Learning from "Shadow Security":

Why understanding non-compliant behaviors provides the basis for effective security

Iacovos Kirlappos, Simon Parkin, M. Angela Sasse
Department of Computer Science
University College London
London, United Kingdom
{i.kirlappos, s.parkin, a.sasse}@cs.ucl.ac.uk

***Abstract*—Over the past decade, security researchers and practitioners have tried to understand why employees do not comply with organizational security policies and mechanisms. Past research has treated compliance as a binary decision: people comply, or they do not. From our analysis of 118 in-depth interviews with individuals (employees in a large multinational organization) about security non-compliance, a 3rd response emerges: *shadow security*. This describes the instances where security-conscious employees who think they cannot comply with the prescribed security policy create a more fitting alternative to the policies and mechanisms created by the organization's official security staff. These workarounds are usually not visible to official security and higher management – hence 'shadow security'. They may not be as secure as the 'official' policy would be in theory, but they reflect the best compromise staff can find between getting the job done and managing the risks that the assets they understand face. We conclude that rather than trying to 'stamp out' shadow security practices, organizations should learn from them: they provide a starting point 'workable' security: solutions that offer effective security and fit with the organization's business, rather than impede it.**

Keywords — Information security management; compliance; security design

I. Introduction

Information Security has traditionally been implemented through policies and technical solutions. It was seen as reasonable to secure systems with policies that dictate what users can and cannot do, and technical mechanisms that enforce this [1]. As IT progressively supports more and more activities within the working environment, this approach becomes problematic because policies and mechanisms demand too much effort, and when the effort becomes unreasonable, humans make mistakes or cease to comply [2][3]. Human error and social engineering can be bigger vulnerabilities than many technical attacks [4]. The organization's technical systems must be fortified, yet effective security management needs to consider the physical and social environment in which those technical implementations are used [5][6].

This new environment pushes responsibility for protecting the organization beyond its information security experts: employees - the users of organizational IT systems - play a key role in delivering the policy. Security experts in organizations usually work together in a central function and try to create and maintain a shared sense of appropriate security behavior through policies. They attribute employee non-compliance to lack of understanding. Thus, when non-compliance is detected, they respond with *security education* campaigns, which exhort users to comply with proscribed security mechanisms and processes. But the truth is that almost no organization evaluated whether these policies and mechanisms were fit-for-purpose in the real working environment [7]. In addition, the increasing complexity of the threat makes it difficult to anticipate, define and communicate all desired policy-compliant behaviors for all potential exceptions and circumstances [8]. Thus, the traditional, centralized "command and control" approach to security becomes impossible [9], and we need to rethink of the way information security is implemented and managed. We know that an employee's choice as to whether to comply with security policies is influenced by his/her own task goals, perceptions, attitudes and norms [2][10]. Security design should acknowledge this and develop an approach for a "middle ground" solution that balances employee and security experts' priorities [11].

We suggest that this is where understanding "shadow security"[1] can help: understanding the security practices outside the jurisdiction of the organization, developed by employees who do not willfully disregard security. When security experts insist on 'standard' or 'best practice policies', these users are left to procure, deploy and refine their own solutions, outside the control of the organization's designated security management.

In this paper we present an organizational case study of shadow security behaviors. We analyzed 118 interviews with employees in a large multi-national organization, in which they discussed their security practices. We outline how understanding their practices can improve the process of deploying and refining security in the organization, involving users in the process of evolving security. We argue this is a plausible route to achieving productivity-enhancing, rather than productivity-

USEC '14, 23 February 2014, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2014.23<007>

[1] Shadow IT is defined as: "employees going around IT to get the IT services they want on their own" [12]

hampering information security; a key requirement for getting users involved in shaping the security environment around them is the creation of feedback channels to security professionals.

II. Current State Of Information Security In Organizations

A. Mechanisms, Policies and Communication

To effectively reduce their exposure to security risks, organizations formulate security policies, and implement them through technical mechanisms (e.g. access control, authentication and authorization mechanisms). Based on regulations and international standards (e.g. ISO27000 series) organizations write security policies to communicate security goals to employees, and implement technical mechanisms to enforce behaviors considered necessary to meet those goals. Policies usually reside on an organization's intranet, define the security objectives of the organization, responsibilities of employees and expected behaviors and sanctions in case of non-compliance. Policy content is communicated to employees via leaflets (often given on the 1st day at work) and/or security awareness and education campaigns. This approach may seem plausible, but evidence of widespread non-compliance (from research studies and analysis of security breaches) suggests it is not effective:

1) *It's Impossible to Comply with Policies and Get Work Done:* security mechanisms that are impossible or difficult to use sap employee resources and reduce organizational productivity [13]. Security experts focus on security and attribute non-compliance to user ignorance or willful disobedience [7]. Failure to consider the requirements of the business process, the context and the environment in which human-technology interaction takes place means that, in practice, security gets in the way [13]: all compliance scenarios are essentially treated as the same, regardless of employee role, the sensitivity of information that individuals deal with, or the variance in threat environment as employees move across locations (e.g. home worker, office worker, field worker) [14].

