Policy and Power

A framework for re-thinking information security

Philip Inglesant
Institute for the Study of Science Technology and Innovation
University of Edinburgh
Edinburgh, EH1 1LZ, UK
p.inglesant@ed.ac.uk

M. Angela Sasse
Department of Computer Science
University College London
Gower Street, London, WC1E 6BT, UK
a.sasse@cs.ucl.ac.uk

***Abstract*— Successful enforcement of information security requires an understanding of a complex interplay of social and technological forces. We focus on organizational security policies, and on power in organizations, drawing on socio-technical literature to develop an analytical framework. We present three case studies from a large empirical study in an international company including 55 interviews with staff members at all levels; each study highlights a different aspect of our framework. We suggest ways in which our framework enables existing security policies to be re-thought. We conclude by showing how our findings complement recent research in the institutional economics of information security.**

Keywords: information security; organizations; Actor-Networks; socio-technical systems

I. INTRODUCTION

In this paper, we analyze information security as a manifestation of forms of *power*: the productive form of power as *power-to,* dominant power as *power-over,* and power as the intended or unintended working out of technological and social changes. [6, 39]**.**

Power, then is the theme, but power *with* technology. Ever since researchers at the Tavistock Institute [36] first analyzed the social implications of technical changes, it has been clear that to understand technology in social structures – that is, *all* technology that actually exists – it is necessary to reject what Burrell & Morgan 1979 [7] refer to as the "*techno-functionalist paradigm*" in favor of an approach to technology which takes seriously both the technical *and* the social.

As these early researchers showed, new, more "efficient" working arrangements manifest themselves in new forms of power, in which some workers find themselves disadvantaged and, in response, adopt various forms of defense, "*even though they may not always be clear as to the exact nature of the resentment or hostility they often appear to feel*" [36:16]. This socio-technical understanding of power is paralleled by rejection of traditional "Hobbesian" or sovereign power [14] towards a view of shifting, unstable power expressed through networks and alliances [13].

The argument, at its most basic, is that information security cannot simply be imposed by rule (as "sovereign power"), but emerges from the interplay of social and technical actors. This realization is a challenge to conventional security thinking, which emphasizes written policies and endorsement by senior management (for example, [37]). These are the necessary underpinnings of information security, but says nothing about the on-the-ground enactment of polices in everyday practice. Understanding the interplay between the social and the technical can guide us towards formulating security policies which are acceptable to users and which meet the needs of the organization.

This highly relevant literature has been largely neglected in socio-technical applications to information security. Certainly, there is a wide socio-technical literature adapting cognitive and psycho-social concepts such as trust to design robust online market places and collaborative environments [26, 34] and the awareness that real threats from "social engineering" and human error arise more from social than from technical vulnerabilities. Economics [2, 4, 22] has also provided insights into the costs and benefits of security practices to organizations and individuals.

It is not that these analyses ignore power, but they assume that power is simply *there,* taken for granted, and, in a sense, invisible. Yet, while not often explicit, power underlies the implementation of information security policies. Organizations may assert their policies through enforcement in various ways; yet for each enforcement there is a reaction. Individuals have a choice in the extent to which they comply with security policies, and their choice is based on their goals, perceptions and attitudes {Beautement, 2008 #6;Weirich, 2005 #23;Adams, 1999 #22}.

In this paper, we "stand back" and explore the nature of power within an organization by going back to earlier socio-technical literature and recent insights in the study of organizations. We relate this to cognitive factors, the needs of "*homo economicus*", and social engineering threats. Our aim is to integrate the insights into guidance for senior information security officers who are, after all, *managers,* and required to balance many competing considerations with the overall organizational imperative to support the business needs of the organization [33].

We draw our findings from 55 interviews with employees in a large international company, conducted between May and October 2010. Our interviews were semi-structured around a

pre-prepared schedule, which was sufficiently flexible to allow for later to explore emerging issues. These were fully transcribed and analyzed using Grounded Theory [11, 21], a well-established methodology to generate unifying theories from qualitative data and validate findings in a process of continuous comparison.

II. POWER IN ORGANISATIONS

Although power has been studied extensively in Information Systems (eg by [24]) it has been less studied from the point of view of information *security*. Here, we develop our security framework from seminal literature in the sociology of power and technology.

A. Dimensions of Power

A simple intuitive – or, as Lukes [31] says, "*one-dimensional*" - view of power is that "*A has power over B to the extent that he can get B to do something that B would not otherwise do*" [14]. This is *potential* power – A *can* get B to do something, but does not necessarily in fact do so. This view also implies *conflict*, or at least a difference in preferences – B would not necessarily *prefer* to do the thing that A would like him or her to do.

However, this simple view focuses too much on power which is "*actual and observable*" [31:27]. It is "behaviorist", looking at decisions which *have* been taken and observed, and on wants which *are* expressed or repressed. More recent literature, influenced particularly by Lukes [31] and Foucault [19] has developed the realization that power operates in many complex and competing ways, through "*micro-physics*" [19, 29], as well as through social rules that are not necessarily clearly observable. "*A may exercise power over B … by influencing, shaping, or determining his very wants*" [31:27].

