The Compliance Budget: The Economics of User Effort in Information Security

A. Beautement & M. A. Sasse

1. Introduction

A significant number of security breaches result from employees' failure to comply with security policies. The cause may be an honest mistake – e.g. when an employee enters their password in a phishing website, believing it to be a legitimate one (Dhamija et al., 2007), or because they are faced with an impossible task – e.g. when an employee has so many different passwords that she has to write them down (Adams & Sasse, 1999).

But there is also evidence that in some cases, employees may *chose* not to make the effort required to comply with manageable security tasks (Weirich, 2005). When asked for reasons for not complying, most respondents justify this with the impact of security measures on personal and company productivity, the perceived absence of risks, and that most of their fellow employees do not comply, either (Weirich, 2005, Beautement et al., 2008).

Many organizations would like to change employees' behaviour to achieve higher levels of compliance with their information security policies. Johnson & Goetz (2007) report a security manager of a major international company saying:

"My biggest challenge is changing behavior. If I could change the behavior of our […] workforce, then I think I've solved the problem."

The problem is that changing established behaviour in organisations is a notoriously difficult task. Security policies often threaten employees with sanctions if policies are not followed. Johnson & Goetz (2007) report that some organisations have tried to change employee behaviour by placing more responsibility for security compliance on line managers by applying financial penalties if one of their subordinates causes a security breach. This approach may have the benefit of adding a personal dimension to an individual employee's decision-making. But like all forms of negative reinforcement, sanctions are only be effective in shaping behaviour when applied consistently whenever the policy is not followed. However, unless non-compliance results in a security breach, it is hard to detect (Vroom and von Solms, 2004), and more often than not goes unpunished.

To detect and punish non-compliance consistently – taking an approach that could be characterised as '*comply-or-die*' - an organisation would have to expend significant resources on monitoring and enforcement of policies. This is, arguably, not a suitable way to run security in commercial organisations:

"Security […] is a means to an end and not an end in itself. For example, in a private- sector business, having good security is usually secondary to the need to make a profit. Security, then, ought to increase the firm's ability to make a profit."

An Introduction to Computer Security (NIST Special publication 800-12)

This raises the question of whether it is possible to increase compliance without taking the expensive *'comply-or-die'* approach. A study which elicited and analysed employees' reasons for not complying with security policies found that decisions were largely based on individual's assessment of the cost and benefit involved in complying with a security policy (Beautement et al. 2008) . The *cost-benefit decisions* they described were idiosyncratic (centred on the nature of their work), but not entirely selfish: when participants were aware of the specific risk that the policy was mitigating, they were more likely to comply. When they decided not to comply, participants justified this in terms of the negative impact of security policies on organisational productivity (e.g. a lost sale because they could not access the system and produce a quote in time) as often as to the impact they had on them (e.g. the difficulty to recall passwords). Employees weighed the *perceived need* for a specific security policy against the *perceived effort* required to comply with it. Since these decisions influence compliance behaviour, we decided to explore whether and how these decisions can be influenced by security managers. It turns out that established economic theories on consumer choice offer relevant insights.

2. Economics

According to microeconomic utility theory, a person[1] makes purchasing decisions based on available resources and preferences for the goods on offer with the aim of maximising their utility; utility being a measure of that person's satisfaction with the ownership or consumption of those goods. As the price and availability of goods changes, so does the person's purchasing strategy:
Person X might normally prefer item A to item B. But - if she finds she can purchase 10 item Bs for the same price as 5 item A - she may decide to buy item B, because she perceives the value of 10 B's to be higher than that of 5 A's. The point at which the person perceives the ratio of A and B to be equivalent is the point at which she is *indifferent* which of the two options she gets (say, given a choice is between 5 item A's and 7 item B's, she has no preference). Using these perceived values, it is possible to plot an *indifference curve* which shows the points at which people will trade-off between A and B with no loss of utility (see Figure 1).

[1] According to economic theory, the decision-marking organisations as well as individuals – we are using an individual person here to illustrate the point.

