The Compliance Budget: Managing Security Behaviour in Organisations

Adam Beautement
University College London
Department of Computer Science
Malet Place, London. WC1E 6BT
+44 20 7679 7214
a.beautement@cs.ucl.ac.uk

M. Angela Sasse
University College London
Department of Computer Science
Malet Place, London. WC1E 6BT
+44 20 7679 7214
a.sasse@cs.ucl.ac.uk

Mike Wonham
Hewlett-Packard Labs
Filton Road, Stoke Gifford,
Bristol, BS34 8QZ
michael.wonham@hp.com

ABSTRACT
A significant number of security breaches result from employees' failure to comply with security policies. Many organizations have tried to change or influence security behaviour, but found it a major challenge. Drawing on previous research on usable security and economics of security, we propose a new approach to managing employee security behaviour. We conducted interviews with 17 employees from two major commercial organizations, asking why they do or don't comply with security policies. Our results show that key factors in the compliance decision are the actual and anticipated cost and benefits of compliance to the individual employee, and perceived cost and benefits to the organization. We present a new paradigm – the Compliance Budget - as a means of understanding how individuals perceive the costs and benefits of compliance with organisational security goals, and identify a range of approaches that security managers can use to influence employee's perceptions (which, in turn, influence security behaviour). The Compliance Budget should be understood and managed in the same way as any financial budget, as compliance directly affects, and can place a cap on, effectiveness of organisational security measures.

Categories and Subject Descriptors
H.1.2 [**Models and Principles**]: Human/Machine Systems – *human factors, human information processing.* C.2.0 [**Computer Communication Networks**] General –*security and protection*

General Terms
Management, Economics, Security, Human Factors.

Keywords
Security policies, security behaviour, Compliance Budget, compliance

NSPW'08, September 22–25, 2008, Lake Tahoe, California, USA.

1. INTRODUCTION
It is widely acknowledged in security research and practice that many security incidents are caused by human, rather than technical failures (e. g. Schneier 2000). Researchers approaching the issue from a Human-Computer Interaction (HCI) perspective – e. g. Whitten & Tygar (1999) – demonstrated that many human failures are caused by security mechanisms that are too difficult for a non-expert to use. Even users with good technical skills, such as systems administrators and software developers, often struggle to keep up with the increased complexity and workload created by security mechanisms (Zurko & Simon, 1996; Flechais et al. 2003). The primary goal of the flourishing research community focusing on usable security, known as HCIsec, is to provide security tools that the intended users can operate correctly [e.g. Yee 2005] and complete a security task – such as encrypting an email - effectively. Other key usability criteria established by the HCI research community – user satisfaction and user cost – have hitherto been addressed implicitly rather than explicitly in usable security research.

It is also often the case that user effort is a blind spot for those formulating and discussing security policies, and this work aims to address that issue. Adams & Sasse (1999), Weirich & Sasse (2001), and Weirich (2005) pointed out that to achieve effective security from an organisational point of view security designers and managers need to consider that:

1) Individual users have a choice on whether to comply with security policies, and

2) This choice is influenced by the individual's own goals, perceptions and attitudes, and norms which govern the individual's behaviour.

Throughout this paper, we assume that the context is one in which the employee has a choice. We recognize that in certain high-security contexts, user choice can be curtailed or removed entirely but will focus on the majority of organizations where security is not a top priority, and compliance cannot be constantly monitored and enforced. For the purposes of this paper we will define compliance as 'the act or process of conforming to or fulfilling official requirements.'

Recent evidence suggests that in these contexts, managing employees' security behaviour is still a major challenge. Johnson & Goetz (2007) cite Theresa Jones, a security manager at Dow Chemical:

"My biggest challenge is changing behavior. If I could change the behavior of our Dow workforce, then I would think I had solved the problem."

Changing behaviour is important, but needs to be accompanied by changes in the security tools and models used. How can this be done? Johnson & Goetz (2007) report that current attempts focus on placing more responsibility on line managers, in some cases even imposing financial penalties on them if an employee they are responsible for causes a security breach.

While we agree that economic reasoning may help to change employee behaviour, Weirich (2005) found that negative reinforcement - which would include financial sanctions for security transgressions– used in isolation, is as ineffective in changing security behaviour as they have been in changing behaviour most other areas of life. We propose 1) that understanding the economics of compliance from an individual's point of view provides a better basis for influencing individuals' security behaviour, and 2) that organisations should accept that compliance with security policies is a finite resource that needs to be carefully managed. We express this proposal in form of a new paradigm – the Compliance Budget. The results of the interview study presented in this paper show that individuals and organisations place different values on the cost and benefits of behaviours associated with security policies[1], and that an individual employee's choice - to comply, or not to comply – with a security policy is determined by the perceived costs and benefits of the security tasks needed to support the policy. The choice is not an entirely selfish one – individuals consider the cost and benefits to both the organisation and themselves – but:

1) The perception of cost and benefit is centered on the individual employee's immediate work context,

2) There is a limit to the amount of effort individuals are prepared to expend on compliance unless there is a perceived benefit to balance it,

3) Cost-benefit imbalances accumulate until the compliance limit is reached.

In the following section, we review previous research on 1) organisational approaches to managing security and compliance, 2) economic techniques can be applied to security and security spending, and 3) factors influencing individuals' security behaviour in organisational settings. Section 3 describes the empirical study we carried out to collect data on individual and organisational perceptions of cost and benefits of security measures. In section 4, we present the costs and benefit of security measures from individual employees' perspective. Section 5 presents the new paradigm derived from those results – the Compliance Budget – and discusses how this notion helps to gain a differentiated view of the overall cost of complying with a security policy. In section 6, we outline two ways in which the notion of a Compliance Budget can be applied to manage security behaviour:

1) Organizations should track compliance efforts required by different groups of employees, and ensure the limit is not exceeded. As with any other budget, this can be done by prioritising compliance on key security goals, and removing the need to comply with less important ones.