2) *Current Policies are Irrelevant and Burdensome:* Information security policies are supposed to provide employees with a clear understanding of security objectives and responsibilities [15]. Despite their importance as a tool that defines the security expectations of the organization, the current approach to information security policy formulation and communication is mostly reactive, driven by past failures. This concentrates security on protecting the organization from breaches closely resembling prior threats, which can be dangerous in a fast-changing environment where new threats appear day-to-day [11]. There is no systematic approach to make sure policies do not contradict each other, nor is effectiveness of policies evaluated [16].

B. Enactment

When mechanisms and policies do not lead to the desired security behavior security experts respond in two ways: Discipline or persuasion:

1) *The Hard Approach – Discipline:* In theory, breach of security policy is punished with warnings and sanctions. But given the widespread use, monitoring to detect breach of policy is expensive. And given that non-compliance is widespread, an unmanageably large number of employees would have to be disciplined [9]. Sanctions that are not enforced are not an effective deterrent, and heavy-handed enforcement increases tension between security enforcers and the rest of the organization – the scenario first described in *"Users Are Not the Enemy"* [7].

2) *The Soft Approach - Persuasion:* responding to non-compliance with security awareness (of the risks) and training (of correct behavior) can potentially influence employee behavior towards compliance. But if polcies and mechanisms are burdensome and get in the way of productive activity, these attempts are just perceived as 'more time wasted by security' [3]. The associated frustration creates a negative attitude to information security, resulting in any and all communication to be discredited, and discouraging compliance even with mechanisms that do not create high friction – because 'it all adds up'[5][20].

The insight that both current routes do not work ought to focus organization's attention on the root of the problem: that non-compliance springs from the friction between security and productive activity. Employees have no other way to respond to security that gets in the way [8][9]. The workarounds we observed are employees' only way to shaping a security environment that they can work in. The emerging negative attitude towards security, combined with the continuously increasing security risks organizations face [21][22], suggest a need to radically rethink the management of information security to provide effective protection to organizations.

III. Using Non-Compliance to Guide Security Design

Past research on usable security mostly focused on devising principles to design new, bespoke software or systems to fit the requirements of specific work environments (e.g. [23][24]). In addition, the only attempt we are aware of that aimed to characterize security behaviors in the environment in which the interaction of end-users and security happens resulted in suggestions that called for radical redesign of technological solutions, including security from the start of the design process [11]. We have encountered many organizations where replacement is not an option, and have been asked to help them to evolve their security policies and mechanisms. This motivated us to develop a methodology to identify high-friction security and replace it with a solution that provides a better fit with individual and organizational business processes [25].

The first step towards creating such an approach is to identify current non-compliance instances in organizations, the factors that contribute to their occurrence and the employee responses that manifest. Usable security research has touched on this in the past: Bartsch and Sasse [17] identified user responses to unusable access control setups and mechanisms, while Weirich [26] and Inglesant and Sasse [27] articulated the true impact of unusable password policies in organizations. Kirlappos et al. [9] provided a categorization of 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 incentive to exhibit security-conscious behavior.
2. *High compliance costs*: Mechanisms or processes impacting heavily upon productivity leave employees with no other option than non-compliance.
3. *Compliance impossible*: Prescribed behavior could not be followed due to problematic mechanisms; employees resorted to finding other ways to proceed with their primary task.

This previous research has informed understanding how specific security policies and mechanisms for authentication and access control can be changed to fit with primary tasks. Here, we develop a detailed, empirically-founded understanding of shadow security practices, and discuss how security experts can leverage these to develop secure and workable solutions in their organizations.

IV. Methodology

To understand how employees respond to unworkable security with shadow security practices, we analyzed a set of interviews conducted with employees of a large multinational organization. The organization gave us access to their employees, and allowed us to explore employee interaction with - and sentiment toward - their current security policies and mechanisms. This allowed us to identify friction points between security and business processes within the organization that lead to non-compliant behaviors. The interviews were semi-structured and conducted one-to-one by a team of three researchers (including one of the authors). Interviews with individual employees lasted approximately 50 minutes each, allowing for elicitation of a suitably rich representation of the employee experience of security. Participants held various lower-level and lower to middle management positions within a number of organizational divisions, including network maintenance, customer service, marketing, administration, finance, procurement and IT and worked in either a US or UK location. Employees were recruited via the company email newsletter, sent to all company employees - the Chief Information Security Officer encouraged participation and assured that participants would not be identified or followed up. The first 120 responders were scheduled for interview in person or by phone. Participants were given a consent form that described how transcripts would be anonymized and only aggregated results reported to the organization; that they could ask the interviewer further questions about the process and terminate the interview at any point. After the interview, participants were paid the equivalent of $40.