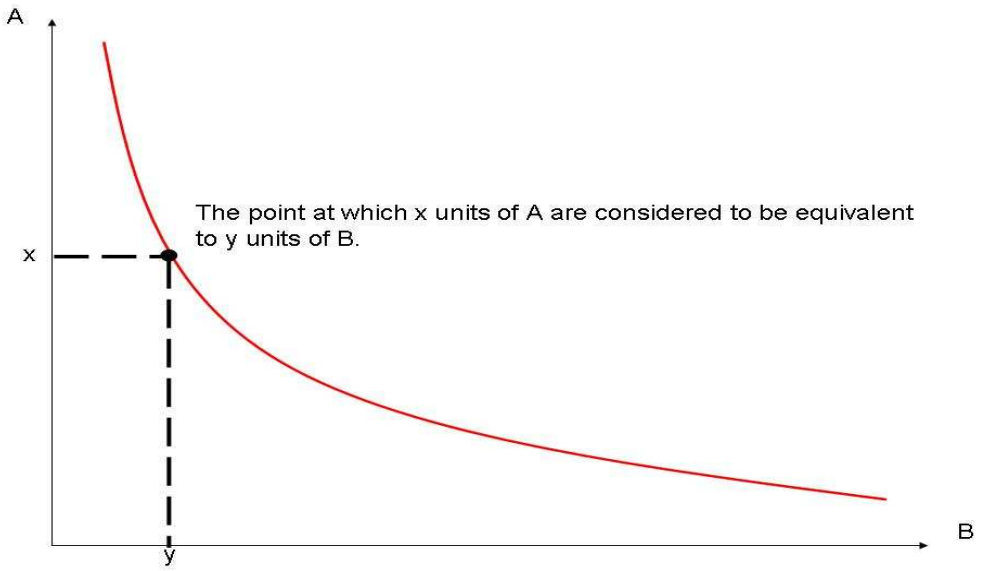

Figure 1: An example indifference curve showing the rate at which two goods, A and B, can be traded off without preference.

It is, however, important to recognise most people do not make a rational choice: this would require that a complete - or near complete - overview of the decision context (i.e. all available options, and the full short- and long-term consequences of choosing that option). Thaler & Sunstein, (2008) provide an excellent summary of decision making by real people (*humans)*, vs. the rational choices made by the rational actors assumed in economic theories (*econs*). In our interview data, we saw that a similar process applies when employees decide whether to comply with a security policy: our participants considered a limited set of subjective factors when deciding whether to comply, and described the choice between complying and not complying as being driven by the anticipated consequences of each option. Following security policies usually requires employees to expend some effort; and usually, the perception of that effort exceeds the perceived benefits they derive from the effort. Conversely, not following security policies usually means less effort for the individual, but may create risks for the organisation (vulnerabilities) and the individual (being caught and punished). The indifference curve represents the point at which the perceived cost/benefit ratio of following security policies and not following them are equally balanced; when the perceived cost-benefit outcome of following the policy clearly exceeds the cost-benefit outcome of not doing so, employees have to make a *compliance effort*. Every time compliance effort is required, the amount is noted implicitly by the individual, and it will accumulate over time. The key insight from our study was that the amount of compliance effort employees are willing to expend is finite - this is what we call the *compliance budget*. As this begins to run out an employee may see more utility in completing tasks more directly relevant to them rather and begin to trade these off with security tasks.

The employee's perception of different costs and benefits, and the environment in which they are making their compliance decisions will change over time. Short-term changes - including emergencies and deadlines - affect the compliance threshold of an

individual employee. An employee under pressure from a deadline may be more willing to take risks. Being asked to make an effort during unpressured stretches of a working day may not be seen as a problem, but being asked to complete the same task at the end of a long working day will make it seem far more onerous.

The exact amount of effort employees spend varies between both employees and organisations – some employees are inherently more inclined to follow policies, and in some sectors employees accept the need to manage risks more than in others – but we propose that for all individuals, there is a limit to the extra effort they will expend over a given time period on a secondary task such as security. The closer an employee is to their compliance threshold, the more burdensome additional tasks will appear subjectively. Organisations can exceed the budget occasionally without triggering a dramatic response. However, employees who are "over the limit" will be less likely to comply when further effort is required... It is therefore important to manage tasks in such a way that the perceived effort does not routinely exceed this limit. In the long term, keeping employees "over the limit" will lead to a negatively charged relationship between the individual and the organisation, and this will make employees with marketable skills more likely to leave, and breed resentment in those who stay behind. Both consequences affect the organisation's bottom line; the latter also creates new security risk because disgruntlement is the prime motivating factor in reported cases of IT sabotage (Capelli 2009).