2) Organisations can influence individuals' perception of cost and benefit of security measures, e.g. through awareness and education, and improved risk communication,

2. BACKGROUND

In an increasingly tougher economic climate, organisations have to decide how to spend their resources most effectively to achieve their operational goals. While IT spending over the past few years has remained fairly flat, spending on IT security has increased by around 17% per year (Huang et al., 2007). But there is growing awareness among researchers in information security that the resources an organisation can spend on IT security are limited, and have to be targeted to protect the assets and processes that matter most to an organisation. Attention has also been paid to the most effective way of disbursing a limited security budget in the face of a variety of threats. Huang et al (2007), for instance, highlight the need to "*minimize security risks with limited resources for implementing security technologies and programs."*

To achieve this, there has been a growing trend in information security research to employ economic models and approaches to support decision-making regarding spending on corporate IT security. Gordon & Loeb [4] argue strongly for applying formal cost/benefit analysis techniques to the process of managing corporate IT security. There is an ongoing research effort to improve and refine the metrics that could be used in information security, e.g. Herath & Herath (2007).

But to achieve meaningful metrics, security needs to be seen in the context of the business it seeks to protect. To deliver effective IT security, one must not only understand the threats to an organisation, but how security fits into its business goals and processes. As Johnson & Goetz (2007) point out, the biggest challenge for security metrics is linking them to business in a meaningful way; for example, being able to state the cost to the business of a security incident in terms of revenue loss. Currently there are no tools for managing security behavior and modeling the impact of policy changes. This is something this paper begins to address.

Equally challenging is establishing a metric's validity and building metrics that change over time to incorporate changes in the organizational and risk environments while still allowing meaningful comparison to previous results. The losses incurred by a breach in confidentiality are very different from those resulting from an availability failure (Kumar et al., 2007) and so threats to availability and confidentiality need to be treated differently depending on the focus of the organisation. Security officers and corporate decision-makers therefore need to have a full range of information about the systems they are working with. By treating security spending as an economic exercise, it is possible to for organisational decision-makers and security

[1] 1. It is important to note that the compliance budget applies to all tasks that interrupt or create friction with the core business of the user. All such tasks will contribute to using up the compliance budget and moving the user towards the budget threshold. Security tasks are a significant and important subset of this larger range of tasks and are the main source of discussion for this particular paper.

specialists to develop a common framework and language for planning and designing an organisation's security policies.

Even though everyone understands that employees play a key part in any organisation's processes and performance, they do currently not feature in the attempts to model the cost and benefit of security measures. We argue that this needs to be changed: any reasoning about cost and benefit of security measures has to include the impact that those security measures have on individual employees. Effective security relies on employees complying with security policies, i.e. exhibiting the behaviours specified in the policies. Previous research on users and security (Adams & Sasse, 1999, Weirich & Sasse, 2001, Weirich 2005) has pointed out that - unless there is constant monitoring and enforcement - individual users have a choice on whether to comply with security policies, and that this choice is influenced by the individual's own goals, perceptions and attitudes. If the individual's goals, perceptions and attitudes are aligned with those of the organisation, then no conflict exists, and most individuals are likely to comply with the policies.

The aim of the study reported in this paper was to explore the relationship between individual security behaviour and organisational security when there is a conflict of interest, i.e. when the behaviour required by a security measure is not aligned with individual employees' goals. Employees focus on completing their primary (production) tasks, and the behaviour required by the security (enabling) tasks often presents an obstacle on the shortest path to the primary goal (Sasse et al. 2001). This misalignment introduces friction between security and business processes into the organizational system, and it is this friction that is at the heart of individual compliance issues.

We explore how economic techniques can be applied to effectively manage these conflict situations. The results from our study show that techniques of economic management and optimisation can be usefully applied to model this situation. There is a limit to the amount of effort individuals are prepared expend on security measures that do not obviously contribute to their key production tasks, and this extra non-productive effort required accumulates until a limit is reached. We have named this limit the *Compliance Budget.* There are two key benefits that can be obtained from understanding this effort:

1) Organisations can focus the effort available on key security tasks to maximize their return on investment and avoid wasteful expenditure on less critical measures.

2) It is possible to determine the cost of achieving an employees' compliance with a security measure, and to include this cost in models of cost and benefit of security measures.

3. THE STUDY

To obtain an empirical basis for our model, we conducted a study to elicit factors that contribute to corporate and individual security cost. One of the authors conducted 17 in-depth interviews with security staff, employees and managers in two major UK companies – a financial institution and the research lab of a technology company. The interviewees included the chief security officers in both companies, and 4 security researchers or operational security staff. The remaining 10 participants were staff working in the companies' main-line activities – financial services or technology research, and one of them was a lawyer. All participants had a university degree and at least two years' work experience.

The interviews were semi-structured, exploring

1) The tasks and responsibilities of interviewees,
2) Their perception of the risks facing the company,
3) Their attitudes to the company's security polices and security measures, and
4) The perceived impact of security measures on individual's tasks and responsibilities, and company productivity.

