Appropriation of security technologies in the workplace

Simon Parkin, Kat Krol
University College London, London, UK
s.parkin@ucl.ac.uk, k.krol@cs.ucl.ac.uk

Abstract. Using two case studies, we examine the appropriation of security technologies by employees in organisations. We find that employees adapt security technologies and procedures in many different ways, and that the implications of adaptation for employees' productive tasks and the wider organisation are not considered in process. We want to understand how appropriation within technology use can be observed, so that organisations can reconcile unanticipated security adaptions with standard practices. Based on lessons learned from studies of security technologies in organisations, we identify areas of focus where appropriation activities could inform the design of organisational security: individual security context; interpersonal dynamics, and; training and support.

1 Introduction

Employees in organisations have primary production tasks and secondary tasks, where security activities – such as authenticating to a company computer – are a secondary task that supports a business process (Fléchais et al., 2007). Employees do not go online primarily to create complex passwords and query the authenticity of phishing emails – these are secondary tasks intended to make communication, collaboration, and sharing more secure (for both the individual and the organisation).

Within large organisations, secondary security tasks constitute security responsibilities, defined in a central security policy and mediated by provisioned systems that have integrated security controls (e.g., password-protected access, access cards, email filters). Where the design of these systems does not adequately consider the

fit of security with the primary task, compliance with security policy and expected use can become burdensome. Users may seek some other means to complete their security tasks, by using coping strategies (e.g., writing down passwords) or by developing workarounds (Beautement et al., 2009). This can include routines enacted pre-emptively to ensure access to critical resources or to avoid negative outcomes such as embarrassment. Even where employees maintain compliance, they may grow increasingly disgruntled, or abandon use of provisioned systems.

Security usability research has exposed many ways in which users – rather than remaining idle – will adapt available technologies to meet their needs (Kirlappos et al., 2014). Where appropriation happens, it is either as a deliberate attempt to shape security to better fit the primary task, or unwittingly without the intervention or support of the organisation's security function.

Employees using security technologies in organisations are rarely security experts, and research has demonstrated how users develop folk models of security and perceived risks, warping the expectations, use and perceived need of security technologies (Wash, 2010). And yet, security effort is pushed to the end-user (Sasse, 2015), such that users who do not have appropriate security knowledge turn not to the organisation for support but to colleagues (Kirlappos and Sasse, 2015).

Lab-based evaluation of technology usability tends to position a knowledgeable researcher with a participant, controlling use of the technology so that no errors occur (e.g., clearly explaining a new authentication mechanism, and guiding the participant to use it in the expected way (Krol et al., 2015a)). In this way, examining a technology in isolation can determine the effects of normal, non-erroneous use to assess user and technology performance. This does not however serve understanding of how an individual in an organisation appropriates a security technology, and how the primary task or unanticipated events influence this process (such as the perceived value of a protected asset or primary task output, or the individual response to errors). Such an understanding could inform regular oversight activities for organisations as they deploy and manage security technologies. Here we explore how to study the appropriation of security technologies, towards shaping these oversight activities.

2 Examples

Here we explore how security technologies have been deployed in organisations, and have led to appropriation activities by employees (both expected and unanticipated) as a means to complete primary tasks to their satisfaction. Examples are derived from studies conducted within our research group that explore the tensions between primary tasks and the use of secondary security technologies.

In Example 1 (authentication to services and devices), diaries were maintained over a period of 24 hours, which captured perceptions around events as they occurred, within a structure defined by researchers, and with a focus on a specific set of events. Subsequent interviews shed light on diary entries, to understand the contexts in which authentication happened. In Example 2, issues with access con-

trol for file-sharing were exposed as part of semi-structured one-to-one interviews, where employees self-reported challenges in using security technologies, guided by researchers through follow-up questioning.

