23], with information security culture as the domain theory and the theories I draw on from other traditions as method theories [2, p. 20].

The first assumption is that culture is a property of people in organisations that can be isolated and measured primarily through human factors. As an alternative to such a "culture-as-metrics" understanding, I draw on organisational culture studies, in which culture is understood as the shared (to various degrees) and often tacit meanings through which people interpret their experiences and make sense of their work [3, pp. 44–45].

The second assumption is that the human and the technical are separate domains. Drawing on the socio-technical tradition, I take up its commitments to humanising work and to people's participation in shaping the systems they work with [4, pp. 321–322]. Drawing on science and technology studies, I propose using actor-network theory (ANT) as an analytical tool, through which security appears as a negotiation that needs no deliberate negotiator, together with work on care and fragility that understands security as something done and maintained in everyday practice [5, pp. 4–5]. I take the position that the social and the material are entangled in everyday practice [6, p. 1437], and use these traditions as analytical vocabularies within that position.

After examining the two assumptions, I illustrate the proposed perspective through two conceptual examples, research-data practice and a reconfiguration towards Zero Trust. I outline how each example could be studied empirically, starting from the ideas presented in this paper. The implication for practice I propose is that organisations could benefit from working with governance, risk management and compliance (GRC) in a way that recognises the negotiations through which security is worked out in everyday practice. Such work can help people work more securely. It does not promise to change information security culture directly, but becomes part of the everyday processes through which culture changes [3, pp. 40–41]. This could complement, rather than replace, established information security culture work that focuses on people's knowledge, attitudes and awareness.

I explore my conceptual research question from two professional positions. On one hand, I work as a GRC professional within the IT department of the university where I also conduct my doctoral research. This means that I both try to uphold GRC processes on an organisational level and act as an advisor who tries to help end users navigate information security within the context of their work. On the other hand, my educational background and research work are situated within the socio-technical tradition and science and technology studies. Insider research, where members of an organisation investigate their own workplace, provides researchers with valuable access and prior understanding [7, pp. 59, 67–69]. However, it also requires them to navigate dual roles and organisational politics [7, pp. 69–72]. My prior understanding includes practical knowledge of GRC frameworks and the standards that underpin them. These frameworks separate human compliance from technical controls [8, pp. 531, 533], and I see this separation in the instruments I use every day, such as policies addressed to users, controls addressed to systems, and reports and metrics that address each separately. My background in science and technology studies gives me a vocabulary for questioning this separation. The two positions are at times in tension, and in this idea paper I use that tension

analytically. As an involved rather than an outside researcher [9, pp. 321–322], I am also a part of what I study, and I return to the methodological consequences of this in section 3.1.

In section 2, I examine the two assumptions, and I then present the two proposed examples for empirical study in section 3. In section 4 I discuss what the conceptual inquiry and the examples show. In section 5 I address limitations, and in section 6 I conclude.

2. Conceptual inquiry

The introduction outlined two assumptions that underlie prevailing models of ISC and CSC, one concerning what culture is and one concerning how the human and the technical relate. I examine them in turn, beginning with culture. For each assumption, I start from the concept at stake, which is the starting point of a theory adaptation [2, p. 23]. In line with problematisation, this involves a narrow coverage and in-depth reading of key texts rather than a review of all relevant studies [1, p. 256]. I trace how prevailing models construct it, and I use existing reviews of the field to document the assumptions involved [10], [11], [12], [13], [14]. I then explain why I draw on the theories I propose as alternatives, and what role each plays in the argument [2, pp. 19–20].

2.1. Challenge 1: The culture concept

I begin with culture because the way culture is conceptualised shapes what is looked for when it is studied. When culture is approached as a property that can be isolated and measured through human factors, technology is easily black-boxed and taken for granted, treated as context or as an artefact of culture, rather than as part of it. I draw on literature on both ISC and CSC. The two terms are often used interchangeably [13, p. 13], [15, p. 5], although they are not synonymous [15, p. 5], [16, pp. 4036–4037]. Some authors treat cybersecurity culture as the broader notion [13, p. 8], while others treat it as a subset of information security culture [17, p. 2]. Definitions also vary across the literature [17, p. 2]. My argument concerns how both treat the relation between the human and the technical. For consistency, I use information security culture as the primary term, and I cite CSC work where it bears on the same question.

2.1.1. Prevailing understandings of ISC and CSC

Existing reviews of the field show that two understandings of culture are especially prominent in the ISC/CSC literature [10, p. 256], [12, p. 13], [13, pp. 10, 14]. The most widely used is Schein's model of organisational culture. A systematic review of 79 studies from 2000 to 2017 found that the majority used Schein's concepts to conceptualise information security culture [12, pp. 12–13]. Frameworks proposed for developing security culture frequently draw on organisational culture models [10, p. 256], [13, pp. 10, 14], above all the three-level model of artefacts, espoused values, and underlying assumptions [12, p. 17], [18, pp. 345–346]. The second is Hofstede's framework of national culture, which has also shaped several research topics in the field [10, p. 256].

This reflects the first assumption outlined in the introduction, that culture is a property of people that can be isolated and measured. In a distinction Smircich draws, as described by Alvesson and Sveningsson [3, p. 44], Schein's and Hofstede's models treat culture as a variable, something an organisation has rather than something it is. For ISC, this could mean that culture, seen as a variable, can be measured with a Likert-scale survey and improved with a mandatory

training module. Reviews of academic literature on ISC show this pattern. Culture is typically assessed through questionnaires, typically on five-point Likert scales and focused on knowledge of policy [13, p. 11]. Measurement scales treat it either as a single variable, often explaining behaviour, or as a multidimensional construct [14, p. 135]. This is the understanding I have called "culture-as-metrics". In GRC practice, the same logic produces auditable human interventions, such as phishing click rates and training completion, while the more complex relations between people and technology receive less attention. Alvesson and Sveningsson also note that, more generally, the concept of organisational culture is often used to refer to top management's beliefs about it, which may marginalise the meaning-making of other groups [3, pp. 47–48].

