"Shadow Security" as a tool for the learning organization

Iacovos Kirlappos
Department of Computer Science
University College London
London, United Kingdom
+44 020 7679 0350
i.kirlappos@cs.ucl.ac.uk

Simon Parkin
Department of Computer Science
University College London
London, United Kingdom
+44 020 7679 0351
s.parkin@cs.ucl.ac.uk

M. Angela Sasse
Department of Computer Science
University College London
London, United Kingdom
+44 020 7679 7212
a.sasse@cs.ucl.ac.uk

ABSTRACT

Traditionally, organizations manage information security through policies and mechanisms that employees are expected to comply with. Non-compliance with security is regarded as undesirable, and often sanctions are threatened to deter it. But in a recent study, we identified a third category of employee security behavior: *shadow security*. This consists of workarounds employees devise to ensure primary business goals are achieved; they also devise their own security measures to counter the risks they understand. Whilst not compliant with official policy, and sometimes not as secure as employees think, shadow security practices reflect the working compromise staff find between security and "getting the job done". We add to this insight in this paper by discussing findings from a new interview study in a different organization. We identified additional shadow security practices, and show how they can be transformed into effective and productivity-enabling security solutions, within the framework of a learning organization.

1. INTRODUCTION

Information security management in organizations has traditionally focused on controlling employee behavior: information security policies specify what staff can and cannot do, and often this is enforced through technical means [2]. The growing use of technology to support activities in the work environment leads to security policies and mechanisms that ask for an increasingly unsustainable amount of effort from those working in the organization. Employees often either make mistakes when operating security controls, or circumvent policy [3][4], and this creates more security problems than the outside attacks the organization faces [5]. To offer effective protection, security management has to consider the impact security has on employees' tasks which are linked to their productivity goals (their *"primary task"*) [6][7].

Historically, security management sees non-compliance as reckless, but the truth is that organizations often do not evaluate if security policies and mechanisms are actually "compliable" [8]. An employee's choice and capacity to comply with security policies is governed by task goals, perceptions, attitudes and norms: employees will comply with security only if they understand the reason for it being part of their responsibilities and if complying will not impact their ability to proceed with their primary task unpunished [3][9].

The centralized "command and control" approach to security is becoming untenable [10]. The possibility of a "middle ground" solution in security design is presently unexplored, even though it has the potential to balance the priorities of employees and security managers within the organization [11]. Adaptation is happening nevertheless; employees appear to already be one step ahead. They can be frustrated by security demands, isolated from policy, or unwittingly untouched by it, but still have a personal desire to work securely. They are left to procure, deploy and refine their own solutions, as *shadow security* practices [1]. Understanding how these practices emerge informs the rethink needed in how organizations secure themselves. In this article we revisit the concept of shadow security, based on an analysis of interviews on information security behavior conducted in two large multinational organizations. We then explain how organizations can use shadow security to their advantage: it can be a powerful tool for organizational learning that can be leveraged to create security implementations that weather changes in the goals and technologies in an organization.

2. CURRENT STATE OF INFORMATION SECURITY IN ORGANIZATIONS

2.1 Mechanisms, Policies and Communication

Organizations implement technical mechanisms that enforce behaviors considered necessary to meet security goals. Where enforcement does not control behavior, shared policies define the responsibilities of employees and the behaviors expected of them, including sanctions for non-compliance. Policy content reaches employees via leaflets or security awareness campaigns, providing information, education, and evaluation of security competency. On the face of it this approach seems effective, but:

- *It's Impossible to Comply with Policies AND Get Work Done:* when compliance is difficult or at worst impossible, employee capacity is drained and organizational productivity is reduced [12]. Yet non-compliance is framed as user ignorance or willful disobedience, and treated on those terms [8]. Where there is a failure to consider the business context and environment of use, it is no surprise that in practice security often gets in the way of work getting done [3].
- *Current Policies are Irrelevant and Burdensome:* information security policies are meant to provide employees with a clear framework of security objectives and responsibilities to support their work [13]. The formulation and communication of security policies is reactive, driven by past failures. Always looking back can be dangerous in a fast-changing environment where new threats appear day-to-day [11]. There is no path defined for making sure that policies do not contradict each other when they come together in a person's work activities, and the effectiveness of policies in supporting security is not evaluated [14].

2.2 Enactment

When mechanisms and policies do not lead to the security behavior that security experts expect, they respond in one of two ways:

1) *The 'Tough' Approach – (Threat of) Sanctions:* in theory, breach of security policy is punished with warnings and sanctions. In practice, it is expensive to monitor employee behavior. And even where compliance is monitored, we have found that sanctions remain a threat, because companies cannot afford to dismiss or discipline large numbers of skilled staff [10]. Organizations that may advocate zero-tolerance for breach of policy, but, in reality, this is not an effective deterrent [15]: attempts for heavy-handed enforcement, increase tension between security enforcers and the rest of the organization [8].

2) *The Soft Approach - Persuasion:* many organizations respond to non-compliance with security awareness and training. But if security policies and mechanisms are a barrier to productive activity, awareness and training is just 'more time wasted by security' [4]: the negative perception of information security is simply reinforced and all security communication thereafter loses credibility [6][16].