The structure of interviews touched upon aspects of security awareness and compliance, including:

a. What is the employee perception of how security impacts their role? Are they aware of the potential sensitivity of the information they handle?
b. What do employees appreciate in terms of organizational support for security? Are they aware of the existence of security policies and those security mechanisms that they should or could use to protect information and reduce security risks?
c. Where employees exercise non-compliance as a response to shortcomings or frictions in the organizational security experience, what conditions led to those behaviors divergent from organization policy? Are they still conscious about the need for security? If so, what do they do about it?

We did not encourage participants to tell us about security infractions, but simply asked about their awareness of, and experience with, a set of corporate security policies.

Interviews were recorded and transcribed, and a Grounded Theory analysis [28] using *open*, *axial* and *selective* coding conducted, using Atlas Ti. A preliminary thematic analysis by one of the authors produced the non-compliance categorization that is described in Section III and was previously published in Kirlappos et al. [9]. From this emerged that in many cases, employees were trying to act in a secure way even when they were not complying with policies. We decided to conduct a further, more in-depth analysis of those responses.

All three authors coded an initial set of ten interviews and a codebook and related categories were devised. This was then used for the full analysis of all the interviews by one of the authors, which aimed to accurately understand the conditions that lead to the creation of shadow security in the organization. The results of this analysis are presented in the next section.

V. Results

Our analysis identified narratives of employee security behaviors, how the organization environment contributes to non-compliance, and how employees respond. The Grounded Theory categories of non-compliance that emerged fell into four groups: (i) compliance drivers and capacity of employees to behave securely, (ii) shadow security emergence due to high security overheads, (iii) security mediation at team level and, (iv) existence of employee willingness to report security problems, which then appears to be ignored. In this section we frame the emerged categories as narratives using interview extracts that include both *friction causes* (problem with security mechanisms and processes) and the associated *effect* (employee response). We also include a quantitative measure of the number of code occurrences related to each narrative, as identified in the analysis, which indicates the prevalence of the identified behaviors in the organizational environment that was investigated.

A. Employee Compliance Drivers

Contrary to the archetypal view held by security managers, employees appear sufficiently motivated to comply with security and possess some individual capacity to do so effectively. All 118 participants showed awareness of the importance of the information they handle within their role, and the potential consequences of information leaks. 108 participants said they take active measures to protect such information. For example:

P24: *"Some folks in my area have privileged access to customer address information, usage information, that certainly other*

industries and other entities that are interested in selling to our customers would have interest in acquiring and it's part of our roles and responsibilities and ethics requirements that we do not release that information, either for someone else's gain or for our own gain."

Fifty-six participants explicitly mentioned that the main driver for secure behavior was security communication (as we explain later this does not necessarily mean communication from the organization's security enforcers):

P86: "*We've just been told not to mention it on social networking sites, because of the critical importance and the kind of environment we live in now, it's best not to share that kind of stuff. It's just company policy, that's the way they want it.*"

For 15 participants security motivation existed even when they were not aware of an applicable clause in the security policy on the topic:

P112: "*I guess general like not leaving confidential information around on your desks and bits and bobs like that really but I do not know any policies*".

This suggests that, despite some understanding about the need for security being present amongst employees, the organization did not communicate relevant aspects of policy to them (in this case the '*clear desk* 'policy). It also suggests that individual employees try to compensate for perceived gaps in policy.

We found some cases where the environment supported policy, and this had a positive compliance effect. Nineteen participants mentioned that security "piggybacking" on other business processes or imposing minimal compliance cost had lead them to behave securely:

P65: "*the new wing has just been opened up that'll be hot-desks, you won't be able to leave anything out. 'Cause you won't know tomorrow if you're going to sit at the same desk*"

Individual secure behavior was increased by peers who encouraged secure behavior in others: 20 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:

P95: "*I have somebody on my team who likes to change the mouse buttons round and turn your screen upside down if you don't, so you kind of get used to locking your screen when you leave your desk.*"

This willingness to proactively communicate the need to be secure and take action to remind colleagues about it was also present in one participant's reports that they remind their managers about the need to lock their screen:

P116: "*But my line manager was not until I insisted that he locked it.*"

There were also reports that past security incidents act as a reminder for company employees to behave securely. Twenty-one participants mentioned that their awareness of past security incidents affected their perception about the need for security:

P61: *"When I saw some of the recent security breaches, people losing disks and CDs and laptops, things like that. It is something that I'm aware of and do try and minimize what's on there."*

The above example again suggests there is concern for security and employee capacity to behave securely; it also suggests that employees are able to relate security consequences to personal practices, which can act as a motivator to improve their security behavior.