This more nuanced understanding fits very well with our data; in this organization of knowledge workers [16] - that is, of "*responsible individuals who exercise power*" [31] - the organization is not "sovereign", in any simple sense, but asserts its "*power in-the-world*" [23:119] through *play of strategic forces*. Rather than a force which acts directly, we could think about power as like a "*billiard table that is skewed or made uneven"* [12:209].

B. Power and trust

As we shall show, even where policies are enforced by technological means – firewalls, filters, software and hardware configuration - this enforcement is rarely total. Despite the technological controls, the organization has to *trust* its employees not to circumvent or otherwise negate policies, even if there is a strong technological enforcement in place [17]. Trust necessarily involves the acceptance of *risk*; trust is "*an attitude of positive expectation that one's vulnerabilities will not be exploited*" [35:386]; there is *expectation*, not certainty. Conversely, the trust thereby placed in employees is nearly always only one part of a web of social and technological power through which security is maintained in the organization.

Yet, while the concern of security policies is ostensibly to prevent "*bad things from happening*" [8] – while maintaining availability - to protect systems and data from external or internal threats, the actual *operation* of these policies in mainly *disciplinary*, in Foucault's [19] terms. That is to say, it is concerned much less to punish malicious acts than it is with *non-compliance*; while the intention is to *prevent*, this is enacted by requiring positive *effort* on the part of employees, through myriad small rules. This carries a cost: as Beautement et al [5] have shown, compliance is a limited resource.

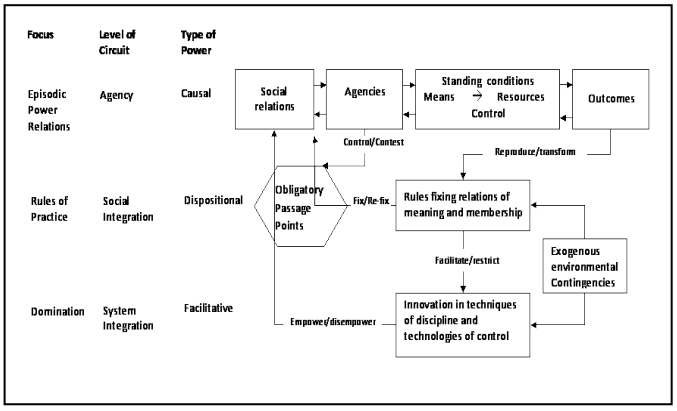

Figure 1: Representing the circuits of Power: from Clegg [12:214]

In this paper, rather than taking trust and enforcement as a *dialectic*, we consider both as different facets of *power*. In the remainder of the paper, we develop a framework, based on developed from Clegg's [12] Circuits of Power model, and use it to analyze some specific studies of security in action, drawn from our empirical research. Using this framework enabled us to identify the breakdowns in security policies, and to suggest ways in which these might be overcome.

III. POWER AND TECHNOLOGY: "*TECHNOLOGY IS SOCIETY MADE DURABLE*"

How does an organization assert its policies? Certainly not by expecting employees to read and then follow written documentation or rules; in this organization, few participants are even aware of the existence of written policies (on the company intranet). Rather, power is inscribed and normalized through micro- and macro-level "circuits" of integration (to use Clegg's [12] explicitly electrical metaphor).

A. Episodic Power

The most obvious and easy accessible instances of power, as an organization asserts the need for information security, are the passwords, ID cards, open or closed work spaces, open or closed computer builds, firewalls, etc., which form the daily practices of information security. As the most visible manifestations of power, these practices are easily mistaken for the totality; this is the "normal power" of most social science and security studies.

But the achievement of the aims of a security policy depends on 1) the alignment between the policy and its intended outcome as well as 2) the level of compliance with the policy, so that any security measure must be both "*correct*" and "*dependable*" (actually being used as intended) [17]. This micro level focuses only on the dependability in the details of

practice; we have to go beyond these most evident phenomena, to consider how best to achieve the desired *outcomes.*

Episodic power draws from, and leads into, "macro-level" *circuits of power* in which "*rules, relations and resources*" [12:211] are reproduced or transformed, fixed or re-fixed, facilitated or restricted. These other circuits, which Clegg [12] terms the circuits of *social* and *system* integration, make up a "field of force" within which certain fixtures of meaning are given more power; an *actor network* [10] is constructed.

B. Social integration

Social integration in the "dispositional" circuit of power centers on the construction of *meaning*. This construction may draw on (or "enroll") various human, social and technological actors and techniques of control, but *power* comes from the meaning that is attached to each of these entities.

Latour [28] provides an illustration of human and non-human domination as an artifact and its associated network – hotel customers and their room keys - is progressively *transformed*, via polite notices and a heavy weight attached, so that customers leave the key at the hotel front desk rather than walking off with it, not because they have read the polite notice – they might not even speak the language – nor because they are particularly well-mannered, but because "*they cannot do otherwise. They don't even think about it*" [28:105]. There is a clear parallel with Lukes' insight that "*power is at its most effective when least observable*" [31:1].