Whilst the interviews covered a range of security policies and measures, all interviewees were asked about their usage of one specific bit of technology - USB sticks- and their awareness of security policies surrounding the use of these policies. These sections of the interviews have been analysed in-depth and reported elsewhere (Pym et al. 2008). For this paper, we analysed the transcripts of the interviews in their entirety, and analyzed using techniques from Grounded Theory. Grounded Theory (Strauss & Corbin 1990) is a qualitative data analysis method widely used in social sciences, which allows identification of salient concepts and relationships between them. Over the past 10 years, the method has been successfully applied to model user perceptions and attitudes in Human-Computer Interaction in general. Adams & Sasse (1999) used this approach to identify factors that affect employees' perceptions of corporate security policies, and Weirich & Sasse (2001) modeled employee decision-making on compliance with password security policies. The interviews using axial coding (the first stage of Grounded Theory) to produce an inventory of the individual employee's costs and benefits associated with security policies and mechanisms they came in contact with, and the costs and benefits for the organization. Data were coded by two researchers independently.

4. RESULTS

The analysis of the interviews provided many examples of participants complying and not complying with security measures. The costs and benefits of security policies featured large in individuals' discussions of their security behaviour. This is not, however, a simple equation *compliance = cost to the individual, benefit to the organisation*, and *vice versa*. Rather, the actual costs and benefits are a complex web of perceived costs and benefits to the employee (both from a professional and individual point of view), and the perceived cost and benefit to the organisation. The individual employee's perception of cost and benefit is, however, largely determined by the impact of compliance on their tasks and responsibilities; the goal of their primary work task dominates their perspective whereas the security goals of the organization are subordinate. We identified a number of different scenarios in which individual cost/benefit decisions were traded off against compliance with security policies. These are described in detail in the following section.

4.1 Example Cost/Benefit Scenarios

In this section, we present 5 key scenarios illustrating individuals' cost/benefit perceptions of security measures. The quotes from the interviews illustrate the examples given.

4.1.1 Centrally scheduled maintenance tasks, such as weekly automated virus scan

Participants provided many examples of production tasks being disrupted by centrally scheduled maintenance tasks, such as virus checker updates, patches, and licence management software. The effect is either a complete interruption of the employee's production tasks, or their machines being slowed down to the point where they cannot work effectively:

P6: "when [the virus scanner] is turned on, our program takes an extra 20 minutes to build and test".

Most participants acknowledged that there was a purpose to those security measures. If they had the luxury of doing so, they would re-organise their work: *"go for a coffee",* and resume when the maintenance task was completed. All participants felt it was justified to circumvent these security measures if they interfered with their ability to deliver their work on time, especially when they were up against a deadline. A minority, however, was more militant, feeling that no interruption of their work was justified. Each participant seemed to evince some awareness of the tradeoff between personal and organizational good.

P3: "Anything that loses time is not good for the business."

Others were clearly resentful of the loss of control over their own machines, and their ability to complete their work being at the mercy of *"whatever they think of next",* especially if they could not perceive any benefit of those updates. In one of the organisations, several employees had permanently opted out of the updates:

P11: "next thing I know I'm installing some tiresome patch that I don't want to be installing... I used to circumvent that whenever I was in this building."

Employees did this either openly or covertly (some deliberately switched to an operating system or application software that was not centrally supported) - some with, some without knowledge of the security/IT managers. Most employees were aware that there must be organisational need for running these updates, and that their "opting out" would undermine this.

P16: "different IT groups all want to scan these machines so I don't think they are too happy about that."

The prevailing attitude, however, was that - whatever the organisational need for these measures - it did not justify *"stopping people from getting their work done",* and leaving several participants to wonder *"why they cannot run these things at night?"*This last example highlights a lack of awareness that there might also be conflicting goals at the organizational level, in this case the desire to reduce energy consumption by closing down all systems at night versus effective security.

4.1.2 Additional authentication

Several passwords need to be (re)entered, e.g. to connect to additional VPN's (Virtual Private Networks). At worst, failure to recall the correct password leads to failure to access (no availability), which in turn means inability to get work done.

P3: "The only [problem] I can think of is if either you lose a password or forget it."

Additional passwords increase cognitive load and worry about accurately recalling passwords.

P10: "there are a lot of systems that need a lot of passwords and you know keeping a track of them is a bit of a pain."

Additional authentication hurdles cause delay in accessing systems and cause frustration at having to repeat a task.

4.1.3 Using encryption for data storage/transfer

An example of this would be the mandatory use of encryption for all data stored on USB sticks. For some participants, the risk to availability of data they needed was the key concern, but many participants balanced this against the confidentiality risk to their organisation.

From the individual's perspective, the worst-case cost is permanent loss of data or lack of availability at a critical time for their tasks. The very possibility of losing access to data was an unacceptable cost to some participants.

P12: "I just feel a lack of control because most of the time the threat is unavailability created by the encryption system."

The fear of the risk to availability is deep, and several participants expressed a fundamental unwillingness to rely on a technology they did not understand.

P13: "I know very few people who run encrypted file systems on a laptop ... because they don't trust the file system. They want their data to be accessible."

In this context, data does not equal data – the fear is strongest for data that individuals have created or generated themselves; they felt strong ownership and resented this date being subject to a blanket company policy.

P10: "[USB encryption] would be irritating because much of the content is private."

Even if the data would not be permanently lost (e.g. because the file is still on the organisation's system) there a perceived risk to availability: not being able to access the data when it is needed. The result could be lost business opportunity, or embarrassment (looking incompetent).

P1: The only one I can think of would be the password on the device - I could forget it.

I: And what would be the result?

P1: I wouldn't be able to do my presentation. And that would be quite embarrassing.

The additional time to encrypt and decrypt data was a lesser perceived cost.

P10: "there is a cost to [USB encryption] in that it wastes my time."

These perceived costs made some participants feel entitled to break the policy.

P10: "if {USB encryption] was mandated I would probably work around it."

Others acknowledged the risk to the organisation, and the consequences that a breach of confidentiality would have.

P5: Well, for sure, a competitor could get hold of something and do something with it. The press could find out there was a breach and publicize that. And the client wouldn't be too happy.