In general, employees appeared motivated to invest some proportion of their time to keep the organization secure. They 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). Individuals also encouraged their colleagues and superiors to behave securely, implying that if security enforcers manage to instill appropriate behaviors in employees, these can then be reinforced across the employee base. In addition, the findings of this section reinforce past research reports that security mechanisms that imposed minimal additional workload have positive effect on employee compliance behaviors [2][9].

B. Effects of Burdensome Security Implementations

Despite recognition of the need to protect the organization and the resulting practices of secure behavior, some employees spoke of security as something that creates significant additional burden to them. The perception of an excessive impact upon the ability to proceed with a business task lead to employees choosing to procure their own - less demanding and less disruptive - solutions to support (what they believed to be more proportionate) security behavior. In the majority of the examples we present here, participants appeared to recognize their chosen action as an insecure approach, but provided some reasoning to legitimize their behavior; either due to compliant behavior constituting an unreasonable draw upon their time, or compliance being regarded as simply impossible. The security burden was variously articulated in terms of time, cognitive load, organizational adaptability, and disruption.

1) *Time:* Time-related problems occurred when employees found themselves in situations where enacting the prescribed security behavior resulted in slower completion of primary business processes (47 participants):

P49: "*You should use an encrypted one but, you know, for ease and generally because, I haven't got an encrypted one so I just use an unencrypted one, whip it across and then just delete the copy off the flash stick which isn't perfect but it's quicker, easier than having to follow the policy.*"

Individuals would then have to find other, lower-impact, ways to proceed with their primary tasks. For instance, problems in the VPN connections led to 12 participants maintaining local versions of active files:

P111: "*At times we do have to transfer the data to our laptops because the network is slow, response times can be really bad and some of the files are quite large so we transfer them to our laptops to work on and then transfer them back at the end of the day.*"

The slow or unresponsive nature of IT support had the same effect. Thirty-eight participants reported that they are at times

forced to derive their own security solutions, due to slow response from IT support, and the processes for configuring secured access to systems proving slow. A demonstrative example mentioned by 13 participants involved employees using the system accounts of other employees to afford access to information, due to the need for immediate access and slow access control setup processes:

P91: "*That does happen sometimes. It's just partly to fill a gap in IS, you know - because we use lots of systems here, and they take ages to set up, and sometimes when someone joins a team, […] he actually only obtained access to the systems about four months later, when he was going to leave, so in the interim time, he was sort of using other people's logins*."

2) *Lack of Adaptability:* A lack of adaptability in the organizational IT systems to account for changing organizational conditions also caused disruption problems. In many cases employees did not have timely access to information necessary for their role, and so had to derive ad-hoc solutions when a problem arose (28 participants):

P97: "*There has been an instance where I have, I was off for a month earlier this year and because of the resolutions were coming through and no-one had an idea what these resolutions or this packs were not being resolved so I gave it to one of my colleagues for him to go to my e-mail to check for the resolutions and that's been the only instance I think.*"

3) *Increased Cognitive Load:* Employees also needed to devise their own security mechanisms when the organisation's password policies produced excessive cognitive load. Thirty-seven participants reported that they felt necessary to physically write down the passwords for system accounts that they rarely used (and as such could not readily recall), then applying security principles to take some action to protect the physical artefact recording the password(s):

P58: "*I have got a list of passwords written down somewhere unfortunately. I just find there's too many to remember otherwise, and we've got a different username and password most of the time for each of each of the logins, so it's written down on a bit of paper."*

4) *Disruption:* In other cases, security restrictions led to disruption of employee tasks; fifty-three participants mentioned that they found themselves in situations wherein security mechanisms were blocking their primary task:

P101: "*Sometimes it can be quite frustrating because you are genuinely waiting for work documents to come in from external sources, and where our security's so tight, some of the documents that we're waiting for can't get into us, so sometimes that can be a hindrance as well.*"

In response to this type of situation, 43 employees reported that they had to resort to other non-prescribed practices:

P2: "*The first trick that was taught to me was you tell them to send it as a different type of file. Change the extension so you can get the file so that you can get your work done*"

Another employee reported he carried two laptops with them, as access restrictions did not permit all of the tasks he needed to complete to be carried out on the same machine:

P88: "*I've got two company computers, one laptop unlocked which allows me virtual areas so that I can install software and use it for technical reasons. And I've got my day to day laptop which is going to be locked up again.*"

The findings in this section indicate that shadow security behavior was caused by security either imposing a prohibitive personal cost, or simply not fitting to the primary task. The alternative security solutions and circumventions derived by employees were driven by their focus on business process.

