"Comply or Die" Is Dead:

Long live security-aware principal agents

Iacovos Kirlappos, Adam Beautement and M. Angela Sasse
University College London, Department of Computer Science,
London, United Kingdom
{i.kirlappos,a.beautement,a.sasse}@cs.ucl.ac.uk

Abstract. Information security has adapted to the modern collaborative organisational nature, and abandoned "command-and-control" approaches of the past. But when it comes to managing employee's information security behaviour, many organisations still use policies proscribing behaviour and sanctioning non-compliance. Whilst many organisations are aware that this "comply or die" approach does not work for modern enterprises where employees collaborate, share, and show initiative, they do not have an alternative approach to fostering secure behaviour. We present an interview analysis of 126 employees' reasons for not complying with organisational policies, identifying the perceived conflict of security with productive activities as the key driver for non-compliance and confirm the results using a survey of 1256 employees. We conclude that effective problem detection and security measure adaptation needs to be de-centralised - employees are the principal agents who must decide how to implement security in specific contexts. But this requires a higher level of security awareness and skills than most employees currently have. Any campaign aimed at security behaviour needs to transform employee's perception of their role in security, transforming them to security-aware principal agents.

Keywords: Information security management, compliance, decision-making

1 The need for Information Security

Organisations today face an ever-increasing number of information security threats: intellectual property theft can severely impact competitiveness, loss of customer information can damage corporate profiles and loss of access to corporate systems can impact the organisation's productivity [1]. Despite the significant amount of time being invested in producing effective security solutions by researchers and industry experts, the challenges and potential threats organisations face today are higher than ever [1].

After implementing technical controls strong enough to minimise an organisation's exposure to all but the most sophisticated (and costly) attacks, security researchers and practitioners today focus on humans as the "weakest link" in the security chain [2]. Information security turned to the disciplines of Human-Computer Interaction (HCI) and Behavioural Economics for security solutions that their employees can, and will, comply with [3-5]. Research in usable security and economics of security has yielded some valuable insights, but the problem of non-compliance is still rife. There have been steps to re-designing security solutions to fit human capabilities and limitations [5-7], and to base on them on people's real security needs, rather than what experts think [8], but we are still lacking an understanding of drivers of security behaviour 'beyond the interface'.

In this paper, we examine real-world non-compliance examples to understand drivers for non-compliant actions in information security. We present a study designed to identify the drivers of deliberate non-compliance, and then consider how this understanding can be used to transform Information Security Management. We begin by summarising existing literature on managing security behaviour.

2 Organisational approaches to Information Security

Information Security management currently attempts to reduce an organisation's exposure to security risks primarily by formulating policies of how they should behave to avoid those risks, and communicating those policies to employees. Policies are usually in the form of documents, which define the security objectives of the organisation, the responsibilities of employees, and sanctions for non-compliance. Policies are vital for organisations - without them, specific security implementations can be developed without a clear understanding of the organisation's wider security objectives and employee responsibilities [9][10]. But current security policies do not address the security challenges organisations face for two reasons:

1. Employees have no insights on policy design [11]: policies are designed to reflect the way the policymakers *believe* employees should behave, usually adding elements required to comply with regulations, audit checks and international standards.
2. The formulation of both policies and standards is largely based on lessons learnt from past failures, and is rarely grounded in scientific principles [12]. Security is currently a craft, that is only useful for securing organisations against breaches that closely resemble past events. It also makes assumptions about the context and the environment in which the interaction of employees with information-handling systems takes place, ignoring factors like employee workload, and treating all compliance scenarios as the same [13]. This results in policies ending up as long lists of *dos* and *don'ts* located on web pages most employees only access when they have to complete their mandatory annual "security training" and which has little to no effect on their security behaviour.