It's just bad at all levels if confidentiality were breached. [If] there was any perception of wrongdoing it taints the firm's brand and the value of that is huge."

4.1.4 Restrictive Firewall

Firewall settings blocking access to a wide range of websites – from adult entertainment to social networking. In the worst case, participants reported that they could not get their work done, e.g. software developers could not access ports needed for running a virtual machine, and felt they had to break the policy.

P6: "the [company] firewall doesn't like those network ports being open. It lacks flexibility… By being too restrictive for my use they end up forcing people to cheat to disable things."

Other participants perceived the restrictions as more than an inconvenience – they felt it could damage business, and this, in turn would also affect their earnings:

P5: So how do you quantify that extra cost? … [it] can range from something as dramatic as business we won't win because we're not aware of information. And those fees [we miss out on] could be millions of dollars over 1 year or 2. You know, if a company went public that we just had no idea existed, because we couldn't see the webpage.

Participants felt they were being forced into workarounds, so they work effectively.

P4: "I think people don't try to not follow the rules just for fun. When we do it's for a reason."

4.1.5 Over-zealous security classifications

Participants from one organisation stated that all data and documents tended to be blanket-marked as *confidential.* They reported that this led to unintentional breaches of the security policy, e.g. when sharing data with colleagues outside the organisation, even though the sharing was clearly needed to get their work done.

P10: "there is a kind of blanket imposition of inappropriate security restraints, sometimes on documents."

Not being able to share data was seen as resulting in lower productivity and a loss of freedom of thought/expression.

4.2 Perceived Cost and Benefit

As Weirich (2005) points out, when an individual is presented with a security task, he has a choice of

1) Complying and performing the required behaviour (at least try to do so), or

2) Attempting to bypass the task.

The results from the analysis of our interviews suggests that the decision – to comply, or not to comply - is the result of an internal cost/benefit analysis, in which the individual weighs up the advantages and disadvantages of complying or not complying. This does not mean individuals regard compliance with security behaviour purely as a cost: the participants in our study value security, both for themselves and for the organisation they work for. The initial disposition is to comply with security policies - up to the point at which the perceived benefit of doing so is exceeded by the costs associated with complying. (Or the point at which anticipated cost of complying – i.e. worrying about forgetting a password, and the consequences of forgetting it – is perceived to be higher than the benefits of compliance.) Examples of costs perceived by individuals are:

1) *Increased physical load.* These are extra steps added to production tasks, increasing time and effort required to execute production tasks (such as a machine being slower because of security updates**)**, or new tasks added (such as additional authentication to enter building/log in to network, additional training to be completed for new security devices).
2) *Increased cognitive load* – additional information needs to be stored and recalled on demand (such as a password to encrypt/decrypt data). Research in psychology and human-computer interaction has established that human will try to avoid increased cognitive load even more than increased mental load (e.g. Norman, 1983).
3) *Embarrassment* – security measures impacting on business practises may cause the individual embarrassment (such as not being able to open an encrypted file for presentation to a customer or audience) in addition to the inability to complete the task. Individuals also anticipate that the perceptions formed as a result of such an event could have a potential long-term negative impact on their career..
4) *Missed opportunities* – the increased time required to go through the steps of a security task, or the restrictions placed on data access by a security policy may mean a worker in a competitive environment misses an opportunity to effectively do business e.g. websites relevant to a deal blocked by firewall rules. As with embarrassment (3), individuals are concerned about the cost of long-term impact on their career.
5) *The 'Hassle Factor'* – the perceived cost associated with complying is often higher than the actual cost, because of the knock-on effect on certain situational or contextual factors. For example, if an individual is under pressure to meet a deadline, waiting for a patch to install feels more onerous than if it happens over lunch or at a period of low activity.

At the same time, compliance with required security behaviour can have perceived certain benefits:

1) *Avoiding the consequences of a security breach.* The most obvious benefit is avoiding the consequences of a security breach – such as losing data – which would have a negative impact on the individual's task.
2) *Protection from sanctions* – there is no danger of being "caught" in breach of policy, and exposed to the sanctions stipulated by the organisation. Therefore the individual does not have to worry about being caught, or the sanctions. However, the degree of worry depends on the individual's risk appetite (see section 5), and the likelihood of sanctions being applied. Adams & Sasse (1999) and Weirich (2005) point out that if policies are routinely breached, but stipulated sanctions are not applied, individuals quite reasonably do no expect any consequences from being caught in breach of policies.

5. DISCUSSION: THE COMPLIANCE BUDGET, AND HOW TO MANAGE IT

Security policies and mechanisms will not be effective if individual employees choose not to comply. Most employees will comply if this does not require any additional effort. When extra effort is required, individuals will weigh this extra effort against benefits for them, in the context of their production tasks. If their goals are aligned with the organisation's security goals, there is no conflict, as the behaviour required of the individual translates into perceived gain for them as well as for the organsiation. Thus, security policies are likely to be followed – at least by most individuals, most of the time.

(Based on the results of Weirich (2005), there will be some exceptions to this rule, because 1) some individuals have a high propensity for risk-taking, or 2) some individuals may have other issues with the organisation, and contravene security policies as a way of expressing dissatisfaction or dissent.)

Conversely, most individuals will not be inclined to choose the behaviour required by the organisation if there is a conflict between the security behaviour and their own goals. In this case, either some part of the joint set of goals will not be met, or the individual will need to expend effort *without gain* to help the organisation's security goals.