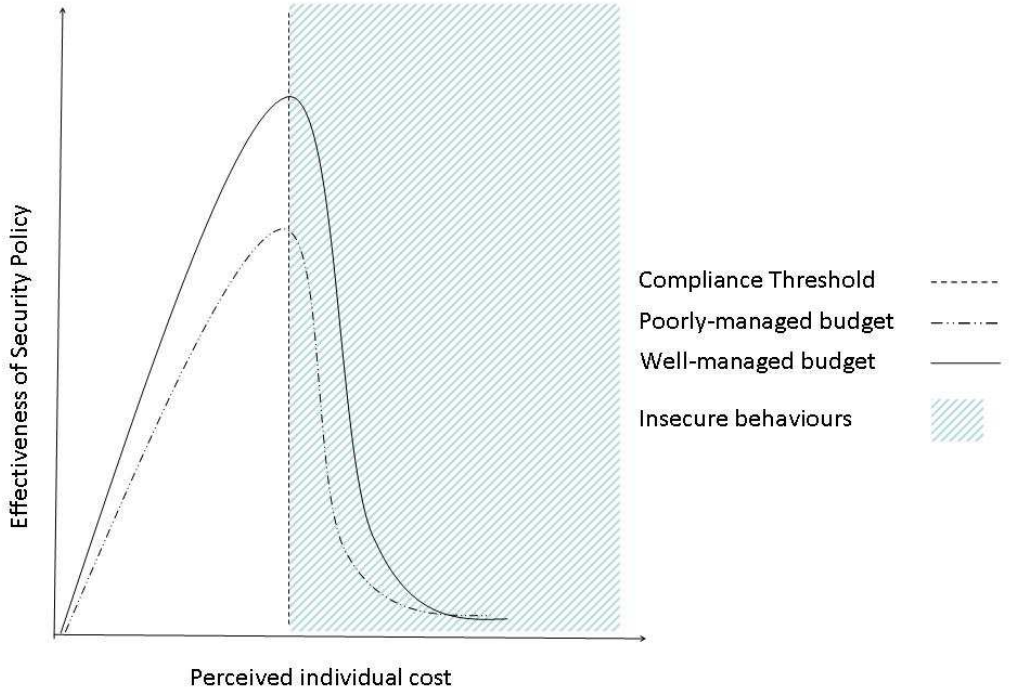

Figure 2: How perceived individual costs relate to effectiveness of security. Alternative rates of compliance expenditure are also shown for comparison. Once the compliance threshold is crossed security effectiveness drops sharply as the employee

elects to complete tasks that benefit him more directly as an individual rather than security tasks that more benefit the organisation as a whole.

While the precise shape of the graph in figure 2 cannot be plotted with total accuracy, and will show variations from individual to individual the same core features will occur. As the figure 2 illustrates, a well-managed budget will spend perceived effort at a slower rate. This means that more security policies can be accommodated before the compliance threshold is reached, resulting in a higher effective security level. Once the limit is exceeded, security policies are less likely to be followed, and effective security will start to decline. In the worst case, the organisation will lost its most valuable employees, and breed disgruntled staff, thus creating additional security risks.

Based on our observations, we propose that the best way of achieving compliance is to accept that extra effort employees will make to comply with security policies is a limited resource, and that - like any another limited resource - it needs to be budgeted and managed correctly. The principles of the compliance budget can be summarised as follows:

1. There is a limit to the amount of perceived effort an employee will expend on security tasks.
2. This means that any individual security policy associated with significantly more perceived cost benefits is likely to be followed.
3. When employees expend compliance effort, it accumulates over time, and once an employee's compliance limit is reached, she is less likely to follow any security police with compliance effort.
4. The rate at which the budget is spent matters: the more rapidly they approach their limit, the less likely they are to comply.