So employees don't comply with security policies. Most organisations respond by trying to reduce the possibility for non-compliance through technical mechanisms –

such as making downloading of information impossible. Enforcement usually takes the form of access control, restricting which employees can have access to which files. Compliance with the policies may be monitored. (In the case of access control, though, what tends to be monitored is whether access entitlements are still appropriate – rather than if an employee is in possession of a document they should not have). Security training and risk communication are used to influence employee behaviour towards compliance and reduce security risks. There are indications, though, that this set of current measures is not effective:

1. Compliant behaviours are being associated with specific threat scenarios or working practises, but there is little understanding of principles, or culture of secure behaviour. This means most employees are unable to take the initiative and make local decisions when new security problems arise [14][15].
2. Enforced compliance with cumbersome mechanisms consumes valuable employee resources, reducing the organisation's productivity [3][4]. In reality, large parts of the organisation (consider line managers, for instance) are complicit in employees' non-compliance, because – whatever the policies say – they value productivity more.
3. Compliance enforcement creates tension and deepens the *value gap* between security enforcers and the rest of the organisation [16]. Frustration with security is attributed back to the enforcers, which can result to any information coming from them being treated with scepticism or ignored and breeds a negative attitude towards information security in general [5] which can discourage compliance with security mechanisms - even sensible and well-designed ones [17].

Recent industry reports state that information security risks are increasing [1][18-20], so Information security research needs to develop more effective and sustainable approaches to managing non-compliant employee behaviour. Our contribution, presented in this paper, is a detailed, empirically-based understanding of reasons for non-compliance. This provides decision makers with a framework for identifying plausible ways of managing employee behaviour more effectively, and evaluating their effectiveness in a systematic fashion.

3 Understanding non-compliance

To obtain more detailed insights into employee compliance, researchers need access to employees who are willing and able to honestly speak about their security behaviour within the work environment. We have built relationships with a number of partner organisations that were prepared to grant us access to their employees, encourage participation, and publicly assure them there would be no reprisals. Over the past two years we have conducted studies in two partner organisations as part of a process to identify areas of friction between the business and security processes, and to design and deploy appropriate interventions.

The first stage in this process is to conduct a series of interviews. This stage has been completed in two organisations. 126 interviews were conducted with the US and the UK parts of a major energy company, and 86 interviews with the UK employees

of a telecommunications company. The interviews were semi-structured and probed aspects of security awareness and compliance, including:

1. The employee's awareness of the sensitivity of information they handle, and why they need to protect it.
2. Their knowledge of existing security policies, and what mechanisms they should or could use to reduce security risks.
3. Their experiences when interacting with the existing security policies and mechanisms.
4. Examples of, and reasons for non-compliance: how they circumvent policies and mechanisms, and their understanding of risks associated with these.

The majority of employees reported non-compliance in the organisation's day-to-day operations; interviewers then asked follow up questions to identify the conditions that led to the use of workarounds, the factors they used to decide whether to comply or not comply, and their understanding of the risks involved in their actions.

The insights we present here are based on a subset of the 126 interviews conducted in the first company, and a complete analysis of all interviews with respect to one mechanism: access control [21]. These were analysed using a thematic coding analysis based on the three Grounded Theory stages [22]: *open*, *axial* and *selective* coding. This led to the identification of three different non-compliance situations: *high compliance cost, lack of understanding, unavailable compliance mechanisms*.

The second stage of the process, completed in the utility company and underway in the telecommunications company, is the deployment of a scenario-based survey that presents participants with an example of a conflict situation drawn from an analysis of the interviews. Participants are offered 4 non-compliant courses of action that would allow them to resolve the conflict and were asked to rank the options in order of how likely they would be to use them and also to rate how severe a breach of policy the course of action is. A statistical analysis of the 1256 results from the survey (utilising MANOVA, Spearman's Rho and Chi-Squared tests) revealed several key "hotspots" where options rated as insecure were still being highly ranked as viable options Additionally, we were able to identify a US/UK cultural difference through the analysis of the results, which allowed us to further refine our understanding of the problem, and potential effective solutions. We also analysed 874 voluntary free-text comments left by participants using a Grounded Theory coding approach.

Using findings from these studies, summarised in the following sections and grouped according to the non-compliance situation they relate to, we aim to devise tangible suggestions to reduce the friction between the existing security implementation and business processes, provide guidelines for the design and deployment of future security mechanisms, and also aid in the development and maintenance of a more mature and resilient security culture.