Compliance is if the individual chooses the behaviour required by the organisation, even though it makes it harder for them to realise their goals, or even prevents them from reaching them altogether. Compliance can be seen as a kind of organisational altruism. From the individual's perspective, this is a situation of 'pain but no gain' (recall we are focusing on conflict situations where individual and organizational goals are unaligned). The 'pain tolerance' - the amount of extra effort an individual is prepared to make for no personal gain – is what we call the *Compliance Budget.* The limit of the Compliance Budget is referred to as the *compliance threshold*; this being the point at which the individual no longer has the will to comply with official requirements. The closer an individual is to his compliance threshold the higher the cost to the organisation of achieving compliance, as the perceived cost to the individual will also be higher. Once the compliance threshold has been exceeded, there will be almost no way to achieve compliance, except through heavy monitoring of individuals' behaviour, and enforcement.

When an individual is faced with a compliance decision, the costs detailed in the results section will be weighed up by the individual (consciously or subconsciously) and measured against the benefits. As stated before the issue of compliance only comes into question when the individual is placed in a situation where there is a cost to him but no direct benefit. The decision to comply or not comply with a single task can be summarized with a brief formula. It is worth mentioning at this point that the *hassle factor* is cumulative. If the task in question is the tenth that day, the individual has been expected to undertake they will see it as a far greater burden than the exact same task earlier in the day. This means that a steady erosion of the Compliance Budget will take place as tasks stack up, and the individual's tolerance for further tasks (or repetitions of the same task) will be reduced. This must be represented in the formula to take into account the cumulative affect of previous tasks already performed. We can express this decision as:

Compliance if (current task cost x *hassle factor*) + total cost of previous tasks < compliance threshold

In addition to the internal factors identified in section 4.2, there are external factors that impact an individual's compliance budget. External factors are created by the production task performed by the individual, and the organisatonal environment. It is factors in this second category that security managers can use to influence individuals perceptions of cost and benefits of compliance, and their security behaviour. Most of these measures are well known measures; the advantage of seeing them in the context of the Compliance Budget is that 1) these measures can be targeted more precisely to influence cost-benefit assessment, and 2) the impact of these measures on employee security behaviour can be understood and measured. The key external factors are:

1. *Design*. a) The most direct way to influence cost-benefit perception is to reduce the actual mental and physical workload that individuals have to expend on compliance. b) Well-designed security seeks to minimize friction between security and business processes, and avoids putting individuals in situations where they have to choose between security goals and production goals. Improving the design of the security system will reduce the cost of each security action, meaning more tasks can be undertaken within the same Compliance Budget.
2. *Awareness, Training, Education*. a) Effective training in using security measures can improve individual performance, which in turn reduces the cost associated with security measures. It can also build individuals' competence – which is a benefit to them, and their confidence – which can reduce the stress and anxiety associated with using security mechanisms. b) Raising awareness of the risks and vulnerabilities faced by the organization increases the perceived benefits of compliance. .
3. *The culture of the organization*. The more security-minded an organization is, the less friction compliance causes. Weirich & Sasse (2001) report that individuals' security behaviour is strongly influenced by behavioural norms – most individuals try to "fit in", rather than seek conflicts with their colleagues. Building a positive and strong security culture reduces friction and perceived cost of compliance
4. *Monitoring*. The visibility of the organisation's compliance monitoring, and willingness to administer advertised sanctions, will determine how likely it is an individual thinks they will be detected and reprimanded if they do not comply with policy. This will in turn feed into their decision to comply or not.
5. *Sanctions*. Avoidance of sanction is a perceived benefit. Thus, for sanctions to be effective, they must be enforced, and seen to be enforced (Sasse et al., 2001) used in response to a security failure will be factored in to the cost/benefit analysis of the individual. They influence the level of perceived benefit from the protection gained through compliance.

In general, each of the external factors affects either the total Compliance Budget, or the rate at which it is spent. This is an important distinction to make, as there is a finite improvement that can be made to the total Compliance Budget available through improving awareness, training and culture. Beyond this limit, further attempts will be counterproductive either in the business sense (time spent away from work) or in terms of the Compliance Budget (individual costs imposed through time taken up and attention demanded away from the individual's agenda). The implication here is that initial gains should be made through reducing the cost of each security task, and therefore slowing the rate of spending of the Compliance Budget. The most effective way to do this is to improve the design and integration of the security system.

The effect of the Compliance Budget and compliance threshold is to place a cap on the effectiveness of an organisation's security policy – the compliance limit. Once this threshold is reached, several outcomes can result, of varying significance. Firstly, adding in further security measures that require compliance from the 'overspent' individuals are unlikely to improve security, unless they are heavily monitored and enforced. In some cases not only will new measures have no effect, but existing security measures will be become significantly less effective as individuals lose patience even with security tasks they were previously willing to undertake.

6. CONCLUSIONS

The results of our empirical study allow us to draw four main conclusions. Firstly, an individual's Compliance Budget sets a cap on the effecitveness of security practices they are involved in. This is because - once the threshold is crossed - the individual will chose work-arounds motivated by his or her own needs, rather than the more altruistic process of compliance. Secondly, the closer an individual comes to crossing the compliance threshold, the higher the organisational cost of achieving compliance will be. This cost may come in the form of an increased need for monitoring and sanctions, and/or a passive cost in the form of increased stress and reduced goodwill. Thirdly, the organisaton can influence individuals' perception of where the threshold lies, through an understanding of the decision-making and feedback cycles associated with a compliance. Fourthly, the organisation can employ economic reasoning to ensure the available budget is used to achieve compliance in areas where it matters most. A possible outline for these cycles is presented as part of this conclusion.