These assumptions matter because culture is both expressed in and made through everyday practices, so how we understand security culture shapes how organisations can facilitate more secure practices. When culture is understood primarily as a property of people, "what should be done about the human problem?" becomes the natural question, and training and awareness work becomes the obvious answer. Such work remains valuable, and recent research maps a growing range of engagement formats, from individual and pedagogical to collective and exploratory ones [19]. On its own, however, work aimed at people's attitudes and behaviour addresses the expressions of culture more than the conditions in which it is made. I do not argue that such work should be replaced, but that it can be complemented by more systematic attention to how people do security in their everyday work with technology.

2.1.2. ISC – culture subset, subculture or cultures?

I address information security culture as a concept used in research on organisations, which is the literature I draw on, rather than as a general concept. Within organisations, one important question is whether information security culture is separable from organisational culture. Karlsson et al. [20] suggest it may not be. A theoretical distinction can be drawn, they note, but "making the distinction in practice is very difficult, perhaps even impossible" [20, p. 384], and they therefore adopt the broader concept of organisational culture. Several studies treat security culture as a sub-component of organisational culture, embedded within it [15, pp. 1, 7], and some describe it as a subculture [12, pp. 19–20], [13, pp. 8, 14].

Both framings presuppose a single organisational culture from which a security part can be separated and measured. Even within this literature, the relation between the two is described as complex and dependent on context [15, p. 5]. Organisational culture research offers a different picture. Organisations hold several cultures, and cultural meanings may be contradictory and run across different social groupings [3, p. 47]. In this literature, cultural variety is associated with social groupings, such as departments, generations, genders and occupational groups [3, p. 47].

I read this to mean that security is unlikely to form a culture of its own, except perhaps among those whose work is security. Meanings about security rather take shape across the different cultures of an organisation and may differ between departments and services [3, pp. 47–48]. I therefore treat information security culture as these meanings, not as a separable part of one organisational culture. Information security culture cannot then be studied as a thing apart from the wider cultures of the organisation.

2.1.3. An alternative concept of information security culture(s)

If information security culture cannot be studied apart from the wider cultures of the organisation, the next step is to ask what culture is, since information security culture builds on that concept. I propose a shift in what "culture" means in the context of ISC. In prevailing ISC/CSC models, culture is treated as a possession of a group – a set of values and attitudes carried in members' heads, see e.g. [17, p. 4], [21, p. 197], often layered in the familiar manner where the technical enters as an "artefact," a manifestation read for the values and assumptions it expresses [10, p. 255], [21, p. 197]. Following Alvesson and Sveningsson [3, pp. 44–45], I suggest we should treat culture differently. Culture is neither what an organisation officially espouses, nor behaviour taken at face value, but the layer of meaning that lies behind both. It is the lived, partly tacit understandings from which statements and actions spring. It cannot be assumed to follow what management espouses. The same action may carry different meaning for those who perform it. Culture must be interpreted in this sense, as it cannot be read off the surface. Culture is expressed in behaviour but refers to the meaning that behaviour has for people [3, p. 45]. A formal rule, such as a security policy, may therefore take on different meanings and lead to different behaviour in different cultural contexts. In this view, information security culture would not be a property held in any one group's heads. Rather, culture is relational, because the meaning people make of security takes shape in their ongoing work with each other and with and through the technologies they use and the functions that govern and support that work. Meaning is not formed inside people's heads before and apart from their work with technology. It takes shape in practice [6, pp. 1437–1438], a position I develop further when I turn to the second assumption, that the human and the technical are separate domains.

This way of thinking has a long pragmatist and culturalist lineage. Kaghan and Bowker [22] describe a tradition in which the sensibility of people's conduct is mediated by the cultures, "both symbolic and material" [22, p. 254], they act within. Culture, in this view, already includes the material, rather than being set apart from it. Technology is then not a condition outside meaning-making, but part of what culture is made of. Information security culture in this sense is therefore not one more factor to be added to an account of information security. It is where such an account can begin, since it is in everyday practice that the human and the technical are held together.

Building on Alvesson and Sveningsson's understanding of culture as shared meanings [3, pp. 44–45], I take information security culture to mean the shared (to various degrees) and often tacit meanings through which people in an organisation make sense of information security in their everyday work with technology. These include the meanings people attach to the rules and technologies they work with.

2.2. Challenge 2: The human and the technical as separate domains

I have now proposed an understanding of information security culture as shared meaning that takes shape in practice. I now turn to the second assumption I have set out to problematise [1], that the human and the technical are separate domains. I first show where the technical drops out of research, theory and standards on information security culture. I then turn to the socio-technical tradition for a direction, and to science and technology studies for an analytical lens, and to both for vocabulary.

2.2.1. A culture of information security where technology becomes invisible

The separation between humans and technology runs through research, theory and standards alike. In research, few studies examine how technological aspects of information security affect the human factors of security culture [11, p. 276], and technology aspects have received limited attention in the wider security-culture literature [23, p. 141]. In theory, the dominant understandings of culture leave little room for technology as an intrinsic part of how culture takes shape. Schein reads artefacts for what they reveal about deeper assumptions, and Hofstede locates culture in values. In both, technology is read for what it reveals about culture, rather than as something that takes part in how culture takes shape. In information security standards, people and technology are addressed through separate sets of controls [8], and culture is placed on the side of the people. I meet this separation in the instruments I use in my own GRC work, which build on the same international standards. The separation is, in one sense, productive, because drawing a line between people and technological systems makes a complex situation more manageable. I argue that it also shapes what can be asked. By assigning failure to either "human error" or "technical fault", it tends to leave the relation between them unexamined. This makes intervention on the humans an obvious move, while a response aimed at the relation itself is harder to formulate.