3.1 Could comply, but cost too high

The first reason we identified as a driver for non-compliance is the high individual resource investment (such as time, or cognitive or physical effort) that certain security

mechanisms demand. The main focus of the majority of employees is not to be secure, but to efficiently complete a *primary production task* – such as manufacturing goods, financial investment, or delivering CNI services. This results in employees being willing to spend a limited amount of both time and effort on secondary tasks, such as security (the *Compliance Budget*, [3]). Security mechanisms that impose high workload overheads make non-compliance an attractive option for quick primary task completion [3][23]. Most organisations are unaware of, or ignore, the impact of security mechanisms on users. Cormac Herley [4] has pointed out, that in the consumer context, "security people value customers' time at zero". Our studies show that in the work context, organisations work on the assumption that employees can simply absorb the effort associated with security compliance. But because most security mechanisms are difficult and cumbersome to use, employees literally feel their time/effort being drained. This experience drives non-compliance: the perceived risk mitigation achieved by complying does not seem worth the perceived cost of effort and disruption to the primary task [4]. The greater the perceived urgency and importance of the primary task, the more attractive or acceptable non-compliant options become - even when employees are aware of potential risk. Employees re-organise their primary tasks to avoid or minimise their exposure to security mechanisms that slow them down significantly [24]. Our interviews yielded several examples of this around file sharing [21]. In our subsequent survey, we included a file sharing scenario, in which a group of employees had to share a large volume of files, but incorrect permissions prevented some of them from accessing those. The pressure of an upcoming deadline, combined with employees knowing that setting up access takes about a week, led to the most frequently chosen response (selected by 32.6% of employees) being *"to email the restricted document archive directly to all recipients on his work group mailing list"*. The same respondents rated this as the second most risky option, giving it a severity rating of 4/5). In the (voluntary) free-text comments for this scenario, most respondents described the consequences of not completing the primary task as definite and severe, whereas the risk associated with breaching the security policy was only a potential one.

In our interview analysis, we identified the following frequent non-compliance instances driven by the primary-task focus:

1. 50% of employees shared their passwords for quick access to systems if colleagues needed access for work purposes, but did not have the necessary permissions, because it *"would take ages"* to get the permissions changed. Password and account sharing is a common workaround. Our interviewees also expected their colleagues to do the same for them. Even some managers reported this as common and acceptable practice: "*employees newly-involved in a project access the system using someone else's credentials until their access is sorted out*". This is an example of organisations becoming complicit in circumvention of policies and mechanisms which do not fit with the primary task.
2. 53% of employees reported having used personal unencrypted USB drives to share data perceived to be sensitive with colleagues because it is faster and easier than company-issued encrypted ones. The effort involved in using the latter did was perceived to be *"not worth it for simple file transfers around the office*". Some

interviewees said "*they immediately wiped the drives afterwards*" to prevent data falling to the wrong hands.

In both cases, the delay to completing the primary task is perceived as "not worth the effort" of guarding against a potential, unclear risk; implicit in these statements is *"we've done it many times and nothing bad happened, so surely it cannot be that bad?"* Employees knew they were not complying with policies but felt this was justified by getting their job done or helping a colleague. The survey also supports our conclusions: in the scenario where an employee does not have an encrypted USB stick, the use of an unencrypted one was second most popular choice, scoring less than 1% behind the most popular option of borrowing an encrypted drive from a colleague. It was also rated as the second least severe risk; only uploading the files to public data storage received a higher severity rating.

3.2 Could comply, but why should I?

Inaccurate perceptions of risk and technology underlie many insecure behaviours [25][26]. In particular employees under-estimate the risk mitigation that can be achieved by compliance with some policies – and this, in turn, makes non-compliance appear a more attractive option. Examples of this include:

1. Employees rarely considered the possibility that their actions might lead to malware being introduced to their organisation's systems – hence the perception that using a personal USB stick would cause no harm.
2. Employees did not consider that deleted data can be easily recovered from drives if those are lost; they believed that deleting all the data from a drive after finishing with a file transfer provides adequate protection.
3. Employees considered any data stored on their company laptops to be secure because a Windows password was required to access them - but the Windows password was only used for access control purposes. This resulted in unsafe practices, like storing sensitive files locally on the laptops, assuming they are adequately protected when travelling on public transport [27].

We also found most employees did not have a good understanding of what information security is, and what it tries to protect. Security risks were described as *"just to confidentiality not security"* when confidentiality is a key goal of information security. There were also varying and inaccurate statements of what particular security policies permitted or prohibited - creating many security myths.