Figure 1 illustrates the effect of the compliance threshold on the effort required to ensure continuing compliance. The closer an individual is to his or her compliance threshold, the higher the perceived cost of each task will be. This means that to ensure compliance, the organisation will have to expend more effort or resources in monitoring/sanctions etc. Once an individual is pushed passed his compliance threshold, it becomes very difficult to ensure compliance as the individual will be seeking ways to reduce the burden of compliance. The possible responses of the individual vary in severity and can be hard to predict, not least of all because the budget threshold is not a hard limit and reacts more elastically to pressure. For example individuals may be willing to accept exceeding the compliance threshold for a short term if provided with sufficient motivation (increased remuneration, promise of future perks etc).

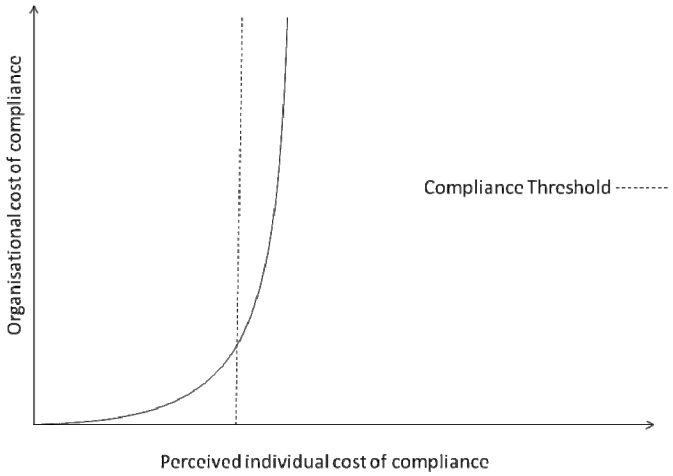

Figure 1: The effect of the compliance threshold on organisational effort required to achieve compliance. Effort rises as we approach the threshold and rises dramatically once it is crossed.

If the budget is exceeded for longer they may continue to undertake their current compliance tasks, but begin to look for ways to undermine or get back at the organization (this may be termed 'spiteful compliance'). In extreme cases, the individual will effectively cease to comply whenever possible, and focus on his or her own goals entirely. His or her last resort is, of course, to simply leave the organization.

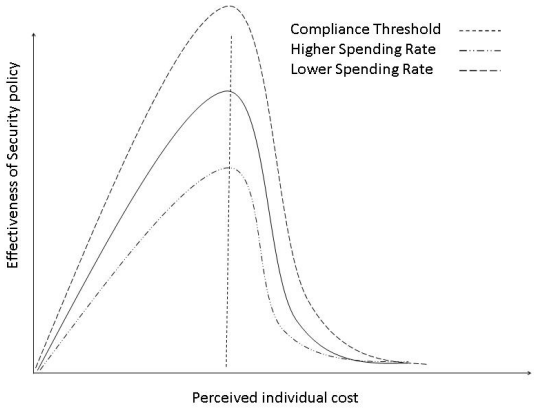

Figure 2: How perceived individual costs relate to effectiveness of security. Alternative rates of compliance expenditure are also shown for comparison. Once the compliance threshold is crossed security effectiveness drops sharply as altruistic behaviour is increasingly exchanged for selfish options.

In Figure 2, we can see how the effectiveness of the security system changes with the costs placed on the individual. It is important to recognise that it is *perceived* cost that is important. The individual is making decisions from a personal perspective, so it is the impression of the costs placed upon him that is relevant. Adding new security measures will place some burden on the individuals using or encountering them. This will

increase security in the organisation. However, as the compliance threshold approaches, the rate of gain of effectiveness starts to slow as the individual perceives a higher cost to each new task. Once we cross the threshold, the individual may choose to remove himself from the security process, at which point the effectiveness of the system drops dramatically. Now not only are new measures ineffective, but previously-performed tasks may be neglected. The level of effectiveness does not return to zero because in the course of normal business practise certain security measures will still be undertaken (such as using a password to log in to the network) even though no effort is being expended on security per se. Additionally we are now operating in the grey area discussed above, where individual responses to exceeding the budget are hard to predict. The innate flexibility and mobility of the budget limit itself also contributes to the uncertainty.

The initial gradient of the lines indicates how fast the security budget is being spent in each scenario. The more each task costs, the faster the budget is used up and the lower the gradient of the line. If each task costs relatively less we spend the budget slower and the gradient of the line increases. We can achieve better security behaviour, and a better return on security, for the same level of effort. By changing the rate of spending (for example by reducing the cost of each task through better system design), it is possible to alter the how effective it is possible to make the security of the system before this breakdown takes place. This is illustrated by the 'lower spending rate' line in figure 2. When compared to the 'normal spending rate' we can see that this line ascends more rapidly, reaching a higher level of effective security before reaching the budget threshold.

Spending the budget at a faster rate for example by implementing security tasks that conflict with the business process leads to a lower maximum level of security (we are able to implement fewer security policies before the threshold is reached) as shown by the 'faster spending rate' line. In this scenario security measures are more costly to the user and so at the point that the compliance budget threshold is reached effective security is below that of the other more efficient spending rates.

So how is the Compliance Budget set, and how can the rate of expenditure be influenced? In answering these questions we must be aware that these are not set values. They exist in a dynamic situation, and are subject to constant change and revision. The results of previous compliance decisions and the organisational environment all contribute to the maintenance and expenditure rates of the Compliance Budget. This is illustrated in figures 3 and 4.

Here we can see how the organisational environment impacts on the cost/benefit analysis performed by the individual. Improving system design, and creating a positive security culture, will simultaneously decrease the perceived cost of security tasks, and lower the rate of expenditure of the Compliance Budget. On the other hand increasing sanctions and monitoring will give more weight to the benefits associated with compliance. Both sides of this cycle make a positive compliance decision more likely.