Hotels? Room keys? There is, superficially, only a slight link with information security (Latour is not concerned with doors, only with keys); that is the strength of the framework. This very general framework applied to information security strengthens our analysis, allowing us to put to one side our pre-existing assumptions about "the social", "the technological", and "power"; we are "agnostic" in our assumptions, and "symmetric" in our approach to technology and society [9].

C. System integration

While recognizing that "society" and "technology" work together, it is also useful analytically to maintain a separation between social and "system" forces: "*material conditions most obviously include the technological means of control over the physical and social environment"* but also *"the material means of organization*" [30:251]. *System integration* covers whatever an organization uses, whether technology, physical constraints, or rules backed up by contractual enforcement, to enforce the institutional patterns. This is also productive power, or "power-to", and hence also *facilitative power* [12].

Employee compliance is harder to obtain where there are *tensions* between social and systems integration; that is, where requirements imposed by rules or technological means are in conflict with social expectations [1]. In the wider context, these tensions may lead to institutional change, but also to resistance, strain, and failure to meet organizational aims.

An "obligatory passage point" – a concept drawn from Actor Network Theory [9, 10] - is the crux of these circuits of power [23]. This can be thought of as a rhetorical device; one set of actors presents a problem in a way which asserts that there is "no alternative" but to see the solution in a certain way, and then to "enroll" the other actors around this central problem; power, then, is a construction of *meaning* in such as way as to favor the interests of some actors over others.

IV. Empirical Research

Our 55 interviews covered employees at all levels of the company and their interactions with the organizational security policies. From our knowledge of the policies, we had some specific areas of interest to explore, but we were keen to encourage wide-ranging discussion and narratives around the ways these policies are encountered in everyday working practice.

At the highest level of attitudes to security, we developed our interview schedule around three dimensions:

- How much do participants know about organizational security policies? What training and induction have they received in security policies?
- To what extent do they comply with these policies? If they do not comply, how do they express this non-compliance and what reasons do they give?
- How much do they think *others* know and comply with the policies? What is the organizational security culture?

Our research was based in an industry with a strong *safety* culture, and this safety culture extends to all staff. But does this strong safety culture extend to information security? What are the interplays between physical and information security?

Although we were interested in security policy and compliance across all areas, we focused particularly on specific policies around acceptable use, ability to install and configure software on PCs and laptops, physical security practices – clear desk, screen locking, and controlled access to sites, and encrypted USB sticks – a policy that had been recently introduced.

Our Grounded Theory analysis produced a total of 3320 quotations labeled with 3114 raw codes organized by these policy interests, annotated with 311 memos (short notes made during Grounded Theory analysis), which we then organized into networks and families. Unlike other studies that have applied Clegg's [12] model to information security [27], we did not start from the intention to place organizational power at the centre of our data analysis. Rather, following Grounded Theory [21] tradition, we started from the data, with little more than the general intention to investigate from the data the responses of individual staff members to organizational rules; thus, the search for a suitable theoretical framework was deliberately *a posteriori.*

V. Applying Power: Three Case Studies in Information Security

To show how this works in practice, and to explore the use of our framework for information security policies, we analyze three situations of power in the company.

In the first study, compliance is largely enforced through technological means; in the second, compliance is not enforced directly, but by rule; in the third study, social norms are

enrolled to assist in compliance, but, as we shall see, these norms both strengthen and, in other ways, act against compliance.

A. Study 1: Technological Enforcement:"Closed build"

Our first study analyses a situation in which compliance is actively enforced by technological means: restricted use of software on company-issue personal computers and laptops, enforced through a "closed build" which requires approval by a manager and action by outsourced technical support to install or configure software. A similar policy restricts acceptable use of the Internet and external email through filters and firewalls.

In our analysis (Figure 2), the actors – employees, the company, computers, software, outsourced technical support, and also actors such as colleagues and customers, with their demands on staff - are "enrolled" to a *problematization* that asserts "locked-down access" as an *obligatory* passage through which access to software *must* pass. The construct is not actually quite as simple as "no use of non-standard software"; the policy provides for negotiable use of other software or, in exceptional cases, a computer build that is more or less open. Adding or re-configuring software takes time, however; and the company is trying to reduce the use of open builds.

1) Response 1: Acceptance

We start by noting that many participants express themselves unaffected by the acceptable use policy; they never have a reason, in the course of their work, to use non-standard software. Yet these participants, too, are complying with the policy and are, in fact, affected by it, not by what they are "got to do" [14], nor even by what they are prevented from doing, but in what they *do not even consider doing*. In these situations, we can say that the company has successfully stabilized the meaning of "acceptable use" to the extent that staff members comply without even considering alternatives:

> *No we don't have rights to most things. You know you can't do anything really, very much. And I mean truthfully most of us don't know what to do anyway – European staff member*

The "closed build" avoids security problems from unknown software or viruses, problems with maintaining multiple versions, etc. - but this enforcement carries *costs*. These costs are in terms of employee time, and hence productivity:

> *I mean, it's a pretty tedious process, but you just put in the request for what you want, fill in a form, send the request away, and then it gets approved by your manager. – European staff member*