The separation between human and technical factors has long been contested. Usable security research argued early that users are not the enemy [24]. Socio-technical information systems research using a work system perspective [25, p. 35] has documented how security policies fail when they are disconnected from actual work practices [26, pp. 467, 470], [27, pp. 138, 143]. Within ISC and CSC research, one recent contribution brings an explicitly socio-technical perspective. Evripidou et al. [23] review information security culture in organisations that operate industrial control systems. Through the notion of latent design conditions, they highlight how technical arrangements, such as missing fail-safe mechanisms, shape perceptions that are otherwise attributed to individual error [23, pp. 137, 142].

2.2.2. The socio-technical tradition as a direction

As Mumford [4, p. 321] tells its history, socio-technical design grew out of the Tavistock Institute as a value system with two core commitments, namely humanising work and democracy at work. Against the determinism of the assembly line, its guiding objective was the joint optimisation of the social and technical systems. The two were given equal weight, and the human member of any team was seen, in Pasmore's account as reported by Mumford, as complementary to the machine rather than subordinate to it [4, p. 323]. The ambition, in other words, was to hold people and technology together rather than to optimise either alone. These commitments speak to my critique. Humanising work, I would claim, stands against culture-as-metrics – where people appear as a variable to be improved, and against culture as an instrument of management.

Mumford also records that this ambition was only partly realised. The approach flourished in the 1960s and 1970s but receded in the harsher economic climate of the 1980s and 1990s. Cost-cutting, lean production, and business process reengineering took hold, and socio-technical approaches came to be seen as expensive and risky [4, pp. 331–332]. On Mumford's account, this was a matter of economic and organisational circumstance rather than of any flaw in the tradition's aim. Already in the 1990s, Mumford warned that managers eagerly adopt new,

often untested management ideas, such as business process re-engineering, without anticipating the human and organisational risks they bring [28, pp. 321, 328, 330]. Contemporary socio-technical research continues this aim. Bednar and Welch, for example, argue for one integrated socio-technical whole rather than separate social and technical strands, a whole that evolves through human agency and the meanings people seek in their work [29, pp. 286, 289, 292].

The tradition has developed a range of methods, from participative design to models for accident analysis and the ergonomics of work systems [30, p. 242]. Malatji et al. apply the tradition to cybersecurity, and their framework proceeds by sorting organisational practices into social, technical and environmental dimensions, which are then to be aligned [30, pp. 241, 253]. Culture appears there as an attribute of the social dimension [30, p. 238]. I take a different route, and supplement the tradition with science and technology studies for a vocabulary in which the social and the material are not sorted in advance. Kaghan and Bowker read the socio-technical tradition as an early precursor of actor-network theory, and actor-network theory as a natural outgrowth of concerns close to those of the tradition [22, p. 255]. Where the two differ, they argue, it is mostly a matter of emphasis and focus [22, p. 265]. The socio-technical tradition has attended to the social and psychological conditions of work and to the participation of employees in designing it. Actor-network theory has developed concepts for following how people, technologies and other materials are drawn together, and treats the world as socio-technical "all the way down" [22, p. 262]. I take up the socio-technical tradition for its direction, and science and technology studies for an extended vocabulary and analytical tools.

2.2.3. Science and technology studies as an analytical vocabulary

I turn to science and technology studies for concepts that make the relation between people, cultures and technology available for empirical study. Perspectives from this field have begun to enter security research in the study of cybersecurity politics [31], in cybersecurity [8] and in information security management [32]. Hedström et al. [32, pp. 43, 51–52] read a university security breach as a failure of negotiation and alignment among human and non-human actants. Vuorinen [8] traces the human–technical split in cybersecurity to a dualist lineage in Western thought, and shows how it is embedded in standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. These perspectives have also entered studies of everyday security practice [5]. Of this work, I build most closely on Kocksch's study [5, pp. 4–5, 8] of how people live with technologies that are never fully secure. It shows information security as something done and maintained in everyday practice, and approached through care. I direct these perspectives at a different object, namely the concept of culture through which ISC research approaches security practice.

Actor-network theory, developed by Callon, Latour and Law among others, studies how arrangements of people, technologies, documents and other materials are assembled and held together [22, p. 253], [33, p. 224], [34]. Rather than starting from fixed categories of the social and the technical, it follows the actors and the relations through which an arrangement comes to work, or fails to.

I take the position that the social and the material are constitutively entangled in everyday organisational practice [6, p. 1437]. By this I mean that people and technologies do not first exist as separate entities that then interact. What a technology is and does, and what people do and mean, take shape together in practice [6, p. 1438]. I refer to this as a sociomaterial position.

Within this position, the distinction between people and technology is analytical rather than ontological. It can be drawn to describe a situation, but it does not tell what the situation is made of. This is why I can use actor-network concepts as an analytical vocabulary without adopting actor-network theory as a whole. What becomes visible if the relation between people and technology is described symmetrically, without deciding in advance what counts as a human factor and what counts as a technical control? Such a description does not attribute intention or understanding to technologies. Meaning, on this view, takes shape in sociomaterial practice. Symmetry is also what allows the meaning-centred account of information security culture proposed above to sit alongside actor-network analysis without contradiction. The one is a discipline for observing, and the other a way of understanding what the observed relations come to mean.

What security is in practice is better conveyed by work on care and fragility. This work shows security as never finished, and as held together by ongoing and often invisible maintenance of arrangements that are never fully secure [5, pp. 4–5, 8]. Actor-network concepts help analyse how such arrangements hold or break, and care and fragility describe what kind of arrangements they are. Table 1 summarises the concepts I use. The selection is not exhaustive.