3. Managing the Compliance Budget

Understanding the implications of the compliance budget will benefit an organisation because it will a) reduce friction between individuals and the organisation, and b) increase security compliance. And we suggest that it will c) lead to a better integration of security into the organisation's primary business processes, realising the ambition that security should to increase the ability of the organisation to make a profit. NIST reference [ref no.] In this section, we provide some examples of how an organisation can work towards this ideal using the compliance budget principles.

Step 1: Auditing security effort

Getting to grips with the compliance budget requires establishing the actual and perceived workload associated with security policies that employees have to follow. In most organisations today, the workload associated with security policies is "pushed down" towards individual employees, with little though of whether the effort is manageable, or how disruptive it is to the employee's primary tasks (Sasse et al., 2001). Security managers should know how many security policies any group of employees has to deal with, and how much effort each group has to expend on complying with them. They also need to collaborate with business owners and line

managers to determine the impact on individual and organisational productivity, and where the threshold of acceptability lies.

Step 2: Considering the overall cost and benefit of security policies

In a recent case study, we compared the password policies of two large financial organisations. Policy 1 required shorter but more complex passwords, while Policy 2 required longer, but less complex passwords. Our analysis of these passwords using the compliance budget theory showed that the users of Policy 1 passwords required longer times to on average to enter their passwords. They also had a longer learning period – i.e. it took them longer to reach error-free performance. And when we compared the reset rates for these two passwords (requested resets per use for forgotten passwords) we found that the policy 1 passwords were being renewed more than twice as often as the policy 2 passwords.

This increased volume of resets indicates that the password is not being used frequently enough to cope with the cognitive burden and longer learning period that the password policy dictates. Our research also indicates that password length places less of a burden on users than password complexity (represented by the range of non-lower case letters in the password). In this case, trading complexity for length to maintain security but reducing the burden on its users (which is in line with Step 1). In line with Step 2, choosing Policy 2 reduces the operational cost for the organisation and increases productivity. By using compliance budget security managers can identify security policies that provide the required level of risk mitigation at the lowest cost to individuals and the organisation.

Step 3: Influencing the Compliance Threshold

Security managers can raise the compliance threshold by communicating the risks the organisation faces, and making clear links between those risks, and the behaviour that security policies require. This will increase the perceived benefits of policies that require a significant compliance effort, but are genuinely necessary to manage organisational risks.

Step 4: Why less friction means better overall risk mitigation

An employee pushed over their compliance threshold increases the risk to an organisation in two ways. As discussed in section 2, once an individual is working at or over their compliance limit they will begin to adopt insecure behaviours. Typically, these will result in neglecting or bypassing onerous security procedures, creating potential vulnerabilities in the security system which might be exploited by external attackers. For instance, in an organisation where most employees have problems recalling their password, a social engineering attacker claiming to be a fellow employee who has locked himself out of the systems has a high chance of success. In the long term, we would argue that it is likely to increases the risk of insider attacks to two ways. Recent research on insider attacks (Richardson, 2003) has shown that the approximately 80% of organisations see their own workers as a likely source of attack, and an increase in vulnerabilities means more opportunities for exploitation by

internal attackers. For instance, if employees write their passwords onto post-its and whiteboards, they make it easier for a fellow employee to misuse their access.

An employee forced to work over their compliance budget will also build up resentment towards the parent organisation, which is likely to result in disgruntlement. Capelli at al. (2009) have shown that disgruntlement is the starting point for many employees who end up attacking their own organisation's system.

Based on their findings, the CERT researchers say that correct management has to *"pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment. It must look beyond information technology to the organization's overall business processes and the interplay between those processes and the technologies used."* (Capelli et al., 2009).

4. Conclusions

We argue that applying the principles of the compliance budget to manage human effort in security adds a dimension to security management. Tracking user effort is important and effective in both maintaining security and reducing friction between employees and organisations, and between business and security processes in an organisation.

There is an important principle at the core of our discussion between security effectiveness and user effort. It is often suggested that there is a trade-off between usability and security – that reducing employees' security effort means reducing the level of security, and conversely, that it is legitimate to increase employee's effort because security is important. We argue that the trade-off in this form is overly simplistic and misleading. As we have argued in section 3, placing too much burden on employees will creates new risks for an organisation's security. The trade-off exists only for a limited range, and there is an optimal operating point - somewhere close to, but below the compliance threshold. This is illustrated in Figure 3.