In effect, maintenance is more centralized and controlled, constraining the availability of software; and this, too, carries *organizing* costs [32]. Company power is maintained by disempowering staff members, in Clegg's [12] terms:

> *P: I wish I had administrator access though.*
> *I: Is that because you find it gets in the way, not having it, or …*
> *P: It has, occasionally, um, you know, and it's more along the lines of, … I don't know if I actually care about administrative access to my laptop, but …, because [the standard build includes some] outdated programs, there are things I can't do that I'm used to doing on computers. – North American staff member*

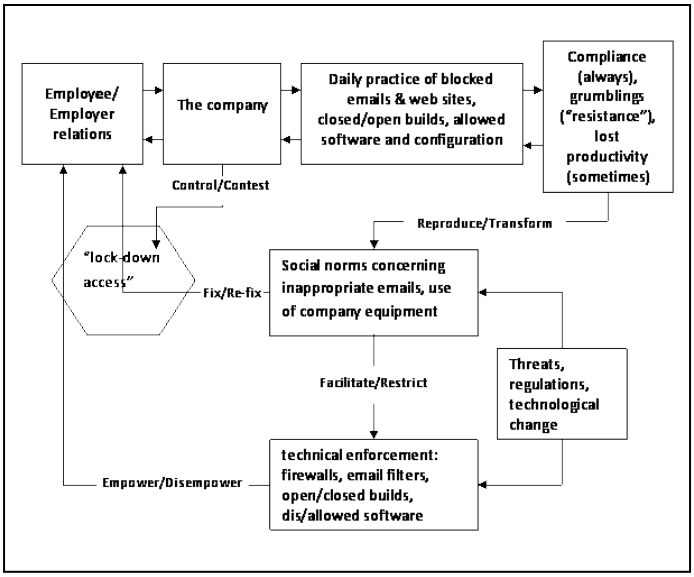

Figure 2: Locked-down access to "closed build" PCs and external Internet

2) Response 2: Avoidance

Even though the policy is enforced by technological means, this does not mean that compliance is total; a participant describes a simple form of avoidance, using a home computer when software required for business uses was not readily available:

> *I think I tried to download Skype …, because I was helping … on some project, I had to communicate with China. So I was trying to do that through a company computer it wouldn't, it wouldn't work.*
> *I: So, um, so, so what did you do then?*
> *Well, I used my home computer. – North American staff member, closed build*

Avoidance allows the user to get the job done; it is a resistant action to avoid centralization, not to avoid the policy as a whole. This enforcement is shown to be doubly problematic: the participant felt forced to avoid the rules, but nevertheless was inconvenienced both in attempting to obtain the software and in making the eventual circumvention.

3) Analysis

Everything revolves around the construction of "locked-down access", in the form of "closed build", firewalls, filters, etc. In Callon's [9] terms, these are "*obligatory passage points*". But **i**t is clearly *not* the case that that all access to software must necessarily pass through these points. Certainly, company policy is enforced if accesses do pass through the obligatory points; but the policy is easily circumvented if an employee – or their software – rejects the approved route by, for example, using their home computer instead.

There is *contested meaning*. The security policy constructs points through which all access must pass, but, against this, staff members also ascribe meaning to the process in their own

terms as "business needs"; an alternative reading which simply does not require passage through these "obligatory" points.

B. Study 2: Trust in Situations of Contingency: USB sticks

Our second case study focuses on a policy that had been recently introduced in the company. This is the requirement that, whenever data is transferred onto an external USB "thumb drive" or "memory stick", the device used must be a company-issued, 256-bit encrypted drive of a specified brand.

This aspect of security policy is of particular interest because of its recent introduction. From the point of view of enforcement, the issue is interesting because such a policy clearly could be enforced using technological means, but, at the time of our research, was not being so enforced.

Use of encrypted USB sticks is clearly an important tool to preserve confidentiality – the "C" in the "CIA" model [38]. It does not in itself prevent other USB-associated risks, such as that of importing viruses and malware on media of unknown origin, but some participants spontaneously mentioned this issue, and, potentially, the requirement to use only company-approved media could also reduce this risk.

1) Actors and Factors in (non)-compliance

The ban on unencrypted USB sticks in the company is, in principle, absolute. However, this absoluteness is challenged by employees in least two ways:

- Will the USB stick and its data leave the immediate work area, or the company building?
- How sensitive is the data (perceived to be)?

For example, a common use of USB sticks is to transfer data onto a colleague's computer, or to take it to a nearby printer – in this way, potentially actually reducing the risk of data leakage through unattended printing over a network.

As intended by the company, this policy relies strongly on episodic power in the daily practices which are to be followed. That is, the emphasis is on micro-techniques of enforcement, with very little leeway allowed for alternative interpretations. In practice, in the absence of technical enforcement, this power is weak; instead, the power circuits of social and system integration come to the fore.