Table 1
Analytical concepts from actor-network theory

Concept	What it describes
Actor-network	Security is held together by people, technologies and documents. A technology works as it does because of the network it is part of, not because of properties it has alone [8, p. 534], [34].
Translation	How a rule or a meaning changes as it travels from policy to architecture to daily practice, and how instruments turn practice into objects that governance can read [33, pp. 203, 214–215, 223–224].
Enrolment	Drawing actors into an arrangement and holding them there. The moments where enrolment breaks are revealing [33, pp. 211, 219–221].
Inscription and delegation	Interests and tasks are inscribed into written material and technical systems, such as a security policy or password protection, and people must arrange themselves around them [32, p. 47]. A human "failure" can then be read as one end of an inscription shaped in a particular way.
Symmetry	A principle of method, not an ontological claim. The division between human factor and technical control is withheld long enough to study the relation [33, pp. 200, 221].
Negotiation	The back-and-forth through which the secure and the insecure are done together in the relations themselves, without a single deliberate negotiator [33, pp. 211–212, 218]

The word "negotiation" may seem to imply more intentionality than the relational view explained so far should allow. I retain the word here in its actor-network sense, in which a

negotiation among actors does not require a single deliberate negotiator, nor indeed deliberate negotiation, since it plays out in the relations themselves [33, pp. 211–212, 218]. Kaghan and Bowker describe socio-technical arrangements in the same spirit, as negotiated orders whose routines are reproduced through ongoing negotiation, and note that even a stable arrangement takes continuing work to hold in place and is never final [22, pp. 257–258], [35, p. 382]. It is not a meeting of human parties at a table. Information security, in this view, is neither a static configuration of technical controls, nor a patch to be "installed" into the culture and instilled in people's behaviour. Instead, it takes shape in sociomaterial practice. Negotiation in this sense includes the pragmatic, daily compromises people make between security protocols and the demands of their work, but it is not limited to them. In a symmetrical analysis, the protocols, systems and data take part as well.

3. A research agenda and two conceptual examples

I intend the alternative, sociomaterial concept of information security culture to be put to empirical work. This makes a particular kind of case interesting, namely a setting where sociomaterial practice is visible and contested. In other words, cases where the meaning people make of security can be observed as it forms in everyday practice. The two examples below are conceptual vignettes, not empirical findings. They draw on general practitioner knowledge and do not describe any particular organisation, but also draw on the author's practical work experience. Each example shows first how the case appears when seen through the two assumptions, and then what the concepts from science and technology studies make visible. The examples are offered as inspiration for further research rather than as a fixed study design. They can be taken up by researchers in other organisations and countries, and the possibilities for variation are many. The criteria suggested below are illustrations, not a complete list.

3.1. Methodological considerations

Methodological commitments follow from the concept of culture I have presented. If information security culture is the layer of meaning behind what is espoused and done, rather than the espoused statements or the behaviour alone, it has to be interpreted through qualitative, interpretive organisational study. Such study should be attentive to the gap between what is said and what is done, and conducted where people work through the technologies they use. In practice, this means combining interviews, individual and in groups, with observation of the situations where security is worked out, such as advice and support, and with documents and traces read as texts [9, p. 323]. The need for such study is underscored by research documenting the disconnect between corporate security policies and actual security practices [26, p. 467]. Kocksch describes security as an ephemeral object that appears and disappears in practice, and argues that studying it requires praxiographic attention, that is, attention to the practices through which security is done, to what is rendered organisationally invisible [5, p. 10].

One commitment follows from symmetry. The researcher does not decide in advance whether a breakdown is a human or a technical matter. Logs, alerts, support tickets and policies therefore need to be treated in the analysis as participants and as texts shaped by both human behaviour and system configuration, interpreted alongside interviews rather than read as objective measurements of security. Symmetry in turn makes the researcher's own position part

of what is studied. A researcher who also holds a role in the arrangements under study, as I do, both helps to uphold them and advises the people who work within them. Participants who know this may present compliance rather than practice [9, p. 322], while an advisory role may make some more willing to share their workarounds. The researcher is then an actor within the negotiation, caught between compliance enforcement and symmetrical observation, and should document that position reflexively, noticing the awkwardness and moral imperatives that a researcher's presence induces [5, p. 10]. Where a study develops alternatives with practitioners, it follows a co-productive approach in which participants take part in shaping the research, and in which the terms of participation are themselves worked out with the participants [36, pp. 13, 22], in line with the participative tradition of socio-technical design [4, pp. 318, 322] and with action research. For each example, a table translates these commitments to the specific case.

3.2. Example A: Research data in everyday research practice

What makes research-data practice a relevant case for information security culture is the ongoing work through which research data are kept secure enough. Researchers and support staff decide what counts as personal data, important, or confidential. They must choose where data are stored and shared, and keep imperfect arrangements of services, plans and routines going. Meanings of security take shape in this work, and knowing what is sensitive is itself a sign of "membership and competent practice" [37, p. 333]. Since research is the core activity of a research organisation, security here concerns the core of the work rather than a support function. The first example is therefore the care, maintenance and fragility of everyday research-data practice.

Seen through the two assumptions I have questioned, that culture is a property of people and that the human and the technical are separate domains, culture appears as researchers' awareness of the rules, to be raised by training, and the storage service appears as neutral infrastructure outside culture. Researchers who store data outside approved services become a compliance problem. The concepts from science and technology studies show more. Read as negotiation, research-data practice is an ongoing process in which what is secure enough is worked out, again and again, between researchers, support staff, plans, services and the data themselves. Each concept below follows that process at a particular point. Read through translation, a data management plan translates a research plan into a governance object. What the plan comes to mean, as a tool for the research or as a form to be filled in, cannot be read from the template. Table 2 suggests how the commitments in section 3.1 can be taken up in this example.

Read through enrolment, the approved storage service draws researchers, data and support staff into one arrangement. Callon's study of the scallops of St Brieuc Bay illustrates what such an arrangement depends on [33, pp. 202, 219–220]. It depended not only on persuading the fishermen but on whether the scallops anchored to the collectors provided for them. In the same way, whether the storage arrangement holds depends on more than researchers' awareness. It also depends on whether the service fits the data's size and format, whether collaborators outside the institution can reach it, and whether it supports the analysis the research requires. When the data, like the scallops, do not stay where the arrangement expects them, the researcher's workaround is where the negotiation becomes visible. Workarounds mark where enrolment fails, and may reveal a mismatch between the service and the epistemic needs of the

research rather than a lack of awareness. In a symmetrical analysis, the service, the plan and the data take part in that negotiation as well.