2.1 Example 1 – Authentication to Organisation's Systems

In a study by Steves et al. (2014), 23 knowledge workers in a large US governmental organisation were asked to log all their authentication events for the period of 24 hours and were subsequently interviewed about their authentication experiences. The study uncovered that having to log in to the organisation's systems significantly increased employee workload and in particular, re-authenticating after time-outs and having to use 2-factor authentication contributed to an authentication fatigue. The authentication burden was disruptive to employees' natural workflow, caused frustration and meant they were less likely to – for example – respond to their colleagues' emails from home or while travelling.

This high authentication effort led participants to develop a number of coping strategies that allowed them to manage their workload. Some reported giving up on devices to limit the authentication effort which is a case of disappropriation as explained by P12 *"I don't have a laptop [. . .] one of the reasons why I gave up the laptop was the password thing for the SafeBoot. I had all kinds of trouble with that, but that's another story. [. . .] that was one of the reasons why I didn't want to deal with the laptop anymore because I could not remember my SafeBoot code."*

One of the most common coping strategies for dealing with authentication was for participants to store their passwords in a password manager or in the browser. P5 explained that this contributed to them being able to appropriate different communication tools: *"that was a surprise, realizing that almost every authentication I made was actually stored somewhere for me. And I couldn't live without that. If I had to truly authenticate every single time I went in to check my e-mail or every single time I wanted to log into – well, mainly e-mail. Email's a big one, or instant messenger or something like that. I wouldn't do it as much. I wouldn't use three different instant messenger clients, you know – Yahoo! and AOL and G Talk. I wouldn't use them all. I would really limit myself."*

2.2 Example 2 – Secure File-sharing in an Organisation

Bartsch and Sasse (2012) looked at secure file-sharing – using shared folders and filespaces – in a large organisation. They conducted a set of 118 semi-structured in-depth interviews with employees in management roles, focusing on their experiences with the security policy, and how it affected the primary tasks.

Interviewees reported failings in the authentication systems, manifesting as restrictive policies and over-entitlements. It was difficult to make access policies workable, and change requests required a significant lead time before coming into effect. Those requesting changes then felt forced to circumvent the authorisation measure, or otherwise felt deterred from requesting permissions changes in the first

instance. Activity then moved outside of the view of the security function, for example to the use of email to share information. Support procedures were unknown or known not to help, increasing the perceived effort – alternative solutions were then indirectly encouraged and yet not supported by the organisation.

Many stakeholders were involved with managing access policies, including managers, technical operatives, and personal assistants. A high-level security policy did not define who could access what, indicating that expectations of users and use were not anticipated, and making it difficult to enforce appropriate restrictions. Decisions were then taken without adequate consideration of the wider consequences, leading either to over-entitlement or restrictive policies. Some decisions were based on formalities rather than the nature of the request, for example having a user demonstrate that they had completed specific training. There also was an emotional cost when requests were denied, illustrating how the design of the system was failing the user.

A number of interviewees reported that issues with authorisation processes lead to circumvention of the system. Documents were being sent by email, thereby appropriating the existing electronic communication system for file-sharing purposes. Users were found to be using other provisioned technologies within the system (multiple accounts with different access privileges) or outside of it (storing documents on physical media, signifying activity unobservable by the organisation). Social circumvention was also employed, for example, sharing passwords with coworkers (co-opting them as unanticipated users).

3 Discussion

The example studies have incidentally exposed a number of triggers for adaptation, barriers for adoption, and the capacity of individuals to shape existing technologies to serve an emerging security need. Here we wish to determine where appropriation occurs in organisations, in the face of compliance expectations and a complex, changing business environment. Policy, technology, and process change regularly, and do not always move in step with each other, where individual action to adapt technologies supports the continuation of business processes (Kirlappos et al., 2015). When provisioned systems, recovery processes, and guidance are unsuitable, they encourage this appropriation.

There is potential for organisations to learn from emergent appropriation activity in a systematic and repeatable manner, to moderate the technologies, training materials, etc., that users are exposed to, and to craft technologies to support business tasks. From our examples and the work described in the Introduction, we have identified the following areas of focus for organisations:

- **Respect Individual Security Context**: Perceived workload and risk perception inform the emergence of coping strategies and workarounds. The need to appropriate may be anticipated by the user (e.g., re-using an existing password for a new system). Disappropriation may occur in response to the complications of applying a particular technology to a business task, where some

security solutions may not fit at all with working practices or policy (Kirlappos et al., 2013).