2) Non-human actors: USB Sticks and Data Transfer

However, both in the episodic and social/system integration circuits, there are non-human factors in operation that *discourage* compliance with the policy. Our findings confirm those of Beautement et al. [4, 5] in terms of the risk of embarrassment if an important presentation cannot be given. Additionally, some of our participants mentioned problems with size and reliability of the company-approved USB brand:

> *… Sometimes, if you've got a big document you know, sometimes 1 gig is not enough … so I've struggled to get it on- …. Sometimes I've got a document on to give to somebody in the office, the others in the office, …I only need to leave there for a short period of time. And it's not really that sensitive… - European staff member*

A strong dis-incentive to use the company-approved USB sticks emerged in terms of *cost*. Here we noted a wide divergence of practice across the company, with some groups purchasing the approved brand in sufficient numbers for each employee, contrasting with other groups in which the approved sticks were not available; and we found correspondingly varied practices in USB stick use across the company.

The case also illustrates nicely the interplay of emerging technologies, as increasing use of shared, access-controlled filestore – now ubiquitous in large organizations – implies that ad-hoc methods such as USB sticks for transfer data are less and less necessary. At the social level, organizational decisions, such as managers' choice to provide budgetary allowance for company-approved USB sticks, and variable training practices, come into play; compliance is therefore highly dependent on *external contingencies*.

3) Analysis

This second study provides a useful comparison to the first; there are more complex contingencies in terms of variable access to the technology, and also more alternative routes to the overall goal of getting the job done. Returning to the metaphor of an obligatory passage point, enforcing passage of data through the approved USB route and not through any other requires several contingencies to work together. Several actors must be enrolled to act together [9], and that, without this alignment of actors, non-compliance becomes the easier path.

Technically, it would be possible to disable USB transfers altogether – as has sometimes been done in this company. This could deny all USB file transfers, or only unencrypted access. So the rule on its own is a move towards trust in employees. As with closed builds, if the accepted path through the controlled obligatory point is not available – if there is tension between the company-approved and localized meanings - then "business need" is likely to be the dominant discourse.

C. Study 3: Physical security and social norms

It is rarely the case that policies are enforced using *purely* either technological or social constraints, however. In this third case study, we investigate issues around physical security policies that rely on a mixture of social and system power for their enforcement. System power, in this study, is itself partly technological – physical access control on doors, electronic access cards for staff – and partly mediated by humans - dedicated security staff and receptionists.

1) (Non)-Obligatory Passage Points

Physical security begins with access to the car park, where a barrier and, sometimes, a security guard controls access. However, access by other means is not controlled at this stage.

The second, and most crucial, point of access control is at the point of entrance to the building. This is a very physical example of an obligatory passage point – unlike the barrier to the car park, which can be avoided in various ways.

First problem: there is in reality often not one single entrance, hence no single "passage point". Second problem: the apparently obligation at to identify oneself at the building entrance is only partial; doors can be held open politely, or intruders can rush through doors which have been left ajar accidentally.

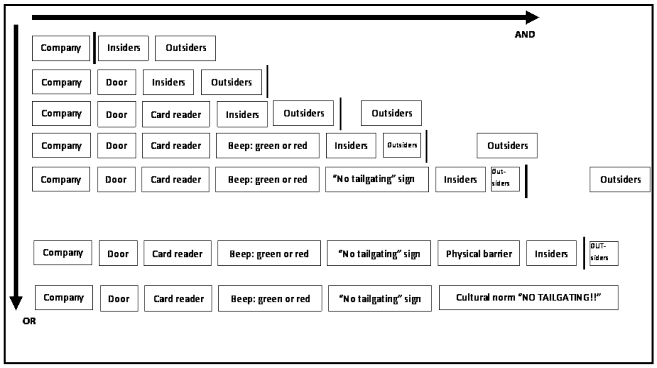

Figure 3: Successively adding actants to control entrances

2) Human Actors in Alliance with Technology

The company could install turnstiles or some other strongly physical barrier, but this might be difficult where there are many entrances. Instead, the company has chosen to form "alliances" [9, 28] with the staff members themselves, who are strongly encouraged to avoid "tailgating" or "piggy-backing". Further allies are "enrolled" in the form of large notices by each entrance. Some entrances also have a card reader, which "beeps" and flashes red or green, but is left to staff members themselves to verify whether this is a "red beep" or a "green beep", so this still requires human actors to play their parts.

Staff members are not always willing to accept the role of "security enforcer", however; moving from "*interessment*" to "*enrolment*", in Callon's [9] terms, requires negotiation. The desire of the company for enforcement pulls against the normal social politeness towards other staff members, as well as their natural desire to avoid confrontation:

> *you do tend to recognize people, but I think in this day and age, you don't want to confront people, it can make it a bit awkward – European staff member*

Nevertheless, with the help of additional "allies" – the large signs, along with a wish to ensure a workplace which is safe for themselves and their colleagues - compliance with the rule is said to be high:

> *I think people are pretty honest with it. I haven't myself ... I've heard people reference that other people tried to piggy back on them, but I think for the most part the majority of people coming in and out of the building are following that policy". – North American staff member*

This compliance, however, – like that of the hotel customers in Latour's [28] example – comes at a cost. Latour says that increase in the AND dimension, progressively excluding outsiders, comes at the cost of "enriching" the desired program of action with a series of "translations" in the OR dimension.