3. INVESTIGATING NON-COMPLIANCE

To better understand employee experience with security we conducted interviews with employees of two large multinational organizations. We were asked to advise on how existing security policies and mechanisms can be revisited to better match the security needs of the organization. We engaged with their employees and explored how organizations can pragmatically improve their security while minimizing the impact on productivity-related tasks. This motivated us to develop a methodology that not only identifies instances of user non-compliance, but also suggests solutions that are potentially a better fit with individual and organizational business processes. Both organizations facilitated direct access to a sample of approximately 100 employees (the majority UK-based), and allowed us to explore employee interaction with - and sentiment toward - their current security policies and mechanisms. Participants held various lower-level and lower-to-middle management positions within a number of organizational divisions. The structure of interviews first touched upon aspects of security awareness and compliance, including:

1. What is the employee perception of how security impacts their role?
2. What do employees appreciate in terms of organizational support and policies for security?
3. Where employees exercise non-compliance, what conditions led to those behaviors that are divergent from organization policy?

This allowed us to identify friction points within the organization: individuals ending up in situations where they have to choose between security goals and production goals, leading to non-compliant behaviors [3].

In earlier work [10], we categorized the various factors that lead to employees adopting non-compliant behaviors:

1. *Lack of awareness*: Employees unaware of security risks or policy content have no clear incentive to exhibit security-conscious behavior.
2. *High compliance costs*: Mechanisms or processes which impact too heavily upon productivity leave employees with no other option than non-compliance.
3. *Compliance impossible*: Prescribed behavior cannot be followed due to problematic mechanisms; employees resort to finding other ways to proceed with their primary task.

These findings improved our understanding of how specific security policies and mechanisms for authentication and access control can be modified to fit with primary tasks.

We then conducted a second round of analysis on the interviews from one of the two organizations, identifying the emergence of "shadow security" (published in [1]). In the remainder of this paper we discuss: (1) How further analysis of the interview set from the second organization - combined with extensive embedded fieldwork - confirmed and informed the understanding of "shadow security" practices, and (2) How security experts can leverage, rather than quash, these practices to develop sustainable security management programs in their organizations.

4. THE "SHADOW" SECURITY

We defined shadow security as: "*instances where security-conscious employees who think they cannot comply with [- or are unaware of -] the prescribed security policy create a more fitting alternative to the policies and mechanisms created by the organization's official security staff*" [1]. It materializes as security workarounds, usually not visible to official security and higher management. These workarounds may not be as secure as the 'official' policy would be if everyone in the organization acted as the policy prescribed, but they reflect the best compromise staff can find between getting the job done and managing the risks to the assets they use. We grounded the development of shadow security to four distinct elements of the organizational security environment:

1. Employees have reasons to comply with security and are motivated to do so, but;
2. Security mechanisms are not fit to support the primary task. As a result:
3. A significant amount of security mediation takes place at team level.
4. The inability of the organization to address employee security concerns accentuates the problem as employees become isolated from the security division.

We revisited the four points to confirm their existence by conducting and analyzing security behavior interviews in the second organization. In the remainder of this section we present interview extracts supporting the presence of shadow security in the organizations and how the four shadow security elements evolved in this organization, confirm the original findings.

4.1 Employees Want to Comply

Contrary to the archetypal view held by security managers, employees appear sufficiently aware and motivated to comply with security.

P36: "*Normally my day to day work wouldn't have very many security implications. Being a home worker, I think I tend to be over-cautious sometimes and I tend to put all the documents I print off at home into a confidential waste bag and I bring it into the office sealed whenever I need to dispose of a full bag."*

Individual secure behavior was increased when peers encouraged secure behavior in others: participants reported that the actions of colleagues - reminding others to comply, and actively responding to peers' insecure behavior - also acted as a driver for their own secure behavior:

P71: "*Someone proposed to share a password so we could get data from a system because the team that supported it didn't want to create new accounts. [...] I said I wasn't comfortable with that. In case someone did something that they shouldn't do, you couldn't directly identify if someone had done something bad [...] We definitely didn't go ahead as planned.*"

4.2 Badly Fitting Security Mechanisms

Despite recognizing the need to protect the organization, some employees spoke of security mechanisms and policies in the organization as something that creates significant additional burden to them, increasing friction between security and productivity. The perceived impact upon the ability to proceed with a business task lead to employees choosing to procure their own security solutions, which have lower workload and/or are less disruptive and less demanding, to support (what they legitimized to be more proportionate) security behavior. The security burden was articulated in various ways:

1) *Time:* employees found themselves in situations where enacting the prescribed security behavior slowed completion of primary business processes:

P27: "*if you want a piece of software on your PC, there's a system we have where you request it and if it's not on there, you can ask for it to be put on there, but a, that costs to have it put on there and b, there's a time delay. So a lot of people think why should I bother, I'll just install it off the Internet. So there is a time delay that forces people down to ignoring the policies.*"

In other cases, they felt they needed support, but provisions for IT support were slow, creating frustration.