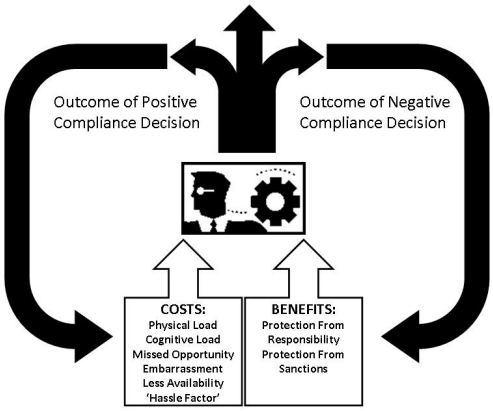

Figure 3: Feedback cycle for the individual. Positive compliance decisions increase the weight given to individual costs. Negative compliance decisions increase the weight given to individual benefits.

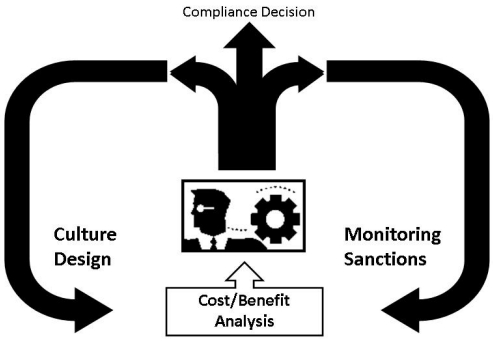

Figure 4: How organisational factors can be used to increase the likelihood of compliance. Improving system design and creating a security culture decrease the perceived cost of compliance. Harsher sanctions and monitoring increase the perceived benefits of compliance.

7. FUTURE WORK

The aim of this paper was to identify a way of understanding and influencing individual employees' security behaviour. Based on the results from an empirical study on the perceived cost and benefit of security measures, we concluded that the effort individuals are willing to make to comply with security policies is limited, and an organization can influence security behaviour by managing the Compliance Budget effectively. However, this is only part of the story. The next phase of our research will look at possible techniques and methods for achieving real-world change based on our insights. The model was derived from subjective data – employees recounting their security behaviour. Such recollections may be incomplete and biased, and need to be validated against objective data of actual security behaviour.

We also need to explore how relevant established theories of human behaviour in the face of risk – principally Adams' (1995) Risk Thermostat - can be integrated with our new paradigm. Adams' model suggests that an individual's propensity to take risks will be influenced by the rewards experienced by risk-taking. In our model, we have indicated that non-compliance will trigger a heightened awareness of the possible sanctions resulting from non-compliance. However, if these sanctions do not arrive (the individual's lack of compliance is not detected) then Adams' risk thermostat will take over and the rewards from non-compliance (increased working flexibility, data availability and spare time) will reinforce this behaviour. This indicates that the window for affecting compliance decisions through sanctions and monitoring may be small. We intend to explore these behaviours and their consequences through our work.

In this paper, we talk exclusively about either the individual or the organisation, but these are not the only participants considered in a decision making process. Weirich & Sasse (2001) identified the influence of colleagues' security behaviour, so the way how they respond to compliance or non-compliance needs to be taken into account.

We anticipate that our research will lead to the development of a software-based compliance management tool. This tool would be intended for use by information security managers and policy designers. Appendix 2 shows a mock-up of an interface for such a tool.

The core function of this tool is to track the effort burden placed on various groups or individuals by the security tasks they are required to undertake. The interface would then allow managers to view this information in several ways.

1) They can select a security task and see which individuals, or groups of employees, are being asked to perform this task. The selected task would appear in the centre left window, showing the cost associated with that task, how often it is performed, and the groups assigned to or excepted from the task. Selecting a group or individual from this window will bring up their details in the centre right window.

2) Selecting a group or individual will bring up their details in the centre left window. Their current and threshold costs will be displayed, along with their current burden, as a percentage. Additionally all tasks associated with this group will be shown below. These can be selected, thus showing their individual details in the centre right window. This is the type of view displayed in the figure.

Below these two windows a timeline will be shown showing the burden on a the selected group over the current time period (chosen from day, week, month, year at the top of the window). If a task is selected this timeline will show how many groups are performing the task at different times. This timeline allows points of dangerous friction to be quickly identified.

3) To the left of the interface are the overview and critical item panels. The overview panel allows the user to browse through all tasks and groups through an expandable menu system. The critical items panel alerts the user to groups that are operating over their threshold, or tasks that are involved in pushing a group over their threshold. It is anticipated that setting the conditions for an item to appear in the critical panel will be part of the functionality of the tool.

4) This tool would allow managers to plan changes in security policy or employee structure and see in advance where hotspots of high friction would be created or removed. Reducing the friction between business and security is beneficial for both processes and this tool could play a major role in achieving that objective. However, we need data to allow us to set up the thresholds and cost values in the software. Without this data, or with only poor approximations thereof, this tool would be useless, and possibly even damaging if it leads to poor decision making. Providing accurate and usable data to support the core function of this tool would be the major contribution of our research.

In summary, we have laid down the seed for a new way of looking at compliance decision making and its affect on security. Although the long term aim of the research is to underpin the creation of a software management tool the real-world implications of this result, and the nature of its interactions with existing techniques and methods must first be more fully evaluated.

8. ACKNOWLEDGEMENTS

The authors would like to thank colleagues on the Trust Economics project (funded by the UK Technology Strategy Board) for granting access and recruiting the staff who participated in interviews: Robert Coles at Merrill Lynch London, and David Pym and Michael Wonham at HP Labs Bristol. Sincere thanks are due to all interviewees for their time and willingness to discuss their security behaviour and decision-making so openly.

9. REFERENCES

[1] J. Adams (1995) Risk. Routledge.

[2] A. Adams & M. A. Sasse (1999): Users Are Not The Enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of the ACM, 42 (12), pp. 40-46* December 1999.