There is, then, a technological cost; but the cost is also felt in the tension felt by staff between company requirements and their own social nature. This cost and tension arises fundamentally from the lack of "fit" [30] between the social and systems integration; staff are asked to comply in ways which run counter to normal social convention.

This tension is expressed, amongst other ways, by *avoidance* in various ways: "having a quiet word" (rather than direct confrontation) or changing practices in subtle ways to avoid the situation of confrontation:

> *I have to time it so that he at least swipes his card. So if I hear the beep, of course I don't know if it's a green beep or a red beep, I don't know [what] happens. So if he swipes it and it beeps, then I'm fine, so I, it, it's a bit of a struggle. So I try and if I see him, fortunately it's all glass so I can see the person coming. So I try and slow down my walk ... - North American staff member*

3) Analysis

Figure 3 is based closely on a figure in [28] – physical and social (and potentially human) "actants" are successively added to the network so that outsiders are increasingly excluded behind the barrier (represented by the solid vertical bar). At one extreme, all doors are locked, and insiders as well as outsiders are excluded; with open doors, the circuit is one of enablement as well as restriction. With only a door and no control, outsiders as well as insiders are allowed in. Progressively adding a card reader, with a beep and red or green light, and signs to remind staff of the "No Tailgating" rule, fewer outsiders get within the barrier, while other outsiders are distanced further from the inside space.

The final two rows go beyond the actually existing physical security to show the "physical access" construct as it might be with either a physical barrier, or where social norms have changed so that "no tailgating" overcomes any residual politeness that staff might feel towards potential outsiders; now, all outsiders are excluded, but at still further costs in technological (barrier) or social (politeness) terms.

VI. DISCUSSION

A. Technology in Trust and Enforcement

In these three studies of areas of security practice, we have considered – as a first pass analysis – the tools available to a security manager in terms of *trust* "versus" *enforcement* of the policy. But, as we have seen that in practice there is almost never complete "enforcement" and never complete "trust". In the first case study, we saw that employees with a "closed" build use "unofficial" circumventions such as using a home computer when required software is not immediately available.

If it could somehow be arranged that enforcement were total, staff would become merely "relay-agencies" with no interests beyond those of the "strategically subordinating agency"; literally, non-actors in any meaningful sense. Conversely, "*high discretionary strategic agency*" expresses power in ways that are "*less prohibitive and more productive, more facilitative of desired outcomes through the disciplined discretion of the agency of empowered authorities*" [12:199].

However, this is not an argument that enforcement should always be minimal. That would be the logical conclusion if compliance were viewed as the antithesis to resistance, and resistance, in turn, as a response to increasingly strong security enforcement [27]. This zero-sum view of power [13] offers little to help security decisions; if security enforcement actions always produce an equal and opposite reaction, then security

can exist only is a state of static equilibrium, under constant tension, and at permanent risk of a loss or shift of equilibrium.

B. Contested meanings

A better metaphor is to consider resistance, not in *opposition* to security requirements, but rather like electronic impedance, so that the "flow" of power around the circuits is inhibited at various points [12]. By considering non-compliance as one among many potential responses to security practices, rather than as a negative practice to be prevented, we shift the central point – the "obligatory passage point" – of our analysis from *resistance* to *meaning*.

Actors attach different *meanings* to security practices. We can see this most clearly in the case of use of unencrypted USB sticks; users frequently circumvent policies but it is almost never the case that users simply refuse to comply; non-compliance is nearly always given as for "a reason", and this reason is usually expressed in terms of the business needs of the organization, which, as we have said, is not so much resistance as an alternative, and equally legitimate, meaning.

This new formulation offers a way forward for re-thinking security policy and enforcement. Rather than taking "locked-down access", "encrypted USB sticks", or "controlled access to the building" as the central points around which trust, enforcement, and technological and human actors are supposed to revolve, the security manager can shift the circuits of power to closely mirror the needs of the business; we could say that "business needs" are the main "actor" who must *interesse* [9] the other actors in the network.

Seen from this viewpoint, the question becomes, not *technology* "versus" *human* enforcement, but "how can meaning be most successfully stabilized around the needs of the business?" Clearly, the "*techniques of discipline*" [19] in the circuit of system integration could be made more "solid", or "reified", but *at the cost of more tension* between the system and social integration, leading inevitably to resistance. As an alternative, and more positive reading. Davenport & Leitch [15] argue that the use of "*strategic ambiguity*" to delegate authority can empower stakeholders while *at the same time* increase the power of the agency which deploys it.

C. Toward an Acceptable and Usable Security Policy

To see how this is useful, we apply our model to one of our case studies – the "closed build" policy (Figure 4). We start, following Callon [9] by rejecting *a priori* assumptions that "locked-down access" is either "correct" or "incorrect" against some normative values. Clearly, if our policy relies on "closed build" as an obligatory passage point, then this policy is effective only to the extent that staff members accept to pass through this point. By using, for example, a home computer to bypass the approved software build, the passage point which we have so carefully constructed is no longer "obligatory"; all the other actors – controlled software, technical support, managers and their approval – which we have enrolled around it become irrelevant.