P66: "*I don't even try. I think the last time I spoke to them, I was listening to music for about 45 minutes and I gave up. [...]I log it online and then I find it frustrating if after a couple of days I've not had a response*"

2) *Increased Cognitive Load:* Employees also devised their own security mechanisms when the associated cognitive load was perceived as excessive for the task. Participants reported that they felt it necessary to physically write down the passwords for system accounts that they rarely used (and as such could not readily recall), and applying ad-hoc security principles to protect the artefact recording the password(s):

P19: "*Sometimes you have to do and sometimes they do so I can remember them all. Other than that it's writing them down and then that's frowned upon. You see my manager doesn't write his password down and he's forever resetting.*"

3) *Disruption:* In other cases, security restrictions led to disruption of employee tasks; participants mentioned that they found themselves in situations wherein security mechanisms were blocking their primary task. In response to this type of situation, they had to resort to other non-prescribed practices:

P23: "*You're slightly forcing people to store things locally simply because the volume of data [...] centrally stored data is more expensive, so there's a definite problem there between the amount of storage that you give people which is central therefore more secured, versus the pressure on them to store things locally.*

4) *Lack of Adaptability:* A lack of adaptability in the organizational IT systems to account for changing organizational conditions caused disruption, leading to employees having to derive ad-hoc solutions:

P2: "*to try and launch new products and services it is quite difficult from a security point of view. It makes mobility really difficult. I deal with it by not using our systems, I use other systems in place. Like, for instance, Dropbox [...] I can see some risks but I think the benefits far outweigh the risks.*"

4.3 Security Mediation at Team Level

Managers are directly responsible for many elements of security on behalf of their teams. They take access control decisions, provide security decision support and prescribe behaviors to team members. Our participants reported that security communication occurs at team level through discussion with their manager or colleagues, in isolation from the organization:

P49: (talking about their manager) "*He bangs something out that says, "Guys, please be aware", or if not him, his manager, or maybe his manager's manager bangs it out, says, "Guys, you know or perhaps we'll have a quick meet about this and discuss the implications and how to stop this".*

4.4 Treatment of Employee Feedback

Employees have opinions about the effectiveness of the organization's existing security implementations; opinions indicate where it is believed the organization has failed to provide adequate security support or indeed failed to keep the organization secure. Housekeeping around access control, for example, was not seen by employees as being managed properly and participants expressed concerns to that effect:

P68: (talking about previous job) "*I would within 24 hrs be required to provide all their company equipment back to a central point and all of their telephone access system would have been terminated immediately and if I hadn't done that within 24 hrs, someone would be sat on my desk demanding it. In this company I have seen instances of, you know, these things not being enforced for weeks or months.*"

Despite employees taking action and reporting perceived security problems, participants reported that to them it seems that organization does not fulfil their requests:

P25: (requesting secure drawer access) "*No. I'd love one but I think it's a bit of a waiting list. I've questioned whether I would use one here. I'm probably here once or twice a week.*"

But employees also seemed to feel reporting is not encouraged:

P48: "*I think the reality with most things is to stay ignorant. I wouldn't go up to the head of Security if I was outside and say "I'll do this and I'll do that" and he'd go "you're not supposed to do that", you'll get told off.*"

We later looked at the call volume to the Security helpdesk and it appeared that the number of requests for support is steadily decreasing and has halved in the past calendar year. A first reaction is to assume that the security division is solving pressing problems, but where regular contact with employees is lacking, it could equally suggest a decrease in the willingness of employees to communicate their concerns or ask for support.

5. IMPLICATIONS FOR ORGANIZATIONAL SECURITY

Our analysis confirms the existence of shadow security practices in an organization environment distinct from where it was originally observed. These practices emerge when employees believe that they are unable to behave in the policy-prescribed way, in response to a combination of the drivers identified in the previous section. Where the organization's existing security implementation is perceived as problematic, it isn't necessarily because security *as a notion* is disregarded; productivity-focused employees can perceive specifically that the organization's provisioned approach to security is inadequate if it does not meet their needs. We identified many cases where employees tried to act in a secure way even when they were not complying with policies. Even where provisioned security is appropriate, this can be undone by dysfunctional security communication which does nothing to address limited awareness of security policies and formal procedures. Shadow security can then develop in isolation from the security function. Rather than remaining passive, employees, peer groups, and managers use their own understanding of security - individually or collectively - to devise adaptations of unsatisfactory security measures or introduce their own novel solutions.

5.1 Benefits of Shadow Security to the Organization

Security-aware employees bring a number of positive qualities for the organization:

1. Employees appeared for the most part motivated to invest some proportion of their time to keep the organization secure (as seen elsewhere [3]).
2. Employees appeared willing to take action to address potential risks when insecure conditions or behaviors were identified (i.e., take care to protect information, behave securely when the overhead is minimal).
3. Security mechanisms that impose minimal additional workload positively affect employee compliance behaviors (as seen elsewhere [3][10]).