Where the arrangement appears established, at least to those who maintain it, the negotiation is mostly quiet. Its outcomes are settled for now, in routines and habits, rather than decided once and for all [38, p. 11], and two further concepts read it well. Domestication describes how a technology is made one's own in a specific setting, through practical as well as symbolic work [38, p. 10]. A domesticated service is no longer noticed as security. It is carried in routines and in local understandings of what the service is for. Care describes the ongoing and often invisible work of keeping an imperfect arrangement going [5, pp. 5, 8]. It is through such care, by researchers and support staff, that each provisional settlement keeps holding. What the arrangement becomes, and what security comes to mean in it, take shape together in this everyday work, entangled with the epistemic cultures of the research.

For governance, the workarounds point to where approved services, data management plans and support routines need to be redesigned together with researchers, so that secure handling of data fits the epistemic needs of the research. They can also inform long-term planning of organisational capabilities, and give a setting in which socio-technical solutions, such as socio-technical cybersecurity frameworks [30], can be tested and adjusted in practice. This puts the socio-technical principle of participation into practice, since those who live with a system take part in shaping it [4, pp. 321–322].

In practice, a study of this example could combine interviews, participatory observation and document analysis. Researchers could be interviewed individually and in research groups, together with the support staff who advise on data management, privacy and storage. The situations where data handling is worked out can be observed, such as advice on data management plans, project start-up and archiving, and one dataset can be followed from collection to archiving together with the researcher. Data management plans, service descriptions, guidance on classification and de-identified support requests can be read as texts shaped by both people and the services they describe.

Further research has rich opportunities to vary such studies, for instance across data types, disciplines with different epistemic cultures, career stages and gender. Comparisons across universities and countries, with different regulation and research infrastructures, could show how such arrangements take shape differently.

Table 2
Methodological commitments in Example A, research data

Commitment	What it means in this case	How it can be done
Interpretive study of meaning, attentive to the gap between what is said and what is done	What "sensitive" and "secure" mean in different research fields, and how this differs from what policy and the data management plan state.	Comparing what the data management plan states with how the data are handled. Example question: What counts as sensitive in your field, and how did you learn to tell?

Commitment	What it means in this case	How it can be done
Attention to where security appears and disappears [5, p. 10]	Where an arrangement appears established, security is mostly unnoticed. It is carried in routines and in the work of keeping an imperfect arrangement going.	Attention to the maintenance work of researchers and support staff. Roles and committees, work processes and technical layers can be used as a checklist of places to look [30, pp. 238, 240], though not as (a priori) categories to sort findings into.
Co-production with participants	Where workarounds point to a mismatch with the needs of the research, alternatives are developed with those who live with the arrangement.	Workshops with researchers and support staff on plan templates and support routines. Participants take part in interpreting what was found [4, pp. 321–322], [36, pp. 13, 25].

3.3. Example B: Zero Trust as a reconfiguration of access

The second example is a possible empirical case, the reconfiguration of a network architecture from perimeter-based security towards Zero Trust in an organisation. In a Zero Trust architecture, access is granted through continuous verification of users and devices rather than through a trusted network perimeter [39, pp. ii, 4]. Vuorinen proposes Zero Trust as a practical counterpart to the symmetry of actor-network theory [8, p. 535]. Because users and devices alike must continually prove their legitimacy, the architecture treats human and technical entities in the same way. I build on this reading, and on Vuorinen's argument that the split is embedded in standards [8, pp. 531, 533]. I also take it further, because I will claim that symmetry in a design principle is not the same as symmetry as a method. Zero Trust inscribes a symmetrical rule, but whether people and devices are treated alike is settled in practice, in configuration, exceptions and support. Symmetry is then the analyst's stance for finding out, not a property the architecture already has. Vuorinen also notes that the system verifies behaviour rather than judging intent [8, p. 535]. However, what the architecture comes to mean cannot be assumed from the design language of the architecture. Verification may be taken as routine, as protection, as an obstacle or as distrust, and whether it is understood in terms of trust at all cannot be assumed. What Zero Trust becomes and what it comes to mean take shape together in sociomaterial practice, entangled with the cultures of the organisation in which it is configured and used. Table 3 suggests how the commitments in section 3.1 can be taken up in this example.

Seen through the two assumptions I have questioned, that culture is a property of people and that the human and the technical are separate domains, culture appears as the awareness of employees and their willingness to comply, and Zero Trust stays outside culture as a technical control. The question then becomes whether they comply with its authentication demands or work around them. The concepts from science and technology studies show more. Read as negotiation, the reconfiguration is a process in which what counts as secure, and what

counts as workable, is worked out anew between employees, devices, policy, the IT function and the architecture. Each concept below follows that process at a particular point. Read through delegation, Zero Trust is designed and described as a re-delegation of trust [39, p. 4]. In this script, the work of judging who may be trusted, once carried by people, context, and the network perimeter, is handed to continuous verification by the system. What the delegation becomes in practice cannot be read from the design. The questions that follow concern who is relieved of trust-work, who is given new verification-work, and what had to change for the system to take the job.

Read through enrolment, the reconfiguration is an attempt to enrol employees, devices, the IT function, and policy into one reconfigured network. The revealing moments are where enrolment breaks, as when an employee who routes around repeated re-authentication to meet a deadline marks a point at which the network failed to hold. In a symmetrical analysis, the authentication system, the policy behind it and the deadline take part in that moment as well, and the workaround is not filed in advance as "user error" or as "system limitation". Following Star [35, p. 382], [40, p. 44], it is also a moment where infrastructure, which usually stays out of sight and becomes visible when it breaks down, becomes visible as it changes. Read through translation, one can follow whether the meaning of "security" holds or shifts as it passes from policy to architecture to daily practice. Here the negotiation is visible, in workarounds, requests for exceptions and adjustments of configuration, and each settlement is provisional.