The survey results indicate that even when employees are aware of a policy and interpret it correctly, this is not a strong motivator for individual behaviour. We linked each of the options in the scenarios to a behaviour and attitude type. When asked what to do when observing a clear breach of policy by a colleague or visitor, the most frequently chosen option was *"report suspicions but take no direct action"* Employees took a passive approach – they did not think they had any responsibility to promote compliance with security policies. It is not sufficient for organisations to just correct employee misconceptions about policies and risks of their actions. They should also make adherence to security policies, and actively promoting adherence,

part of the psychological contract they have with employees [28] – but this will not work if security interferes with individual and organisational tasks and processes to the point that compliance is perceived as *"not worth it".*

3.3 Something's awry, just can't comply

In some cases, compliance may not even be an option, regardless of how much time or effort employees are willing to invest. Employees reported being unable to comply because the implementation the corresponding security mechanisms did not match basic requirements:

1. Employees justified copying files to laptops because there was insufficient space on their network drive, or because they had experienced problems accessing files they needed from home or while travelling.
2. Employees found the encrypted USB drives provided by the organisation were too small, so alternative file-sharing methods such as using unencrypted drives or emailing files had to be used.
3. The large number of passwords required in order to ensure access to the various corporate systems resulted in employees being unable to recall those from memory. This led to writing their passwords down, either in electronic form on their laptop or in a document they carry with them all the time.

In the above cases, most employees were aware of the increased risks associated with their behaviour, but felt that the organisation's failure to provide a "*properly working technical implementation*" forced them into workarounds so they could keep working and complete their primary task. The employees' perception was that the organisation would prefer security transgressions to "*letting everything grind to halt*" – and this was confirmed by similar responses from respondents with managerial responsibility in the survey. This is another example of how the organisation is complicit in employees' non-compliance.

4 Rethinking Information Security Management

Organisations looking to have effective information security need balance between the productivity and risk management goals. Our observations suggest that currently, organisations do not manage this balancing act: they set high targets for both productivity and security, and leave it to employees to resolve any conflicts between them. Most of the time, employees will chose productivity because 1) their behaviour is focussed on the primary task, and 2) they are principal agents who are trying to maximise their own benefit [29]. Based on our results here and those of other studies [5, 24] we suggest that most organisations are complicit in security non-compliance. They enable and reinforce their employees' non-compliance choices because they

1. Reward employees for productivity not security,
2. Fail to identify and fix security policies and mechanisms that create friction, and

3. Rarely enact the sanctions they threaten in case of non-compliance - very few organisations that threaten 'comply or die' on paper act on it[1].

Pallas [29] has applied the economic concept of *Principal-Agent* relationship to managing information security; we found his approach extremely helpful both in explaining the behaviours we identified, and to identify changes that organisations can make to break the non-compliance cycle. Employees are rational actors and to motivate them to comply with security policies, they have to perceive compliance as serving their own best interest [4]. The traditional "*command and control*" approach – where policies are set centrally by security experts, who select mechanisms and specify behaviours that must be complied with, without considering individual tasks or business processes – does not work in modern, flat, geographically distributed organisations who want to be agile, and want productive employees with ideas and initiative. Most organisations and policy makers have moved from compliance to risk-based information security standards (such as ISO27001), but have failed to make the same shift when it comes to managing employees' security behaviour; in that case organisations are 'unwittingly complicit' as they do not realise they are acting in a schizophrenic and uncoordinated way, negatively influencing employee compliance. Central policies and mechanisms cannot fit the variety of local and situational contexts in which individual employee decisions take place. Greater flexibility is needed to adapt to local circumstances, and solve conflict with tasks and business processes as they arise. Employees need to understand the risks surrounding their roles and the benefits of compliance to both themselves and the organisation, and then be trusted to make their own risk decisions in a way that mitigates organisational risks [15]. To aid the effective implementation of this security management approach the implemented security mechanisms need to be better *aligned* with the primary task, aiming to improve the identified employee misconceptions and misunderstandings that lead to non-compliance.

4.1 Align security policies with main productivity objectives

As we previously mentioned, security implementations need to act as enablers to the primary tasks not blocking those. Teo and King [30] introduce the term *Information Systems Alignment* to describe "*The degree to which the information systems plan reflects the business plan*". We argue that the same needs to apply to information security: The more a security policy and its implementation accommodate employee priorities and values, the more it improves the alignment of incentives in the enforcer-employee principal-agent relationship [29]. Thus, the security policy is less likely to be resisted [31].