5.2 Risks of Shadow Security to the Organization

Shadow security behavior poses a number of potential risks for the organization if not managed properly:

1. It creates a false sense of security: employees rationalize that they are protecting the organization, but their understanding of the risks the organization faces can be incomplete or inaccurate. This approach *could* be effective if employees are significantly aware of related risks or choose actions that protect the organization, *but* employees cannot be assumed to be security experts [17] and shadow security practices may lack appropriate consideration of the associated risks.
2. Ineffective communication of policy to managers - those best-placed to convey behaviors to employees - can lead to the development of security "micro-cultures" within teams. Without appropriate support, managers cannot be assumed to be sufficiently aware of policy and the security risks that exist within the organization. The absence of a consistent security position can result in divergent behaviors developing independently, out of the organization's control.
3. "Hard" technical solutions that the organization refuses to change or replace could prevent shadow security practices from developing, but they negatively impact employee productivity, create disgruntlement and can lead to alienation of employees. This further compounds resistance to centrally dictated expectations - shadow security practices may indirectly reduce or stem frustration with security.
4. Not responding to employee feedback about identified security shortcomings is seen to validate adaptation of security by employees when they believe an alternative solution is needed.

5. The presence of a shadow security environment can lead to the emergence of a non-compliant organizational security culture [18]. Key stakeholders in the organization (line managers, for instance) appear to be complicit in the development of shadow security, primarily because these practices moderate the negative impact of security on productivity: like their employees, they value productivity over security compliance. In addition to the immediate risks this creates, it can also act as an additional level of resistance to attempts by the organization to change employee or team behaviors and account for divergence from prescribed behaviors or current mechanisms when a good reason for it exists.

The identified benefits and risks suggest that the potential for shadow security practices to develop cannot simply be ignored by organizational security managers when (re-)designing, or improving existing security mechanisms.

6. LESSONS FROM SHADOW SECURITY

Organizations would do well to consider that shadow security happens naturally and is a valuable indicator that security solutions are not serving the business. Shadow security practices emerge when the organization could do more to align security with productivity goals. Employees will take action if the organization does not, rather than doing nothing or passively relying on the organization to remediate - the work that employees need to do will not wait for workable security to arrive.

For an organization, ignoring the presence of unusable security mechanisms is dangerous: errors and workarounds create vulnerabilities [8], people ignore security advice that requires high effort for little benefit [4], and systemic non-compliance creates noise in which precursors of attacks are hard to detect [3].

Security management should not encourage shadow security simply through ignorance. There needs to be: recognition of individual capacity for consciously considering security as part of work activities; a strategy for engaging with the security needs of users, and; (two-way) channels recognized within the organization that support a dialogue with users.

Where shadow security practices begin to emerge, contributory factors can be addressed to improve organizational security and identify more workable security implementations that align with productivity objectives.

6.1 Reduce Compliance Costs

The policies currently produced by security managers are not necessarily invalid - they are just created with an incomplete picture; organizations do not track the effort that individuals have to expend to comply with what the policies ask (especially when considering the myriad other policies they must comply with [15]). When a security mechanism is clearly crippling the business it may be removed, but then the risks managed by the mechanism are left unaddressed until another solution is found. This requires a move to a participative, risk-based approach that works with users to understand where and how security can align with the productive activity to protect valuable organization assets, especially *during times of change*.

Security experts believe that there is a tradeoff between usability and security. This misconception lead them to think it is ok to ask users to make extra effort because it's either ease-of-use or security that must win. They think usability is a luxury they can only afford to consider once security is assured - in practice that means never. But usability is a *hygiene factor* for security: solutions that are not usable (disrupt and divert effort from employees' primary tasks) will be circumvented, and lead employees to create shadow security practices. At worst they will become disgruntled and see security as an obstacle that they need to get around. This can have severe consequences for an organization: it hinders the development of social capital and shared values [19], resulting in minimal incentive for secure behavior, while increasing the probability of insider attacks [20]. It also impacts the ability of the organization to retain its valuable employees; dissatisfaction can lead to them eventually leaving the organization [21].

An example of replacing disruptive security with productivity-driven solutions is seen in the large number of systems to which employees had to authenticate themselves in both the organizations we studied. Writing down account passwords was the only way to guarantee that secured systems could be accessed consistently. Organizations can address this by - at the very least - providing employees with password managers that work with all systems/websites they need to authenticate to, removing the need for employees to devise their own solutions to the “too many passwords” problem.

Human factors expertise and design methodologies (e.g. Soft Systems Methodology [22] or AEGIS [12]) need to be integrated in the design process of security systems. A more human-centered security design process will allow designers to move away from the current “deploy, if too much noise, remove” approach that can make security implementations expensive to implement, difficult to use and unsustainable.

6.2 Engage Low- and Middle-Management

The increasing decentralization of modern IT implementations begs for a collaborative, decentralized approach to security challenges [23]. Security managers are not in a position to oversee security in practice across the organization - there will be times when policy does not provide answers, or when the distinction between policy-as-guideline and policy-as-rule is unclear. Our findings suggest that motivation for effective security behavior can come from managers in organizations: employees often turn to them when making security decisions. Managers are then making local - and potentially ad-hoc - decisions about security, including access control and information sharing. Given that they moderate security behavior amongst members of their teams, they are best-placed to respond to shadow security. *Security-specific training for managers should then be tailored to acknowledge their role as mediators of security.*

Rather than overloading managers with security knowledge, training can consider organizational goals and organizational security principles. Communication also needs to be two-way: security managers should listen to managers’ questions, problems and concerns, and help them deliver *correct* and *consistent* security advice to their teams.