Where users feel the need to so blatantly reject their ascribed place in the socio-technical network, this is not a failure on the part of the user, but a *breakdown* – "*an interruption of the smooth unexamined flow of action*" [18].

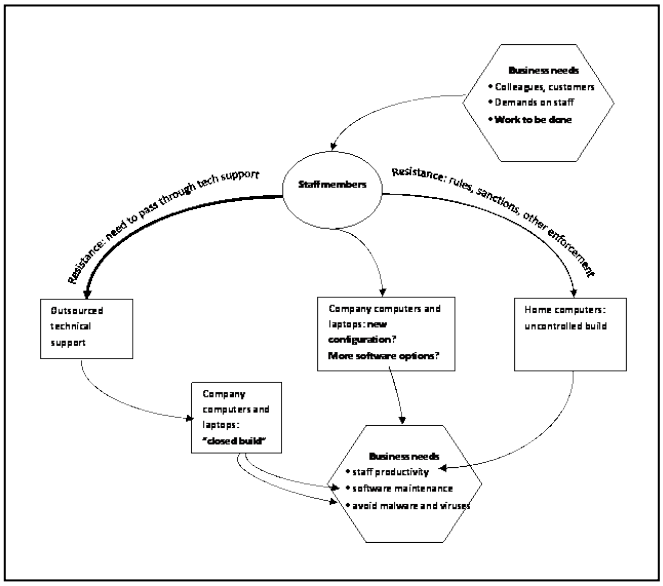

Figure 4: Re-thinking circuits of power in acceptable use enforcement

Such "breakdowns" are a strong clue to tensions between the circuits of system and social integration [12]. Figure 4 shows how the control over software installation might be re-thought by placing "business needs", rather than "closed build", at the centre of the network of actors. Both "closed build" and "home computer" are possible routes for a staff member to meet the business needs of the company and customers.

However, neither of these "passage points" completely meets the business needs. The thick curved arrow on the left indicates that "closed build" encounters *resistance* in the form of the need to pass through technical support – introducing delays. Using a home computer avoids this resistance, but introduces new risks. Clearly, the circuit could be "balanced" by either reducing the resistance on the left-hand route – perhaps by making technical support more easily available – or by increasing resistance on the right-hand route. Both of these choices involved explicit or hidden organization costs, however.

Alternatively, and more productively, both left- and right-hand routes could be replaced by rejecting these established passage points, and building a network centered instead on the business needs. By clarifying the flows of power around the network, other, more imaginative solutions can be explored.

VII. *Conclusions*

It is well-established that security threats are socio-technical; humans are social beings, neither machines nor unconnected individuals – *actors* rather than mere "factors" [3]. In this paper, we return to seminal socio-technical literature in order to develop a view that encompasses both the technical *and* the social, without privileging or making assumptions about either.

Our findings resonate with consistent themes in the literature around the relations between organizations and technology: centralization, de-centralization, hierarchy, and co-operation. From the perspective of information asymmetries, transaction costs and principal-agent relations – central themes of new institutional economics - Pallas [32] investigates the security implications of co-ordination and motivation in organizations,. Enforced

control introduces hierarchical organization costs while at the same time relies on (human) actors who may not always comply – a clear instance of a principal-agent problem [25] – which we could re-specify, in Callon's [9] terms, as a failure of *interessement*.

We have brought ideas from the sociology to bear on these questions. Rather than accepting economic forces as natural, inevitable phenomena, we have analyzed the complex network of actors which work *together* to privilege certain meanings over others. In this way, we have sketched a way to combine sociological and economic perspectives; to focus not only on *why* there are always economic interests but, at macro as well as micro levels, to start to show *how* these pressures operate and how they may be enrolled to the benefit of organizations and their members. In this way, we have developed an understanding which has opened up these complex networks for our inspection, and hence for potential change; it becomes possible to "*penser autrement*" [20:15], to think differently, about the possibilities.

REFERENCES

[1] Adams, A. and Sasse, M. A. Users are not the enemy. Commun. ACM, Vol. 42, 12 (1999), 40-46.

[2] Anderson, R. Why Information Security is Hard-An Economic Perspective. In Proceedings of the 17th Annual Computer Security Applications Conference (2001). IEEE Computer Society.

[3] Bannon, L. J. From Human Factors to Human Actors. Design at work: Cooperative Design of Computer Systems J. Greenbaum and M. Kyng Lawrence & Erlbaum Associates, Hillsdale, NJ, USA, 1991.

[4] Beautement, A., Coles, R., Griffin, J., Ioannadis, C., Monahan, B., Pym, D., Sasse, A. and Wonham, M. Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. In Workshop on the Economics of Information Security (Hanover, NH, USA, 2008).

[5] Beautement, A., Sasse, A. and Wonham, M. The compliance budget: managing security behaviour in organisations. In Proceedings of the 2008 workshop on New security paradigms (Lake Tahoe, California, USA, 2008). ACM.