[1] One of the authors has been involved in a (as yet unpublished) study of a company that publicly declares that non-compliance with any of its 'principal security rules' is grounds for instant dismissal. It would have to dismiss half of its workforce every month if it acted on this declaration; it would not be able to continue operating if it did.

To achieve this *Information Security Alignment*, employee attitudes and beliefs need to be considered when formulating security policies [30]. As shown in Section 3.2 high-level, abstract information security goals are not a strong motivator for employees – they cannot compete with concrete demands of business processes that employees know well, and for which they understand the consequences of failure to deliver.

Failure to take into account the beliefs and attitudes of employees results in the target group (end users) not adequately participating in the design of security mechanisms, or the creation and maintenance of a strong security culture, which inevitably are going to affect their day-to-day jobs. Participatory design [33] has been at the core of most successful human factors and usability engineering processes, and security designers cannot afford to ignore it. The reasons for non-compliance identified in our findings provide a good starting point for incorporating similar procedures into security design. Those need to be communicated to policymakers and security designers, so that information security solutions more suited to employee daily routines can be created. This can re-adjust employees' cost-benefit decisions, increasing compliance rates and creating a positive attitude towards security, which can also render employees more susceptible to attempts to instigate and maintain a stronger security culture within the organisation.

4.2 Adjusting the cost-benefit perception

To improve employee compliance decisions we also need to target their individual *cost-benefit analysis*. After creating policies and security implementations that accommodate for employee needs and priorities, we need to target the cost-benefit balance to shift it towards compliance by making it an economically attractive option for employees [34]. Beautement et al. [3] identify four factors through which this balance can be influenced (*Design*, *Culture*, *Monitoring*, *Sanctions*). In the remainder of this section we discuss how these four factors relate to our current findings, explaining how each one of those can be targeted to encourage compliance by changing the employees' perceived *cost-benefit* balance.

Design. Even for the most risk-aware and knowledgeable employees, the cost-benefit balance will favour non-compliance when implemented systems impose high overheads on their primary tasks [24]. Reduced compliance costs can eliminate the identified "*cost too high*" and "*can't comply*" non-compliance instances. To improve on the security design an organisation needs to:

1. Check that security mechanisms work in a given context. A network drive on which employees are encouraged to store their documents should be adequately sized so that they do not run out of space, combined with auto-archiving systems to prevent employees travelling around with confidential data on their laptops. In addition, encrypted laptop drives could reduce the risks when employees need to have some files stored locally and VPN access should be improved to reduce the need to transfer data through other channels. Single sign-on systems can eliminate

the need to write down passwords, while providing every employee with an encrypted USB drive can reduce the need to use unencrypted ones. In all cases the secure option should also be the easiest one to use.

2. Provide flexibility to make local and situational adjustments. Employees who need access to systems to proceed with their primary tasks cannot wait for a few working days for that to be granted, otherwise they will find another way to get access (usually through their trusted colleagues). Many interviewees reported that outsourcing of IT services had removed previously available routes to getting local and temporary adjustments made. The ability to make such adjustments would reduce password sharing and information sharing through unauthorised channels that is driven by the focus on productivity. The processes required for security, as well as the necessary mechanisms and technology, should mesh cleanly with the needs of the primary task.

Communicating the value of security. Once compliance-enabling systems are implemented, the organisation can consider raising employee awareness of risks and principles for managing them. Blanket 'security education campaigns' are not effective – messages need to be targeted at the perceptions held by specific groups of employees. The question "*why should I care?*" needs to be answered – what are the benefits? Organisations have to move away from the 'fear' sell of breaches and sanctions, and emphasise information security's contribution to achieving organisational objectives, and personal values, such as professionalism, instead [35]. This can be achieved through improved understanding of:

- *Everyone contributes to security*. Employee perception of security needs to be changed from "*getting in the way of achieving organisational goals*" to "*important for the organisation achieving its goals*" [36]. Employees need to realise that by following recommended security practices they are contributing to the smooth and efficient operation of business processes, as security ensures the availability of the resources required for the primary task to be successfully completed.
- *My specific contribution to protecting the organisation*. All employees can damage the organisation when not complying, even in relatively small ways. Thus, they all bear some responsibility for organisational security. Employees need to know what precautions they should be taking to reduce the organisation's exposure to security risks.