C. Security Mediation at Team Level

The way security is managed in the organization also contributed to shadow security practices. Managers are directly responsible for managing many security functions within their teams: they take access control decisions, provide security decision support and prescribe behaviors to team members. Sixty-two participants reported that there is a lack of adequate communication about security from the organization, and 57 said security messages are internalized at team level through discussion with their manager or colleagues:

P14: "*One gentleman that works in my group gave us a whole workshop at one of our team meetings, on how to create secure passwords. Not to use your pet's name and your birthday, you know, simple things that people could figure out, like your phone number*."

P96: "*Well basically we were introduced to the security policy through my team leader. He outlined and gave us a site tour of what we can and cannot do.*"…"(in team talks we discuss)…*if we have encountered what we could identify as a security moment it could be like you know a door being left open or your computer left being switched on or not been locked or any sensitive information lying on your desk, to be mindful of putting away security information also using a flash drive which are not company issued and stuff like that really*."

Eighteen participants also reported that their managers provide additional support when they require advice on the sharing of information, both internally within the organization and externally when there's a need to share documents with external partners:

P108: "*...I have got my immediate manager that helps me understand what I need to do and what needs to go out and not.*"

P29: *"I know from my point of view being an analyst. If I were to ever share any information with any priority, even if I was not sure I would first go to my manager and ask him about it.*"

In addition to communication, 29 employees reported that their managers are responsible for access control (authorizing employee access to data) and information management:

P79: "*the manager of each team is responsible for allocating permissions*"

Despite their key role in managing security within their teams, the three managers participating in the study reported that they have had no security training:

"I: *Are you responsible for their security awareness in any sense?*" "P98: *That's an interesting point. That's not something that has ever been particularly made clear to me. I suspect I would take that on board as a normal encompassing responsibility with regards to having people at work for me doing the right thing but I don't recall any specific guideline*"

One manager explicitly reported that the behaviors they prescribe are their personal beliefs (not company directives):

P36: "*You know, because my responsibility is financial, protecting the, the financial data. I, I take it upon myself to make sure that we're staying abreast of what is appropriate, what's not appropriate. What some of the new requirements may be as they're released. Not that I'm aware of.*"

The findings in this section show that the communication, deployment and evolution of security behavior within organizational sub-divisions mostly relies on managers as a conduit. But the organization did not provide adequate support or training to them, which invites the evolution of local, ad-hoc practices, which may divert from the organization's policy. The absence of a consistent security position encourages independent action on managing security at team level; shadow security is seen to be implicitly permitted by the organization and explicitly by the team manager. The result are ad-hoc practices (P118: "*not policy, my own best practice*"). This results in inconsistent communication, knowledge and interpretation, in effect fostering many differing security behaviors within the same organization.

D. Employee Feedback Goes Unnoticed

In many ways, perceptions of the organization's existing security implementations, as elicited from employees, indicate where they believe the organization has failed to provide them with 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 19 participants expressed concerns to that effect:

P109: "*There is five or six people that have since left the business or, have gone elsewhere in the business but that they have the password*."

Despite some employees taking action and reporting perceived security problems, 8 participants reported that to them it seems that their reported concerns go unnoticed:

P53: "*I've raised security issues and you never get anywhere with them. I raised the issue of memory sticks, I also raised an issue where I had a contractor came to work for the company and he was given a laptop. And it belonged, it had belonged clearly to one of the directors and it had all his information still on it. [..] You were still made to do it and you could, sort of, flag your reservations up but they wouldn't be listened to*",

and 13 others reported that they saw no attempts to improve the current organizational security implementation:

"*I: So, which way would you say the culture is moving? Is it that, security is getting tighter, or it is weakening?*", P110: "*To be honest from day to day things, I do not really see it moving to be honest."*

There appears to be a general perception amongst employees that the organization demands security but does not listen to feedback, and does not respond in an adequate or timely manner when shortcomings are identified. This validates employees who adapt security in their own way when an alternative solution is needed.