What such a breakdown comes to mean for those involved is the question of culture raised above. For governance, routing-around is information about how the architecture fits the work, not only a violation to be logged and met with further awareness training. Where the negotiation shows friction, configuration, exceptions and support routines can be adjusted, so that the secure way of working is also a workable one. In the terms of the socio-technical tradition, this means designing the security configuration jointly with the work it is meant to protect, treating the burden of repeated re-authentication as a question of humanising work, and involving those affected in deciding how exceptions are handled [4, pp. 321–322].

In practice, the groups and material differ from those in Example A. A study could include employees in different kinds of work, as well as those who plan and configure the architecture and those who handle exceptions and support. Planning meetings, the handling of requests for exceptions and support work can be observed, and one access path can be followed from device to service. Relevant documents include architecture and configuration documents, policy, communication about the change, requests for exceptions, and aggregated access and support data.

Here, too, studies could vary, for instance across kinds of work that depend on access in different ways, roles, gender, and the periods before, during and after the reconfiguration. Comparing the reconfiguration across organisations or countries could show how the same principle takes on different meanings in different settings, rather than which organisation has more of a security culture.

Table 3
Methodological commitments in Example B, Zero Trust

Commitment	What it means in this case	How it can be done
Interpretive study of meaning, attentive to the gap between what is said and what is done	What repeated verification comes to mean in daily work, and whether it is understood in terms of trust at all, and what the principle that "trust is never granted implicitly" [39, p. 4] becomes in the organisation compared with what the policy states.	Comparing what the policy states with what the principle becomes in daily work. Example question: How do you experience logging in and being verified in your daily work now, compared with before?
Attention to where security appears and disappears [5, p. 10]	The reconfiguration makes visible what an established arrangement keeps out of sight [6, p. 1444].	Attention to what becomes visible as access practices change. The technical layers, from device to service, used as a checklist of places to look [30, p. 240].
Co-production with participants	Configuration and exceptions can be shaped together with the work they are meant to protect.	Employees involved in deciding how exceptions are handled. The burden of repeated authentication treated as a question of humanising work [4, p. 321].

4. Discussion

Read together with the conceptual inquiry, the proposed empirical examples point to an alternative perspective on information security culture. The research question asked how information security culture can be understood and studied in a way that centres the everyday information security practices of people in organisations and the technologies they involve. My answer is a proposal rather than a finding. Information security culture can be understood as the shared and often tacit meanings of security that take shape in everyday sociomaterial practice (section 2.1.3). These meanings and the technologies they are entangled with can be held together analytically, in the spirit of the socio-technical tradition (section 2.2.2), and analysed symmetrically as negotiations in which security is maintained rather than achieved (section 2.2.3). The two examples show that such negotiation can be mostly quiet where an arrangement appears established, as in research-data practice, where maintenance and care matter as much as friction, or visible, as in a reconfiguration towards Zero Trust, where delegation and translation are reworked at once. Such a culture can be studied where it takes shape. This means following practices and workarounds rather than measuring attitudes alone, reading logs and other traces as texts alongside interviews, and accounting for the researcher's own position (section 3.1).

Across the examples, the concepts open questions that the two assumptions leave out. They ask what a data management plan, or the principle that "trust is never granted implicitly" [39, p. 4], comes to mean on its way into practice, where an approved service or a reconfigured network fails to hold, and who is given new work when a task is handed to a system. Above all, they ask where the compromise between the secure and the workable is worked out, and who and what takes part in it. None of these can be answered by measuring awareness alone.

For governance, recognising the negotiation means treating friction and workarounds as information and involving people in shaping the arrangements they work with. It also means judging success by whether secure work is workable, and not only by compliance metrics. This complements training and awareness work rather than replacing it, in line with calls to complement and extend the prevailing, individual model of awareness [19]. The documented gap between security policies and practices [26, p. 479] suggests that security efforts falter where policy and practice diverge, and this is where such governance can help people work more securely. In this, governance follows the direction of the socio-technical tradition, to design the social and the technical together and to humanise work [4, p. 321].

Recognising these negotiations also raises the question of power. Actor-network analysis has been criticised for describing networks from the point of view of the victors, or of management, and for overlooking the invisible work of those further from the centre [40, p. 33]. This makes power a question for empirical studies of information security culture, whether they take up the examples outlined here or other settings. An arrangement that is stable for some may be a source of trouble for others, who must use it without belonging to the community that maintains it [40, pp. 42–43]. Studies should therefore ask whom an arrangement is stable for, who carries the cost of keeping it in place, and whose meanings of security count [3, pp. 47–48], [40, pp. 43–44].

5. Limitations

The perspective offered in this idea paper has clear limitations. The argument is conceptual, and the examples are thought through rather than studied. In other words, the perspective remains to be tested empirically. Similarly, the claim that organisational governance which recognises these negotiations can help people work more securely is argued here rather than shown. Whether it holds is a question for empirical studies that take up the concepts offered in this idea paper.

The examples do not describe any particular organisation, and an insider position gives access but also shapes what a researcher is likely to see (section 3.1). Negotiation may capture moments of friction better than the steady maintenance of settled arrangements, or the agency of workers, which is one reason to pair actor-network concepts with work on domestication, care and fragility.