The two points above need to be communicated to employees through well-designed Security Awareness, Education and Training (SAET) campaigns. Those need to be formulated on a role-specific basis based on the identified employee misconceptions and non-compliance drivers, rather than flooding them with generic, organisation-wide advice that ends up doing more harm than the attacks they seek to prevent [37]. This approach also allows for increased flexibility, as organisations whose employees are adequately aware about the need for security, can tailor their behavioural change campaigns to start from the education stage. When employees are adequately knowledgeable on threats and vulnerabilities surrounding their role, organisations only need to implement an effective training scheme, testing their knowledge and

only reverting back to education when misunderstanding is identified. Once the 3 steps have been effectively implemented, role-specific reminders of the key messages are needed to reinforce awareness and keep the employees informed on new risks. Also, education material should always be available for employees that need to refer back to it.

Monitoring, sanctions – maybe. Trust, definitely. When the security systems of an organisation are designed in a way that favours compliance and employees are well-aware of the information security risks related to their roles, expensive *architectural means* (physical and technical mechanisms to prevent unwanted behaviours [29]) become obsolete: compliance now comes from employees motivated to behave securely [38], based on norms developed by the existence of both *formal* and *informal* rules that are significantly cheaper to enforce [29]. This can also create a positive environment where employees feel well-trusted by the organisation, inducing further compliance. The definition of trust as "*willingness to be vulnerable based on positive expectations about the actions of others*" [39] may sound like an oxymoron to old-school *command and control* security managers, but organisations where employees have increased responsibilities are more likely to establish a high-level of security awareness and improved understanding of the need for security [15][28][40]. On the other hand, employees that abuse trust should be visibly punished; clever monitoring implementations can detect employee trust abuse [41] and employees that observe sanctions enforced, are less likely to attempt to knowingly abuse trust.

5 Conclusions

Our results show that a better understanding of real-world employee compliance decisions creates a new perspective for information security management. Many organisations know that 'comply or die' is dead – but some still keep conjuring up its ghost, while others struggle to find an alternative paradigm for managing their employees' security behaviour. We suggest that the first necessary step is to recognise employees' primary task focus, and design security that fits into individual tasks and business processes. Only when this can been achieved should organisations focus on communication. Identifying misconceptions and myths that justify insecure behaviour helps to design targeted campaigns to bust or transform these. A clear set of information security principles needs to be identified and communicated to create employees who are risk-aware and know how to manage the risks that apply to them.

5.1 Future research

We are currently expanding our research to include other organisations, aiming for a better multi-organisational understanding of employee security perceptions and compliance-affecting factors. This will allow the generalisation of our research findings to provide an industry-wide view of current problematic information security

mechanisms and practices, together with suggestions on how those practices can be improved to increase compliance rates. The focusing of our research on the analysis of empirical data, gathered by investigating real-world problems from active operational environments, can result in improved effectiveness of security decision making and wider adoption of the underlying principles by organisations when designing their security solutions.

References

1. GRT Corporation, http://www.grtcorp.com/content/british-intelligence-speaks-out-cyber-threats
2. Schneier, B. Secrets and lies: digital security in a networked world. Wiley, (2000).
3. Beautement, A., Sasse, M. A., and Wonham, M. The compliance budget: managing security behaviour in organisations. In NSPW '08: Proceedings of the 2008 workshop on New security paradigms, pages 47-58 (2008).
4. Herley, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 workshop on New security paradigms workshop (NSPW '09). ACM, New York, NY, USA, 133-144 (2009).
5. Adams A. & Sasse M. A. Users Are Not The Enemy: Why users compromise security mechanisms and how to take remedial measures. In Communications of the ACM, 42 (12), pp. 40-46 (1999).
6. Sasse, M. A., Brostoff, S. & Weirich D. Transforming the "weakest link": a human-computer interaction approach to usable and effective security. In BT Technology Journal, Vol 19 (3) July 2001, pp. 122-131 (2001).
7. Weirich, Persuasive password Security, PhD thesis, University College London (2005).
8. Friedman, B., Howe, D. C., & Felten, E. Informed consent in the Mozilla browser: Implementing value-sensitive design. In System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences. IEEE (2002).
9. Fulford, H, &. Doherty, N. F. The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security 11, no. 3 (2003): 106-114.
10. Higgins, H. N., Corporate system security: towards an integrated management approach", Information Management and computer Security, 7 (5), pp 217-222 (1999).