VI. THE EMERGENCE OF SHADOW SECURITY

The shadow security practices we identified represent the sum of self-made security measures created by productivity-focused employees when the organization's existing security implementation does not meet their needs. Rather than remaining passive, employees, peer groups, and managers who have their own understanding of security, individually or collectively devise their own adaptations to unsatisfactory security measures or introduce their own novel solutions. These are perceived by employees as serving the purpose of maintaining security. Isolated from the security division, the alternative solutions deployed are based on their own understanding of what the security experience should be like. But often, shadow security practices do not manage the organization's risks adequately.

Security communication emerges as dysfunctional; there is limited awareness of the existence of security policies and formal procedures. Employees are willing to report problems and suggest better solutions, but there is no effective feedback channel for this purpose. In reality, key stakeholders in the organization (line managers, for instance) are 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 more. Security measures that reduce productivity cause disgruntlement: individuals refuse to accept the interference with their primary task, on which they are ultimately judged. They accept the need for security, but security that does not fit forces them to develop their own solutions. Without security management actively soliciting feedback from employees to identify security-productivity friction points and subsequent employee responses, the security of the organization becomes that which managers and employees - assumed non-experts in security - consider to provide the best fit for their business processes.

VII. RISKS TO THE ORGANIZATION

Whilst it is understandable that employees resort to a "Do It Yourself" approach to security, turning a blind eye harbors a number of potential risks for the organization:

- It creates a false sense of security: employees believe they are protecting the organization, but their understanding of the risks the organization faces can be incomplete or inaccurate (e.g. "*I delete data from unencrypted USB drive*"). As a result they develop their own rationalizations of how to manage security. This approach can potentially be effective if employees are significantly aware about security related risks or happen to choose actions that protect the organization, but any security management approach based on ad-hoc solutions devised in isolation by employees may fail to reflect the actual risks the organization faces: employees cannot be assumed to be security experts.

- In some cases, procured solutions force employees to reshape their primary task to adapt to badly designed security (e.g. "*I carry two laptops*"), instead of security adapting to the task. This can quickly exhaust the employee's *compliance budget* [2]: in a situation where the perceived cost is too high (e.g. a need to travel regularly with two computers instead of one), employees' response may be insecure (e.g. travel with the one laptop that has the widest possible access and perform all tasks on it [29]).
- Ineffective communication of policy to managers - those best-placed to convey behaviors to employees - can lead to the development of varying security "micro-cultures" in smaller teams. Without appropriate training, managers cannot be assumed to be sufficiently aware of the policy and also lack an overview of the security risks that exist within the organization. As a result, managers can only communicate to employees what they themselves believe is important about security at the time and, like employees, they cannot be assumed to be security experts. This can result in divergent behaviors developing, out of the organization's control, rendering the organization vulnerable to insecure employee behaviors that can become common practice.
- The divergence of behavior across different teams provides freedom for the development of team security folk models [30], which are reinforced by both team managers and team members. This can act as an additional level of resistance to attempts by the organization to change employee behaviors and account for divergence from prescribed behaviors or current mechanisms when a good reason for it exists.
- "Hard" technical solutions that the organization refuses to change or replace may prevent shadow security practices from developing, but cause disgruntlement. This can lead to further alienation of users, adding to any existing user-security divide [20], and compounding resistance to centrally-dictated expectations. The identified lack of a response from security to reported employee security concerns (as in Section V.D., P53) can accentuate this divide: if employees resort to shadow security practices, this may indirectly serve to reduce their frustration with security.

VIII. Lessons From Shadow Security

While shadow security practices persist, the organization has an inconsistent security posture which does not align with its productivity goals. However, the existence of shadow security also suggests the presence of a latent capacity for users to appreciate and play an active part in the provision of security, albeit driven by their internalized sense of what security should achieve for the primary task. Employees deploy their own security solutions when they believe a required "affordable" policy or infrastructure is missing, instead of doing nothing or passively relying on the organization to remediate. Security experts should be aware of this individual capacity and the potential for employees to consciously consider security in their activities. Shadow security can inspire more workable security implementations that align with productivity objectives, provide effective protection, and minimize security overhead.

In the remainder of this section we discuss four specific aspects of the organization and its approach to security, where the identified shadow security practices can be used as a leverage for improvements: (a) Reduction of the complexity of mechanisms and processes required for compliant behaviors, (b) Engagement with users in rationalizing the current security implementation, (c) Attention to the assessment of the suitability of proposed security solutions, and (d) Training and participation of managers in guiding security decisions. These areas are related closely to the experiences of individuals within the partner organization, and specifically examples where significant friction between security and the primary task led to the development of activities that can be characterized as shadow security.