6. Conclusion

In this paper, I asked how information security culture can be understood and studied in a way that centres the everyday information security practices of people in organisations and the technologies they involve. I problematised two assumptions that underlie prevailing models of ISC and CSC, drew on organisational culture studies, the socio-technical tradition and science and technology studies to propose an alternative perspective, and illustrated the proposed

alternative through two conceptual examples, one in which the negotiation is mostly quiet and one in which it becomes visible. The central implication is that, alongside training and awareness work, GRC that recognises the negotiations through which security is worked out can help people work more securely and can contribute to how information security culture changes. The path is indirect, in the sense that governance shapes the conditions of everyday work, such as which services are approved, how access is configured and how exceptions are handled. Within those conditions, people and technologies keep negotiating what is secure and what is workable, and it is in this sociomaterial practice that meanings of security take shape. Change is then not a planned move from one culture to another, but continuous, and accomplished by all those involved in their daily work [3, pp. 40–41]. When the conditions change, the negotiation changes, and so, over time, may the culture. This is a proposal to be discussed and tested, not a finished answer. The socio-technical tradition has sought to see the human and the technical as a whole from the start, and the perspective offered here gives that ambition a language for information security culture.

Several research avenues could follow from this. The most immediate is empirical, and involves studying settings where sociomaterial practice is visible and contested. Examples are the care and maintenance of everyday research-data practice and a reconfiguration towards Zero Trust. Such studies would ask how security is done and made sense of there, rather than how closely behaviour matches a policy. A longer-term avenue could be to take up a methodological and epistemological challenge. It could ask how the relational insights I have developed here can inform a re-specification of the functional metrics commonly used in GRC. The aim is not to combine incompatible paradigms, but to use relational insight to re-read and critique what audit-driven compliance measures count and what they leave out. Another aim could be to explore how GRC professionals can work reflexively within functional constraints.

Declaration on Generative AI

During the preparation of this work, the author used Claude (Anthropic) in order to draft content, simulate peer review, paraphrase and reword, improve writing style and draft the abstract. Further, the author used Claude for Tables 1–3 in order to assist with formatting, and for support in checking citations and page references, which the author verified manually and entered using Zotero. The author used Microsoft Copilot in order to simulate peer review, including discussions of cited papers. The author used Grammarly in order to check grammar and spelling and improve writing style. After using these tools/services, the author reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

[1] M. Alvesson and J. Sandberg, 'Generating Research Questions Through Problematization', *The Academy of Management Review*, vol. 36, no. 2, pp. 247–271, 2011, doi: 10.5465/amr.2009.0188.

[2] E. Jaakkola, 'Designing conceptual articles: four approaches', *AMS Rev*, vol. 10, no. 1–2, pp. 18–26, Jun. 2020, doi: 10.1007/s13162-020-00161-0.

[3] M. Alvesson and S. Sveningsson, *Changing Organizational Culture: Cultural Change Work in Progress*, 3rd edn. London: Routledge, 2024. doi: 10.4324/9781003474555.

[4] E. Mumford, 'The story of socio-technical design: reflections on its successes, failures and potential', *Information Systems Journal*, vol. 16, no. 4, pp. 317–342, 2006, doi: 10.1111/j.1365-2575.2006.00221.x.
[5] L. Kocksch, *Fragile Computing: How to Live With Insecure Technologies*. Singapore: Springer Nature, 2024. doi: 10.1007/978-981-99-9807-4.
[6] W. J. Orlikowski, 'Sociomaterial Practices: Exploring Technology at Work', *Organization Studies*, vol. 28, no. 9, pp. 1435–1448, Sep. 2007, doi: 10.1177/0170840607081138.
[7] T. Brannick and D. Coghlan, 'In Defense of Being "Native": The Case for Insider Academic Research', *Organizational Research Methods*, vol. 10, no. 1, pp. 59–74, 2007.
[8] J. Vuorinen, 'Rethinking the Human–Technical Split in Cybersecurity', *International Conference on Cyber Warfare and Security*, vol. 21, no. 1, pp. 531–537, Feb. 2026, doi: 10.34190/iccws.21.1.4460.
[9] G. Walsham, 'Doing interpretive research', *European Journal of Information Systems*, vol. 15, no. 3, pp. 320–330, Jun. 2006, doi: 10.1057/palgrave.ejis.3000589.
[10] F. Karlsson, J. Åström, and M. Karlsson, 'Information security culture – state-of-the-art review between 2000 and 2013', *Information and Computer Security*, vol. 23, no. 3, pp. 246–285, 2015, doi: 10.1108/ICS-05-2014-0033.
[11] H. W. Glaspie and W. Karwowski, 'Human Factors in Information Security Culture: A Literature Review', in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed., Cham: Springer International Publishing, 2018, pp. 269–280. doi: 10.1007/978-3-319-60585-2_25.
[12] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, 'An analysis on the dimensions of information security culture concept: A review', *Journal of information security and applications*, vol. 44, pp. 12–22, 2019, doi: 10.1016/j.jisa.2018.11.003.
[13] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, 'Developing a cyber security culture: Current practices and future needs', *Computers & Security*, vol. 109, p. 102387, Oct. 2021, doi: 10.1016/j.cose.2021.102387.
[14] Š. Orehek and G. Petrič, 'A systematic review of scales for measuring information security culture', *Information and Computer Security*, vol. 29, no. 1, pp. 133–158, Dec. 2020, doi: 10.1108/ICS-12-2019-0140.
[15] A. Sutton and L. Tompson, 'Towards a cybersecurity culture-behaviour framework: A rapid evidence review', *Computers & Security*, vol. 148, p. 104110, Jan. 2025, doi: 10.1016/j.cose.2024.104110.
[16] K. Reegård, C. Blackett, and V. Katta, 'The Concept of Cybersecurity Culture', in *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, Research Publishing Services, 2019, pp. 4036–4043. doi: 10.3850/978-981-11-2724-3_0761-cd.
[17] A. da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, 'Defining organisational information security culture—Perspectives from academia and industry', *Computers & Security*, vol. 92, p. 101713, May 2020, doi: 10.1016/j.cose.2020.101713.
[18] E. Y. Handri, D. I. Sensuse, and S. Lusa, 'Examining Cybersecurity Culture: Trends and Success Factors', *Journal of Internet Services and Information Security*, vol. 14, no. 3, Art. no. 3, 2024, doi: 10.58346/jisis.2024.I3.020.
[19] M. Skov and L. Kocksch, 'The Cybersecurity Engagement Matrix: From Individual-Pedagogical to Exploratory-Collective Awareness Methods', *20th IFIP WG 11.12 International Symposium, HAISA 2026, Orebro, Sweden, July 6–8, 2026, Proceedings*, vol. 800, in press, Accessed: Oct. 10, 2026. [Online]. Available: https://link.springer.com/book/9783032353276
[20] M. Karlsson, F. Karlsson, J. Åström, and T. Denk, 'The effect of perceived organizational culture on employees' information security compliance', *ICS*, vol. 30, no. 3, pp. 382–401, May 2022, doi: 10.1108/ICS-06-2021-0073.