Another key element of the role of managers is that they interact much more frequently with employees and have a unique perspective of both the goals of the business and any frictions between security and productivity tasks. The solicitation of feedback from managers should be incentivized as part of their role, towards an effective reconciliation of shadow security and prescribed security practices.

6.3 Engage Users in Security Design

Our participants openly discussed how security problems interrupt their workflow, and the coping mechanisms they developed as a response. They were also able to articulate ways for the organization to improve security (even without necessarily being security experts), where this feedback could be repurposed to improve the organization's security posture [23]. Where productive tasks can be understood, security needs can be addressed and security designed to match. The purpose of feedback solicitation is to learn something from users that security implementers could not either predict or detect at the early deployment stages or from their position outside of the primary task. Security managers do not see security from the perspective of users, and so cannot assume they have designed security that fits the task *unless* they have otherwise engaged with users in the design/deployment of security solutions.

The importance of involving users in systems design was first identified by Checkland et al. [22], and the value of participatory and contextual design is widely accepted among system designers and developers. But this approach is not adopted in security, with notable exceptions in the formulation of authorization policies [17]. A participatory security design approach represents users' tasks, and this knowledge can be used to identify low-friction solutions that do not compete for users’ attention or effort, disrupt productive activity, or lead to errors. It also helps to align security goals and values with those of the wider organization [24].

Using users as a resource makes it possible to identify specific points of friction and candidate improvements. Our participants openly discussed how security problems interrupt their workflow and what coping mechanisms they developed as a response. They were also able to articulate concerns in a meaningful way where they could see ways for the organization's security provisioning to be improved. Some reported a strong willingness to report their observations.

Crucially, engagement with employees serves to reframe securing the organization as a collaborative activity, not as a barrier to work. Persistent and readily-accessible feedback channels ought to be in place as part of the organization’s structure and culture (e.g. a "we've just upgraded your email client, is it working well for you?" pop-up that "gobbles up" any post-deployment frustration). If an employee reports a security concern, there should be a visible response that describes the impact the feedback has made. In addition, security enforcement among team members can be scaled to cover the wider organization: employees can champion secure behavior within their teams, situating security practices in primary roles in a more meaningful way than sanctioned security communications. By advertising a capacity to listen, the security function can leverage employee experiences as an additional layer of assurance that security mechanisms are serving the business.

6.4 Assess Security for its Effectiveness

The organization will need to decide its tolerance for shadow security behaviors, but before that the precursors ought to be monitored. Currently there is no pre- or post-deployment assessment of the impact of deployed security mechanisms on employee productivity. A lack of visible complaints may be read as proof that all is well, but this silence could equally signal a lack of engagement with the very employees that security is meant to support; they can just quietly resort to their self- or team-procured solutions.

Modern systems design methodologies call for assessment of the effort users need to expend on a system in early design stages and also iterative development and deployment of technology solutions [22]. Currently, updates to security provisions are deployed without testing, mostly in a reactionary way or to comply with regulation and international standards [10]. Attempts for improvement only come when security significantly disrupts production task processes. Early user testing and piloting can improve on this and turn security management into an iterative process, improving its effectiveness. For example, the introduction of a new business system that requires password authentication may seem a straightforward task, but its cumulative effect can create problems. Adding one more credential to the cognitive load placed upon users further strains their capacity to both recall individual passwords (encouraging use of recall aids) and generate truly unique credentials for individual systems (making re-use of existing passwords an increasingly attractive solution) [3][25]. Such a situation could have been recognized - and potentially avoided - if user effort required by existing security implementation was quantified using methods like the NASA TLX [26].

7. TRANSFORMING SHADOW SECURITY

The previous section illustrated that security managers working within organizations need to be mindful of much more of what happens within the wider organization, and as Schein puts it, become *perpetual learners* [27]. An ability to learn is important for adapting to changing organizational environments where the business and technologies change and become more complex. On the surface, control-oriented security may provide a sense of stability that negates the need to place faith in members of the organization to do the right thing of their own volition. But where it appears to be currently failing is to change and adapt to what individuals experience as time goes on (as already demonstrated in public transport systems, for instance [28]). We have illustrated that adaptation is necessary to manage the complexity of business environments, and that if the organization is not willing to adapt, employees will enact those adaptations themselves. Where employees cannot adapt, security managers maintain stiff, brittle systems that can break with spectacular results. Shadow security behaviors demonstrate that, in addition to security managers, employees also want security - the potential exists for both sides to learn. In this context of change, security cultures can benefit from becoming more *learning-oriented*.

7.1 Importance of Measurement

Measuring security behavior helps security managers to understand how security fits with productive tasks in practice. Knowing that individuals within the organization want (appropriate) security that supports their productive work, managers can observe real usage data and user feedback to learn how to adapt security provisions to achieve both productivity and security. Schein [27] notes that if the environment is undergoing increased change, that it is not appropriate to base decisions in the past or in the present, and that it is necessary to think *"in terms of the near future to assess whether or not our solutions are working"*.