A. *Reducing Compliance Costs*

We learnt 15 years ago that organizations with unusable security mechanisms are not effectively protected, because error and workarounds create vulnerabilities [7]. We have since learnt that a high level of non-compliance creates noise in which signs of attacks are hard to detect [2], and people just ignore security advice that requires high effort for little benefit [3]. But our results show there has been little progress in identifying and removing 'ill-fitting' security policies and mechanisms: organizations still do not track the effort that individuals have to expend on security. Burdensome or disruptive security implementations promote shadow security - users create their own workable security solutions. Security experts need to acknowledge that effective security can only be achieved by if it fits and supports, rather than hinders, productive activity. The increasing decentralization of modern IT implementations means that security challenges need to be solved in a decentralized, cooperative way [31]. This requires a move away from 'standard' and 'best practice' solutions for managing a security risk, to a participative approach that works with users to understand where and how security can fit in the productive activity that users are focused on.

B. *Engagement of Users in Security Design and Effectiveness Assessment*

The capacity of users to participate in security can provide leverage to create new, seamless security solutions that are better aligned with their primary tasks. As previously discussed, users do not dismiss security, but act concoct "more appropriate" security solutions when they encounter unworkable security. Employees rationalize their experience with security, and these rationalizations may not necessarily be those that the security experts expect [32]; but these rationalizations dictate how individuals interact with IT security, and the value they see in compliance. Stochastic models have shown that more effective security solutions can at times be counterintuitive to entrenched wisdom [14][33]. Organizations may choose to accept that employee responses happen naturally. In this way, (i) employees are the first indicator if security solutions are not serving the business, and (ii) security management must determine a strategy for engagement with security needs and the associated two-way dialogue with users. Security should not indirectly promote shadow security simply through

lack of proper channels for remediation. Where shadow security practices occur, contributory factors can and should be analyzed and leveraged to improve organizational security.

To reduce the likelihood of shadow security developing in the first place, users can be involved in security design as an integral part of the process. The importance of involving users in systems design was first identified by Checkland et al. [34], and the value of participatory and contextual design is widely accepted among developers. But this approach is still not adopted in security, with a few exceptions [32] in the formulation of authorization policies. A participatory security design approach includes representation of users' tasks – and this knowledge can be used to find a low-friction solution that does not compete for users' attention or effort, disrupts productivity activity, or leads to errors. It also helps to identify security goals and values [35] – as this study shows, employees do try and protect organizational assets against risks they understand. Many security experts still talk (and think) that usability and security create a tradeoff: that usability is nice, but security is important, so it's ok to ask users to make extra effort. But usability is a *hygiene factor* for security: solutions that are not usable will not work as intended, period. At worst, users will become disgruntled and see security as obstacles to scoot around. At best, security-conscious users will create a shadow security solution that is workable as far as they are concerned, but may not manage organization risks effectively. 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 ways for the organization to improve (e.g. Section V.D., P53, P109). All this constitutes valid and useful feedback (even without recognizing employees as security experts), which could be repurposed to improve the organization's security posture [31].

C. Deploy, then Measure

Organizations need to measure the impact of security on employees and productive activity, and keep monitoring it. Currently there is no post-deployment assessment of the impact of deployed security mechanisms on business processes; a lack of complaints may be seen as proof that everything is well, but, as the manifestation of shadow security reveals, silence does not mean security is working as the organization has specified. Regular assessment of the suitability of systems would turn security management into an iterative process, moving away from a static, "fire and forget"[2] approach. For example, the introduction of a new business system that requires password authentication adds one more credential to the cognitive load placed upon users (Section V.B. P58); this 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) [27] – user reaction to such a process can only be accurately assessed after deployment.

D. Management Training – Recognise the Importance of Low- and Middle-Management in Security

Security is a collective achievement [36] and managers are participating in it in many ways: employees turn to them for support regarding their security decisions; they make local - and potentially ad-hoc - decisions about access control and information sharing, and they prescribe and moderate security behavior amongst their team members, thus contributing to the evolution of shadow security practices. Security awareness and behavior amongst managers is thus important: employees listen to and follow their managers' behavior [37]. Security management needs to understand that any security awareness or education they broadcast will be interpreted and mediated locally. They need to be aware of this, and (1) listen to managers' questions, problems and concerns, and (2) help them to develop correct and consistent security advice about security. If organizations neglect to do so, managers and their teams will continue to create their own rationalizations as to what their interactions with IT-security mean, and how to achieve their ultimate goal: to proceed with their primary tasks with minimal damage on the organization's security. Security-specific training should be tailored for managers to acknowledge their role as mediators of security - instead of being overloaded with security knowledge, training for managers can consider organizational goals and organizational security principles. In this way, when individuals consult their managers, they are more likely to design novel solutions that account for the risks faced by members of the team. In addition, managers of small teams interact much more frequently with employees and have a unique perspective of the frictions between security and productivity tasks; soliciting feedback from them can contribute to an effective amalgamation of shadow and prescribed security practices.