[3] I. Flechais, M. A. Sasse, & S. M. V. Hailes. Bringing security home: A process for developing secure and usable systems. In *ACM/SIGSAC New Security Paradigms Workshop*, 2003.

[4] Steven J. Greenwald, Kenneth G. Olthoff, Victor Raskin, Willibald Ruch (2004): The User Non-Acceptance Paradigm: INFOSEC's Dirsy Little Secret. *Proceedings of the New Security Paradigms Workshop.* 2004.

[5] Lawrence A. Gordon & Martin P. Loeb (2006): Managing Cybersecurity Resources: A Cost-Benefit Analysis. *Mcgraw-Hill*.

[6] Hemantha S. B. Herath & Tehaswini C. Herath (2007): Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management*. Proceedings of the Sixth Workshop on the Economics of Information Security,* Carnegie Mellon University*,* June 7-8, 2007.

[7] C. Derrick Huang, Qing Hu & Ravi S. Behara (2006): Economics of Information Security Investment in the Case of Simultaneous Attacks. *Proceedings of the Fifth Workshop on the Economics of Information Security,* Cambridge University*,* June 26-28, 2006.

[8] M. Eric Johnson & Eric Goetz (2007): Embedding Information Security into the Organisation. *IEEE Security & Privacy* May/June 2007 pp 16 – 24.

[9] M. Eric Johnson & Scott Dynes (2007): Inadvertent Disclosure – Information Leaks in Extended Enterprise. *Proceedings of the Sixth Workshop on the Economics of Information Security,* Carnegie Mellon University, June 7-8, 2007.

[10] Vincent Kumar, Rahul Telang & Tridas Mukhopahhyay (2007): Optimally securing interconnected information systems and assets. *Proceedings of the Sixth Workshop on the Economics of Information Security,* Carnegie Mellon University, June 7-8, 2007.

[11] Norman, D. A. (1983): Some Observations on Mental Models. In Gentner, D. A. & Stevens, A. A. [Eds.] *Mental models*. Hillsdale, NJ: Erlbaum.

[12] B. Schneier (2000): Secrets and Lies: Digital Security in a Networked World. *Wiley*.

[13] Strauss, A. and Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. *Sage Publications.*

[14] D.Weirich & M. A. Sasse (2001): Pretty Good Persuasion: A first step towards effective password security for the Real World. *Proceedings of the New Security Paradigms Workshop* 2001 (Sept. 10-13, Cloudcroft, NM), pp. 137-143. ACM Press.

[15] Weirich (2005): Persuasive Password Security. Unpublished *PhD Thesis, Department of Computer Science, University College London, UK.*

[16] Whitten, A. & Tygar, J. D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium,* August 1999, Washington 1999.

[17] Yee, K P. (2005) User Interaction Design for Secure Systems. In L. Faith Cranor & S. Garfinkel [Eds.]: *Security and Usability: Designing secure systems that people can use* 2005. pp 13-30. O'Reilly Books.

[18] Zurko, M. E. & Simon, R. T. User-Centered Security. *New Security Paradigms Workshop* 1997.

APPENDIX 1: TABLE OF COSTS AND BENEFITS ASSOCIATED WITH COMPLIANCE FROM THE INDIVIDUALS PERSPECTIVE

Security Task/Policy	**Individual Costs of Compliance**	**Individual Benefits of Compliance**	**Organisational Costs** (as perceived by the individual)	**Organisational Benefits** (as perceived by the individual)
1. Centrally scheduled maintenance task. e.g. weekly automated virus scan.	Individual's intended task disrupted by the maintenance procedure. A time penalty is incurred. Workstation will also be slowed/blocked preventing other (possibly critical) tasks being completed in time.	Protection of individual's workstation/personal computer increased in case of virus outbreak. Less chance to have work compromised/destroyed/stolen. No risk of sanctions or responsibility for wider failure.	Reduced productivity of workforce thus impacting revenue.	Organisational security improved.
2. Additional authentication. e.g. re-entering passwords to connect to additional VPN's.	Delay in accessing the required systems. Increased cognitive load to recall password accurately. Frustration at having to repeat a task.	Access to systems necessary for business process. No risk of sanctions or responsibility for wider failure.	Slower business process reducing workforce effectiveness.	Organisational systems blocked to unauthorised individuals.
3. Using encryption for data storage/transfer. e.g. mandated use of encrypted USB sticks.	Additional time to copy data due to encryption/un-encryption. Possible loss of availability of data.	No risk of sanctions or responsibility for wider failure.	Longer time required to transfer data meaning a less dynamic and mobile workforce. Potential data loss.	No danger of humiliating data leak in the case of lost or stolen USB devices.
4. Restrictive firewall. e.g. ports needed for running virtual machines for software development blocked.	Working practices need to be changed. Certain tasks may no longer be possible. Individual may feel forced into using a workaround to continue to work effectively. Loss of productivity.	Individual is protected from unauthorised traffic. No risk of sanctions or responsibility for wider failure.	Security compromised to facilitate necessary business process, or business tasks unable to be completed. Possible legal consequence of loss.	Organisation infrastructure more secure in the face of various common threats.
5. Limitations on working practises. e.g. data blanket marked as confidential.	Unintended breaches of policy while collaborating with colleagues. Reduced exchange of information with partners. Lower productivity and freedom of thought/expression.	Lower risk of loss of intellectual property, legal recourse in case of data theft, No risk of sanctions or responsibility for wider failure.	Loss of collaboration and exchange opportunities. Reduced goodwill and reputation amongst colleagues and partners.	Organisation's intellectual property protected.

APPENDIX 2: MOCKUP OF THE USER INTERFACE OF A COMPLIANCE MANAGEMENT TOOL.