The use of metrics to measure security behavior is currently limited. Security managers have access to detailed technical information on intrusion attempts, virus logs, access requests, traffic information and many more. Security professionals very much appreciate the potential benefits of this information [29][30]. Today there is the ISO27004 standard on information security, which defines metrics and measurement for assessing the effectiveness of Information Security Management Systems [31]. But the metrics defined in the latest edition of the standard do not seem suitable to capture the existence of shadow security behaviors in an organization (e.g. *Count of logs/registries with annual information security awareness training field/row filler as "Received"* or *ask each user about number of passwords which satisfy organization's password policy*).

We need to look deeper into information readily available in organizations, for data that can indicate the presence of shadow security behaviors. This may sound impossible at first, but information exists in abundance in modern organizational IT systems and, as Hubbard puts it, "anything detectable at different amounts is measurable" [32] (p. 48). As we demonstrate in this section, if we consider the dynamics carefully there are inferences which can be made from existing measurements and measurement capabilities. This can allow *increasing confidence in prevalence of the security behaviors encouraged within the organization*, where - as we have discussed - this confidence is now in question.

This approach affords:

1. Management of the human element of security, moving away from the currently static, "fire and forget"[1] approach.
2. Accurate assessment of the post-deployment impact that security measures have on employee activities.
3. User involvement without the need for continuous - and disruptive - direct engagement. This further recognizes the value of user time to the organization.
4. Prioritization of security concerns and implementation of targeted interventions to address specific shortcomings.
5. Collation of various metrics to obtain an accurate organization-wide snapshot of employee behavior at any given point in time, allowing for more productivity-focused information security management which addresses risks closer to the concerns of the business.

7.2 Examples of Security Measurement

Security managers ought to consider how to identify the indicators of Shadow Security and develop a capacity to analyze and adapt in cooperation with other functions in the organization - security culture should align with the organizational culture. We worked closely with one of our corporate partners in order to identify the type of metrics that could be used to identify the presence of shadow security. We investigated many sources of evidence for security behavior: organizational logs, leavers' process, usability and availability of organizational systems for information storage and sharing, clear desk processes, IT support and employee feedback mechanisms. Despite our research methodology providing extremely useful insights and potential improvements for the organization, repeating it periodically to continuously assess security behavior in an organization is expensive. To address this drawback we identified a set of potential measurements - based on information that can be readily available through organizational systems – which can be used to identify and manage shadow security in their security domain.

7.2.1 Information Flow

For large organizations like the ones investigated in this research, it is common for employees to engage with colleagues situated in various locations, even overseas. Combined with the increasing prevalence of home working, remote collaboration results in sensitive organizational information being present at various locations across many devices, increasing the potential points of failure that could lead to security compromises. Both of the organizations we studied had implemented internal file storage and sharing systems that employees could remotely access, so in theory, provision for secure behavior was in place. But problems in capacity, slowdown in accessing the organizational systems and lack of flexibility (no access provisions for various types of devices) lead to employees using other provisions. Employees exposed the organization to potential security risks by using third-party cloud storage solutions or by emailing sensitive information due to perceived lack of organizational support for effective file sharing. From an information security manager's perspective the provision for secure behavior exists - it just does not work as expected. The effectiveness of the implemented solutions can be assessed by observing the following:

1. *Metrics generated by agents on managed organizational computers to deduce data handling information* (e.g. Data Loss Prevention agents - DLP). This software can provide quantitative data on information shared through emails or sensitive information stored locally on corporate machines. Security managers can track number of attachments or pattern-matched text excerpts being sent to out-of-company email addresses. If staff find it easier to send files to their personal accounts via email and it does not contravene organizational guidelines (for e.g. working from home, client visits/presentations, etc.), what support can be given (e.g. file-centric encryption technologies)? If there are particular kinds of data being shared, can other business functions inform the sensitivity of that data?
2. *Check volume of access to third-party cloud storage servers from inside the corporate network*. This cannot provide absolute certainty on how much of cloud storage access is for corporate information, but extensive use of cloud providers can indicate *the need to investigate* current use of organizational systems.

[1] Military term for missiles that require no further guidance after launch

3. *Check utilization of internal file-sharing systems*. Does it make sense if an employee has not accessed their personal file space in two or three working days? It may be that remote access to organization systems is difficult in unforeseen circumstances, requiring a complementary solution that protects data at rest.

7.2.2 Access Control - Provisioning of Accounts

Modern access control systems can be monitored and tuned to match demand, as can privilege management processes. Quick deactivation of a leaver's account was reported as being very important by the information security managers of both participating organizations (in one of the two companies there was a target of a maximum of 48-hours for deactivation). But in looking at account control systems and talking to account managers we identified many cases that leaver's accounts were left active for much longer, either for potential future need to access to the systems or because accounts administrators were not informed about an employee having left the organization. An interesting example came from contractor accounts: many people whose contract expires join the organization again after short periods of time, so their accounts were left untouched "just in case". We also heard of new starters being logged in to their supervisor's accounts - while the supervisor remained close by during use (as a security precaution) - until their own account could be set up. There are a number of metrics that an organization can use to identify account misuse:

1. *Mean time for leaver account deactivation*: Measure mean time it takes for an employee that has left the company to be removed from systems they had access to and compare this to targets defined in the organization's security policy.
2. *Mean time for new account creations*: Measurement of account creation time is important - if new accounts take too long to create, teams will use what they already have (they may not be able to create accounts, but managers can manipulate those that they have jurisdiction over). The time when an account creation request is received and the actual arrival of the account owner can indicate the perceived lead-in time required. If accounts could be created in time for new staff, there then wouldn't be a need to even consider holding on to "template" accounts.
3. *Account usage*: If an account is showing no usage activity, it implies that it is either unused (and should be a candidate for deletion), or the owner has simply chosen to act outside of the access control system and access files some other way. This is doubly important in that security managers will need to ask themselves whether a provisioned system that is seeing inconsistent use (and in turn, provides inconsistent coverage and security) has relative value to an assurance of complete coverage.

7.2.3 IT support - Response to Helpdesk Requests

Organizations need to recognize that even information not directly related to employee behavior can lead to the emergence of shadow security behaviors. As we previously discussed, slow access control request response leads to employees finding other ways to obtain information necessary for their work. Devising metrics like *time to fulfil access request* can aid assessment of the impact of potentially problematic support functions that may impact employee ability to comply with security.

For instance, support processes may be appropriate, and employees instructed as to when to contact a helpdesk in specific circumstances, but then the response time becomes critical. If call response times are slow, employees with momentary pressures (e.g., deadlines, one-off meetings with associated deliverables) will have to adapt there and then using their own understanding of IT and security expectations. Helpdesk staffing and staff training may need to be revisited if the number of unsatisfied requests is perceived as too high - some means of recording details of "unusual" requests may also be necessary to target that same training (e.g., if staff are using unexpected devices or software and want tailored support).

7.3 Benefits of Shadow Security Measurement

The metrics discussed here are generated based on readily available (or relatively easy to generate) information. A combination of the above examples (and many others) can provide a suite of indicators of not just the performance of the technical systems deployed, but also the performance of processes that support employee behaviors.

Security managers are at times asked to resolve security issues with services too late in the process (at their own resource cost and expense), where perhaps they could have been involved earlier (e.g. service deployment). The same argument applies to Shadow Security - managers may simply have to decide to be involved in user requirements, or to provision for redundant capacity to hold back for nasty surprises caused by insecure workarounds. The reconciliation of shadow security is a chance to provide greater assurance to organization leaders that security mechanisms are working as intended; standards exist as a guideline, but could be considered as the low bar - if employees are involved in security the organization can do better. Schein [27] argues that organizations with diverse cultural resources are better equipped to weather unpredicted events, and further that subcultures are necessary for learning and innovation.

To instrument the infrastructure to measure Shadow Security could be relatively cheap compared to maintaining or rebuilding fractured security mechanisms (or a demoralized, fractious workforce that has developed too many non-sanctioned security habits). Meeting the security needs of various sub-groups of end-users may seem difficult to scale up (especially for large organizations). However, IT and business environments can change rapidly to create a fast-changing environment, for instance when an organization merges its IT systems with those of another organization, or an organization changes IT supplier and thereby replaces core systems with something wholly different (which staff and administrators alike must learn to use). It may be possible to position Shadow Security engagement as a resource which organizations can call upon in times of upheaval, to adapt to turbulent times. No organization has to panic about shadow security – measuring it and managing it can be business as usual.

8. CONCLUSION

User reaction to an organization’s security implementation needs to be heard, lest it weaken the organization’s security posture. Employees are not evading provisioned security, but attempting to balance security and productivity for lack of organizational support. Learning from, and not ignoring, employees can enhance security, aligning it with organizational goals and increasing its effectiveness. If users are not heard, they can become disenfranchised, and should they have a legitimate concern about security, they will not remain passive in the face of ill-fitting solutions - they will engineer their own "shadow security" environment.

Organizations must be able to recognize when and where shadow security is created, its causes, and in turn how to adapt security provisions to respond to user needs - without a consistent means of engagement with users, security enforcers cannot claim absolute certainty that the security infrastructure exists exactly as intended. Once identified, shadow security existence should be not be treated as a problem, but as an opportunity to identify shortfalls in current security implementations that can be leveraged in providing more effective security solutions for organizations.

We propose that security managers can learn from shadow security in a number of ways: simplifying compliance with security, measuring the effectiveness of security mechanisms after deployment, engaging users when designing security solutions, and leveraging the position of team managers as both a mediator for security and a conduit for feedback as to the appropriateness of security solutions in supporting productive tasks. As we explained in this article, the foundations of a continuous learning and improvement process for organizational security can be implemented without imposing significant overheads: much of the information needed to identify the existence of shadow security behaviors is already available in various forms around various organizational systems.

9. FUTURE WORK

The identification of shadow security creates a number of future research challenges. To empirically assess the effectiveness of shadow security driven security management as an integral part of a holistic security management process, we are currently conducting similar analyses on additional sets of interviews from other organizations. We are also designing improvements in organizational systems informed by identified shadow security behaviors within two partner organizations. This will allow deployment of security solutions informed by shadow security behaviors and assessment of their real-world effectiveness.