IX. Conclusion

User reaction to an organization's security implementation needs to be heard, lest it weaken the organization's security posture: 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. 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. Essentially, shadow security should be treated as an opportunity to identify shortfalls in current security implementations and their effects on the organizational environment, to be leveraged in providing more effective security solutions for organizations.

X. Future Work

The identification of shadow security creates a number of future research challenges. To determine if shadow security

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

practices can be leveraged within a holistic security management process, we are currently conducting similar analyses on additional sets of interviews from two further organizations, and are negotiating deployment of solutions - informed by identified shadow security behaviors - within partner organizations. This will allow deployment of security solutions informed by shadow security behaviors and assessment of their real-world effectiveness.

We also agreed with a partner organization to conduct further interviews and in-depth analyses studying the rationale 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. P49 on use of unencrypted USB sticks, was the participant aware that simply "deleting" unencrypted files does not stop an attacker from recovering them from the flash drive?). 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.

XI. ACKNOWLEDGMENTS

The authors are supported in part by UK EPSRC and GCHQ, grant nr. EP/K006517/1 ("Productive Security") and the EPSRC-funded UCL SECReT Doctoral Training Centre.

We thank IT security managers at our partner organizations for facilitating the interviews with employees and Philip Inglesant and Simon Arnell for conducting some of the interviews.

We also thank our USEC shepherd, Sameer Patil, for comments and guidance.

REFERENCES

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

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

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

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

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

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

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

[8] G. Stewart and D. Lacey. "Death by a thousand facts: Criticising the technocratic approach to information security awareness". Information Management & Computer Security, 20(1), pp.29-38, 2012.

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

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

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

[12] M. Settle. "Shadow IT: Are you solving the problem or just policing it?" BMC Software, 2013.

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

[14] A. Beautement, R. Coles, J. Griffin, C. Ioannidis, B. Monahan, D. Pym, M. A. Sasse, M. Wonham. "Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security". In Managing Information Risk and the Economics of Security. pp.141-163. Springer US, 2009.

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

[16] F. Björck. "Security Scandinavian style". PhD diss., Stockholm University, 2001.

[17] S. Bartsch and M. A. Sasse. "How Users Bypass Access Control - And Why: The Impact Of Authorization Problems On Individuals And The Organization". ECIS 2013: 53

[18] M. G. Morgan, B. Fischhoff., A. Bostrom., and C. J. Atman. "Risk communication: A mental models approach". Cambridge University Press, 2001.

[19] C. C. Wood. "An unappreciated reason why information security policies fail". Computer Fraud & Security, (10), pp. 13-14, 2000.

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

[21] PWC, "UK Information Security Breaches Survey Results", 2012.

[22] GRT Corporation, "British Intelligence Speaks Out On Cyber Threats", 2013.

[23] I. Fléchais, C. Mascolo and M. A. Sasse. "Integrating security and usability into the requirements and design process". International Journal of Electronic Security and Digital Forensics, 1(1), pp.12-26, 2007.

[24] S. Faily and I. Fléchais. "A meta-model for usable secure requirements engineering. In Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems (pp. 29-35). ACM, 2010.

[25] T. S. H. Teo and W. R. King. "Integration between business planning and information systems planning: an evolutionary-contingency perspective". In Journal of management information systems, pp.185-214, 1997.

[26] D. Weirich. "Persuasive Password Security". Doctoral dissertation, University College London, 2005.

[27] P. G. Inglesant and M. A. Sasse. "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, 2010.

[28] A. Strauss and J. Corbin. "Basics of qualitative research: Techniques and procedures for developing grounded theory". Sage Publications, Incorporated, 2007.

[29] A. Sasse, "A Tale of two laptops", Personal communication, 2011

[30] R. Wash. "Folk models of home computer security". In Proceedings of the Sixth Symposium on Usable Privacy and Security, p. 11. ACM, 2010.

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

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

[33] S. Arnell, A. Beautement, P. Inglesant, B. Monahan, D. Pym, and M. A. Sasse. "Systematic Decision Making in Security Management Modelling Password Usage and Support". Presented at the International Workshop on Quantitative Aspects in Security Assurance. Pisa, Italy, 2012.

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

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

[36] P. Dourish and K. Anderson. "Collective information practice: exploring privacy and security as social and cultural phenomena." Human-computer interaction 21 (3), pp.319-342, 2006.

[37] M. E. Johnson and E. Goetz. "Embedding information security into the organization". Security & Privacy, IEEE, 5(3), 16-24, 2007.