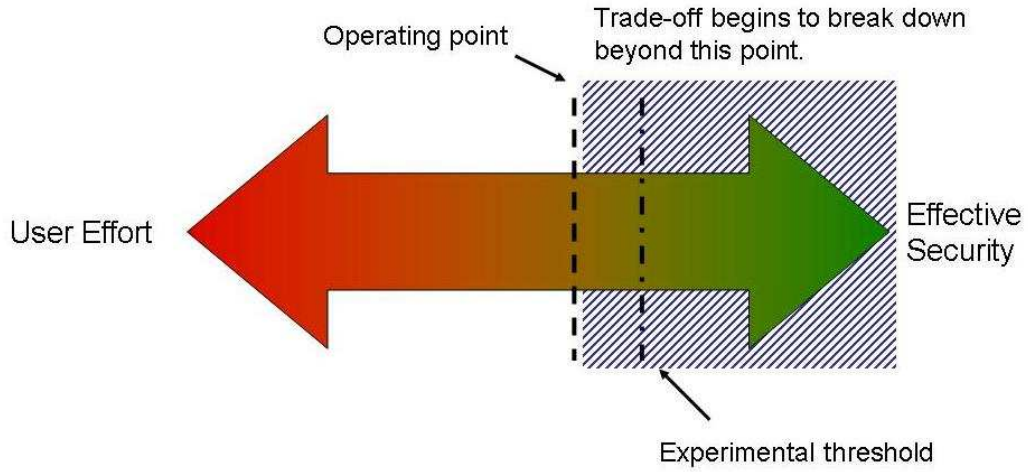

Figure 3: How user effort and effective security trade off against each other. This is not a pure trade-off: the striped region as illustrates the area where attempting to increase user effort results in insecure behaviours rather than higher security.

It is possible to move a security system closer to this operating point, through effective decision-making and manipulation of the context in which security policies are used. This point is not just optimal in terms of delivering security, but also optimal in an economic sense, because for it represents the best return financial resources and human effort expended on security. Beyond this point, either

1. the security policies are not followed, opening up vulnerabilities, or
2. significant resources are needed to
    a. monitor the employee behaviour and enforce sanctions, and
    b. deal with the problems of employees who cannot cope.

If the system is operating below this point, there is room for improvement, and security measures are not operating at their full capacity. This approach goes hand in hand with the notion that security should support the primary business process not unnecessarily interfere with it. Managing the compliance budget effectively then becomes a primarily financial decision driven by the needs of the organisation as a whole, rather than a niche method of generating more security for its own sake.

5. References

1. 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.

2. A. Beautement, R. Coles, J. Griffin , B. Monahan, D. Pym, M. A. Sasse, M. Wonham (2008). Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. *Workshop on Economics in Information Security 2008*. 25-28 June, 2008, Hanover, New Hampshire, USA.

3. A. Beautement, M. A. Sasse, M. Wonham (2008). The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms.*

4. R. Dhamija, J.D. Tygar and M. Hearst (2006). Why Phishing Works. *Proceedings of the 2006 SIGCHI Conference on Human Factors in Computing Systems.* Montreal, Canada, April 24 – 27 2006.

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

6. National Institute of Standards and Technology (1995). *An Introduction to Computer Security: The NIST Handbook.* (Special Publication 800-12).

7. R. Richardson (2003*). Eighth Annual CSI/FBI Computer Crime and Security Survey,* Computer Security Institute.

8. M. A. Sasse, S.Brostoff, and D. Weirich (2001): Transforming the "weakest link": a human-computer interaction approach to usable and effective security. BT *Technology Journal, Vol 19 (3), pp. 122-131* July 2001.
9. R. H. Thaler and C.R. Sunstein (2008). Nudge. *Penguin Books.*

10. C. Vroom and R. von Solms (2004) Towards information security behavioural compliance. *Computers & SecurityVolume 23, Issue 3, Pages 191-198,* May 2004.

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