11. Bartsch, S. & Sasse, M. A. Guiding Decisions on Authorization Policies: A Participatory Approach to Decision Support. In ACM SAC 2012, Trento, Italy, (2012)
12. Björck, F. Security Scandinavian style. PhD diss., Stockholm University, (2001).
13. Fléchais, I. Designing Secure and Usable Systems. PhD diss., University College London, (2005).
14. Wood, C., C. An unappreciated reason why information security policies fail. Computer Fraud & Security, (10), 13-14 (2000).
15. Flechais, 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 (NSPW '05). ACM, New York, NY, USA, 33-41 (2005).
16. Albrechtsen, E., and Hovden, J. The information security digital divide between information security managers and users. Computers & Security 28, no. 6: 476-490 (2009).
17. Karyda, M., Kiountouzis, E., and Kokolakis, S. Information systems security policies: a contextual perspective. Computers & Security 24, no. 3 246-260 (2005).
18. PWC (2012) http://www.pwc.co.uk/audit-assurance/publications/uk-information-security-breaches-survey-results-2012.jhtml
19. Ashford, W. (2012) http://www.computerweekly.com/news/2240148942/Infosec-2012-Record-security-breaches-cost-UK-firms-billions
20. Deloitte (2009) http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/UK_ERS_2009_CB_Security_Survey.pdf
21. Bartsch, S. and Sasse , M. A. How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization, ECIS2013: the 21st European Conference in Information Systems (2013), in press
22. Strauss, A., & Corbin, J. Basics of qualitative research: Techniques and procedures for developing grounded theory. Sage Publications, Incorporated. 2007.
23. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly, (34: 3) pp.523-548 (2010).
24. Inglesant, P.G. & Sasse, M.A. The true cost of unusable password policies: password use in the wild. In Proceedings of the 28th international conference on

Human factors in computing systems. Atlanta, Georgia, USA: ACM, pp. 383-392 (2010).
25. Adams, J. Risk, University College London Press, (1995).
26. Wash, R. Folk models of home computer security. Proceedings of the Sixth Symposium on Usable Privacy and Security. ACM,(2010).
27. http://www.pcworld.com/article/261754/does_the_windows_logon_password_protect_your_data_.html
28. Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. Human vulnerabilities in security systems. Human Factors Working Group, Cyber Security KTN Human Factors White Paper (2007).
29. Pallas, F. Information Security inside organisations, PhD Thesis, technical University of Berlin (2009)
30. Teo, T. S. H., and King, W. R. Integration between business planning and information systems planning: an evolutionary-contingency perspective. In Journal of management information systems, 185-214 (1997).
31. Trompeter, C. M., and Eloff J. H. P. A framework for the implementation of socio-ethical controls in information security. Computers & Security 20, no. 5: 384-391 (2001).
32. Dhillon, G., & Backhouse, J. Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153 (2001).
33. Checkland, Peter B. & Poulter, J. Learning for Action: A short definitive account of Soft Systems Methodology and its use for Practitioners, teachers and Students (2006).
34. Furnell, S. M., Jusoh, A., & Katsabas, D. The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1), 27-35 (2006).
35. James., H. L. Managing information systems security: a soft approach. In Proceedings of the 1996 Information Systems Conference of New Zealand (ISCNZ '96). IEEE Computer Society, Washington, DC, USA, 10- (1996).
36. Von Solms, B., & von Solms, R. From information security to business security. Computers & Security, 24(4), 271-273 (2005).
37. Kirlappos, I., & Sasse, M. A. Security Education against Phishing: A Modest Proposal for a Major Rethink. Security & Privacy, IEEE 10.2: 24-32 (2012).
38. Vroom, C., and Von Solms, R. Towards information security behavioural compliance. Computers & Security 23, no. 3 (2004): 191-198.
39. 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 62, no. 3 (2005): 381-422.

40. Schlienger, T. & Teufel, S. "Analyzing information security culture: increased trust by an appropriate information security culture." InDatabase and Expert Systems Applications, Proceedings. 14th International Workshop on, pp. 405-409. IEEE, 2003.
41. Caputo, D., Maloof, M., & Stephens, G. Detecting insider theft of trade secrets. Security & Privacy, IEEE, 7(6), 14-21(2009).