[21] T. Schlienger and S. Teufel, 'Information Security Culture', in *Security in the Information Society: Visions and Perspectives*, M. A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan, Eds, Boston, MA: Springer US, 2002, pp. 191–201. doi: 10.1007/978-0-387-35586-3_15.
[22] W. N. Kaghan and G. C. Bowker, 'Out of machine age?: complexity, sociotechnical systems and actor network theory', *Journal of Engineering and Technology Management*, vol. 18, no. 3–4, pp. 253–269, Sep. 2001, doi: 10.1016/S0923-4748(01)00037-6.
[23] S. Evripidou, U. D. Ani, J. D McK. Watson, and S. Hailes, 'Security Culture in Industrial Control Systems Organisations: A Literature Review', in *Human Aspects of Information Security and Assurance*, N. Clarke and S. Furnell, Eds, Cham: Springer International Publishing, 2022, pp. 133–146. doi: 10.1007/978-3-031-12172-2_11.
[24] A. Adams and M. A. Sasse, 'Users are not the enemy', *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999, doi: 10.1145/322796.322806.
[25] S. Alter, 'Sociotechnical Systems Through a Work System Lens: A Possible Path for Reconciling System Conceptualizations, Business Realities, and Humanist Values in IS Development', in *Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development*, S. Kowalski, P. Bednar, I. Bider, and J. Mwakalinga, Eds, in CEUR Workshop Proceedings, vol. 1374. Stockholm, Sweden: CEUR, Jun. 2015, pp. 32–39. Accessed: Oct. 10, 2026. [Online]. Available: https://ceur-ws.org/Vol-1374/#paper3
[26] M. Sadok, S. Alter, and P. Bednar, 'It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs', *Information and Computer Security*, vol. 28, no. 3, pp. 467–483, Jun. 2020, doi: 10.1108/ICS-01-2019-0010.
[27] P. Bednar, C. Welch, and M. Sadok, 'IS and Cybersecurity Practice: avoiding self-sabotage', in *CEUR Workshop Proceedings*, 2023, pp. 138–145. Accessed: Oct. 10, 2026. [Online]. Available: https://ceur-ws.org/Vol-3598/paper12.pdf
[28] E. Mumford, 'Risky ideas in the risk society', *Journal of Information Technology*, vol. 11, no. 4, pp. 321–331, Dec. 1996, doi: 10.1057/jit.1996.6.
[29] P. M. Bednar and C. Welch, 'Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems', *Inf Syst Front*, vol. 22, no. 2, pp. 281–298, Apr. 2020, doi: 10.1007/s10796-019-09921-1.
[30] M. Malatji, S. Von Solms, and A. Marnewick, 'Socio-technical systems cybersecurity framework', *Information and Computer Security*, vol. 27, no. 2, pp. 233–272, Feb. 2019, doi: 10.1108/ICS-03-2018-0031.
[31] M. Dunn Cavelty, 'Cybersecurity Research Meets Science and Technology Studies', *Politics and Governance*, vol. 6, no. 2, pp. 22–30, Jun. 2018, doi: 10.17645/pag.v6i2.1385.
[32] K. Hedström, G. Dhillon, and F. Karlsson, 'Using Actor Network Theory to Understand Information Security Management', in *Security and Privacy – Silver Linings in the Cloud*, K. Rannenberg, V. Varadharajan, and C. Weber, Eds, Berlin, Heidelberg: Springer, 2010, pp. 43–54. doi: 10.1007/978-3-642-15257-3_5.
[33] M. Callon, 'Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay.', *Sociological Review*, vol. 32, no. 1, pp. 196–233, May 1984, doi: 10.1111/j.1467-954x.1984.tb00113.x.
[34] B. Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*. in Clarendon Lectures in Management Studies. Oxford: OUP Oxford, 2005. Accessed: Oct. 10, 2026. [Online]. Available: https://research.ebsco.com/plink/bbb66d9b-8d22-35cd-a279-7c7f0c5a8c9a
[35] S. L. Star, 'The Ethnography of Infrastructure', *American Behavioral Scientist*, vol. 43, no. 3, pp. 377–391, 1999, doi: 10.1177/00027649921955326.
[36] O. P. Askheim, I. M. Lid, and S. Østensjø, 'Samproduksjon i forskning – hva er det, og hva innebærer det?', in *Samproduksjon i forskning*, O. P. Askheim, I. M. Lid, and S. Østensjø, Eds, Universitetsforlaget, 2019, pp. 13–35. doi: 10.18261/9788215031675-2019-02.

[37] P. Dourish and K. Anderson, 'Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena', *Human–Computer Interaction*, vol. 21, no. 3, pp. 319–342, Sep. 2006, doi: 10.1207/s15327051hci2103_2.
[38] M. Lie and K. H. Sørensen, *Making technology our own?: domesticating technology into everyday life*. Oslo: Scandinavian University Press, 1996. [Online]. Available: https://urn.nb.no/URN:NBN:no-nb_digibok_2008070700049
[39] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 'Zero Trust Architecture', National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
[40] S. L. Star, 'Power, Technology and the Phenomenology of Conventions: On being Allergic to Onions', in *A Sociology of monsters: essays on power, technology and domination*, J. Law, Ed., in Sociological review monograph 38. , London: Routledge, 1991, pp. 26–56.