[6] Bijker, W. E., Hughes, T. P. and Pinch, T. The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology. The MIT Press, 1987.

[7] Burrell, G. and Morgan, G. Sociological paradigms and organisational analysis: Elements of the sociology of corporate life. Heinemann, London, UK, 1979.

[8] Butler, W. L. Computer Security in the Real World. 2004.

[9] Callon, M. Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In Power, Action and Belief:A New Sociology of Knowledge Routledge, London, 1986.

[10] Callon, M., Law, J. and Rip, A. Glossary: Actor-network xvi Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World. Macmillan, Basingstoke, UK, 1986.

[11] Charmaz, K. Constructing Grounded Theory: A Practical Guide through Qualitative Analysis (Introducing Qualitative Methods series). Sage Publications Ltd, 2006.

[12] Clegg, S. Frameworks of Power. SAGE, London, UK, 1989.

[13] Clegg, S. and Wilson, F. Power, Technology and Flexibility in Organizations 223-273 A Sociology of Monsters: Essays on Power, Technology and Domination J. Law Routledge, London, 1991.

[14] Dahl, R. A. The concept of power. Syst. Res., Vol. 2, 3 (1957), 201-215.

[15] Davenport, S. and Leitch, S. Circuits of Power in Practice: Strategic Ambiguity as Delegation of Authority. Organization Studies, Vol. 26, 11 (November 1, 2005), 1603-1623.

[16] Drucker, P. F. Landmarks of Tomorrow. Heinemann, London, UK, 1959.

[17] Fléchais, I., Riegelsberger, J. and Sasse, M. A. Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In Proceedings of the 2005 workshop on New security paradigms (Lake Arrowhead, California, 2005). ACM.

[18] Flores, F., Graves, M., Hartfield, B. and Winograd, T. Computer systems and the design of organizational interaction. ACM Trans. Inf. Syst., Vol. 6, 2 (1988), 153-172.

[19] Foucault, M. Discipline and Punish: The Birth of the Prison. Penguin Books, London, UK, 1975/1977.

[20] Foucault, M. L'usage Des Plaisirs, Histoire De La Sexualite. Éditions Gallimard, Paris, France, 1984.

[21] Glaser, B. and Strauss, A. The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine Transaction, 1967.

[22] Herley, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the workshop on New security paradigms Oxford, United Kingdom, 2009). ACM.

[23] Introna, L. D. Management, Information and Power. Macmillan, Basingstoke, UK, 1997.

[24] Jasperson, S., Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J. P. and Zheng, W. Review: Power and Information Technology Research: A Metatriangulation Review. MIS Quarterly, Vol. 26, 4 (2002), 63.

[25] Jensen, M. C. and Meckling, W. H. Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, Vol. 3, 4 (1976), 305-360.

[26] Joinson, A. N., Reips, U.-D., Buchanan, T. and Schofield, C. B. P. Privacy, Trust, and Self-Disclosure Online. Human‚ÄìComputer Interaction, Vol. 25, 1 (2010), 1 - 24.

[27] Lapke, M. and Dhillon, G. Power Relationships in Information Systems Security Policy Formulation and Implementation. In European Conference on Information Systems (Galway, Ireland, 2008).

[28] Latour, B. Techology is society made durable 103-131 A Sociology of Monsters: Routledge, London, UK, 1991.

[29] Law, J. Power, discretion and strategy. A Sociology of Monsters Rutledge, London, UK, 1991.

[30] Lockwood, D. Social Integration and System Integration 244-257 Explorations in Social Change G. K. Zollschan and W. Hirsch Routledge & Kegan Paul, London, UK, 1964.

[31] Lukes, S. Power: A Radical View. Palgrave, Basingstoke, UK, 2005.

[32] Pallas, F. Information Security Inside Organizations: A Positive Model and Some Normative Arguments Based on New Institutional Economics. Technischen Universität Berlin, Germany, 2009. unpublished thesis

[33] Parkin, S., van Moorsel, A., Inglesant, P. and Sasse, A. A stealth approach to usable security: helping IT security managers to identify workable security solutions. In Proceedings of the workshop on New security paradigms (Concord, MA, USA, 2010).

[34] Riegelsberger, J., Sasse, M. A. and McCarthy, J. D. The mechanics of trust: A framework for research and design. International Journal of Human-Computer Studies, Vol. 62, 3 (2005), 381-422.

[35] Riegelsberger, J., Sasse, M. A. and McCarthy, J. D. The mechanics of trust: a framework for research and design. Int. J. Hum.-Comput. Stud., Vol. 62, 3 (2005), 381-422.

[36] Trist, E. L. and Bamforth, K. W. Some social and psychological consequences of the longwall method of coal-getting:. Human relations, Vol. 4, 1 (1951), 3.

[37] UK Department for Business Enterprise & Regulatory Reform Information Security: How to Write an Information Security Policy.

[38] Wikipedia: Information security.

[39] Winner, L. Do Artifacts have Politics? Daedalus: Modern Technology: Problem or Opportunity (Winter 1980), Vol. 109, 1 (1980), 121-136.