We have also agreed with a partner organization to conduct further interviews and in-depth analyses studying the rationale and risk perception of employees engaging in shadow security behaviors: in many cases employees admitted to knowing that their practices were compromising security, so there is a need to determine if and how they assess the risks created by their behaviors before following a course of action (e.g. when cloud storage is used to store corporate data, are employees aware that cloud storage providers may be compromised?). We also aim to examine the compatibility of shadow security-driven information security management with current regulatory frameworks and international standards with which modern organizations need to comply.

10. REFERENCES

[1] Kirlappos, I., Parkin, S., Sasse, M. A. 2014. Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security. In *Workshop on Usable Security*.

[2] Von Solms, B. 2006. Information security–the fourth wave”. In Computers & Security, 25(3), pp.165-168.

[3] Beautement, A., Sasse, M. A. and Wonham, M. 2008. The compliance budget: managing security behaviour in organizations. In *Proceedings of the 2008 New Security Paradigms Workshop* pp. 47-58. ACM.

[4] Herley, C. 2009. So Long, and No Thanks for the Externalities. In *New Security Paradigms Workshop* (NSPW).

[5] Schneier, B. 2000. *Secrets and lies: digital security in a networked world*. Wiley.

[6] Karyda, M., Kiountouzis, E., and Kokolakis, S. 2005. Information systems security policies: a contextual perspective. In *Computers & Security*, 24(3), pp.246-260.

[7] Sasse, M. A., Brostoff, S., and Weirich, D. 2001. Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3), pp.122-131.

[8] Adams, A. and Sasse, M. A. 1999. Users are not the enemy. In *Communications of the ACM*, 42(12), pp. 40-46.

[9] Herath T. and Rao, H. R. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. In *European Journal of Information Systems* 18 (2), pp. 106-125, 2009.

[10] Kirlappos, I., Beautement, A. and Sasse, M. A. 2013. Comply or Die Is Dead: Long live security-aware principal agents. In *FC 2013 Workshops, USEC and WAHC 2013*, Okinawa, Japan, April 1, pp.70-82, 2013.

[11] Dourish, P., Grinter, R. E., De La Flor, J. D. and Joseph, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. In *Personal and Ubiquitous Computing* 8, no. 6: 391-401.

[12] Fléchais, I. 2005. Designing Secure and Usable Systems. *PhD diss.*, University College London.

[13] Fulford H. and Doherty, N. F. 2003. The application of information security policies in large UK-based organizations: an exploratory investigation. In *Information Management & Computer Security* 11(3), pp.106-114.

[14] Björck, F. 2001. Security Scandinavian style. *PhD diss.*, Stockholm University.

[15] Herley, C. 2014. "More is Not the Answer", In *IEEE Security & Privacy magazine*.

[16] Albrechtsen, E. and Hovden, J. 2009. The information security digital divide between information security managers and users. In *Computers & Security* 28(6), pp.476-490.

[17] Bartsch S. and Sasse M. A. 2012. Guiding Decisions on Authorization Policies: A Participatory Approach to Decision Support. In *ACM SAC 2012*, Trento, Italy.

[18] Da Veiga, A. and Eloff, J. H. P. 2010. A framework and assessment instrument for information security culture. In *Computers &* Security, 29(2), 196-207.

[19] Kirlappos, I., Sasse, M. A. 2014. What usable security really means: Trusting and engaging users. In *HCI International.*

[20] Moore, A. P., Cappelli, D., Caron, T. C., Shaw, E. D., Spooner, D. and Trzeciak, R. F. 2011. “A preliminary model of insider theft of intellectual property”, Technical Report, Carnegie Mellon University.

[21] Ken Blanchard, “Building Trust”, Ken Blanchard companies, 2010, retrieved from: http://www.kenblanchard.com/img/pub/Blanchard-Building-Trust.pdf

[22] Checkland P. B. and Poulter, J. *Learning for Action: A short definitive account of Soft Systems Methodology and its use for Practitioners, teachers and Students*, Wiley, 2006.

[23] Pallas, F. 2009. *Information Security Inside Organizations-A Positive Model and Some Normative Arguments Based on New Institutional Economics*. Available at SSRN 1471801, 2009.

[24] Friedman, B., Kahn Jr, P. H. and Borning, A. 2006. Value sensitive design and information systems. In *Human-computer interaction in management information systems*: Foundations 5: 348-372.

[25] Inglesant, P. G. and Sasse, M. A. 2010. 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*. pp. 383-392. ACM.

[26] Hart, S. G. and Staveland, L. E. 1988. Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In *Advances in psychology*, 52, 139-183.

[27] Schein, E. 2010. *Organizational Culture and Leadership.* 4th Edition, Jossey-Bass.

[28] Molotch, H. 2013. Everyday Security: Default to Decency. In *Security & Privacy*, IEEE, 11(6), 84-87.

[29] Brotby, W. Krag, and Gary Hinson. 2013. P*ragmatic Security Metrics: Applying Metametrics to Information Security*. CRC Press, 2013.

[30] http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

[31] http://www.iso.org/iso/catalogue_detail?csnumber=42106

[32] Hubbard, D. W. 2014. *How to measure anything: Finding the value of intangibles in business*. John Wiley & Sons.