- **Support Interpersonal Dynamics**: Teams have a role in the development of security behaviours (Kirlappos and Sasse, 2015), including the sharing of security effort, development of ad-hoc solutions, reporting and resolution of problems, and management of local security expertise. Security technologies may then be used by groups in ways that the recognised security team in the organisation did not anticipate, to support primary tasks that are not directly understood by anyone outside of the group and which may introduce unanticipated risks. However, collaborative appropriation activities may be fed back into policy to benefit the wider organisation, where groups use similar technologies or experience similar pressures.
- **Target Training and Support**: Users need time to learn a technology or commit a credential, routine, or element of training to memory. The settings in which habituation and skills develop are also dynamic – appropriation may occur in isolation, under supervision, or during times of stress. It may be possible to identify the critical steps in becoming familiar with a new security technology, where experiences of seeking support – due to failure or a need to recover a situation – can inform ad-hoc responses or reinforce learned strategies. There may be points in the process where training and support can be best placed to assist the end-user. Assistance would be important to recover from one-time mistakes that weaken security, or reshape learned behaviours that are not secure.

The work described in the Examples captures post-adoption. The aim of this work is to explore which aspects of appropriation can be actively identified and measured in the system as they arise, through dialogue with employees and security managers, and through observation. Appropriate research methods will be developed to capture both the leading indicators of appropriation and disappropriation (such as disgruntled of overburdened employees), and the implications of post-adoption. Study of the appropriation of security technologies can begin with a range of socio-anthropological studies of the workplace (as seen for example for public transport systems (Molotch, 2013)), with attention to the use of security technologies and how observations can be applied to improve system design. The complexities of monitoring the fit of security to tasks over time, altering system design, and enacting changes can subsequently be considered as regular activities for the organisation. This may be one route for organisations to capitalise on users' appropriation activities to weather changes in both the business and security environments.

4 Future Work

Although the examples described here relate to use of security technologies in organisations, it is desirable also to examine appropriation of security technologies in peoples' personal lives. Our research group has started conducting research in

this direction, with a study looking at 2-factor authentication technologies for online banking post-adoption (Krol et al., 2015b). One of the main findings was that participants conducted banking and used banking tokens and apps in many different ways, where analysis suggested that users may be given choice as to what technology they use, based on personal preferences. These findings are useful for understanding the expectations of tech-savvy employees as they join organisations, or where organisations consider Bring Your Own Device (BYOD) policies. Individuals may transfer coping strategies learnt in one context to another with varying results, or conflate mental models of security and risk (with the potential to add complexity to their behaviours).

References

Bartsch, S. and M. A. Sasse (2012): 'How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization'. AIS Electronic Library (AISeL) / Berkeley Electronic Press.

Beautement, A., M. A. Sasse, and M. Wonham (2009): 'The compliance budget: managing security behaviour in organisations'. In: *NSPW 2009*. pp. 47–58.

Fléchais, I. et al. (2007): 'Human Vulnerabilities in Security Systems'. Human Factors Working Group White Paper Cyber Security KTN Human Factors White Paper.

Kirlappos, I., A. Beautement, and M. A. Sasse (2013): "'Comply or Die" Is Dead: Long live security-aware principal agents'. In: *Financial Cryptography and Data Security*. Springer, pp. 70–82.

Kirlappos, I., S. Parkin, and M. A. Sasse (2014): 'Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security'. In: *USEC 2014*.

Kirlappos, I., S. Parkin, and M. A. Sasse (2015): 'Shadow security as a tool for the learning organization'. *ACM SIGCAS Computers and Society*, vol. 45, no. 1, pp. 29–37.

Kirlappos, I. and M. A. Sasse (2015): 'Fixing Security Together'. In: *USEC 2015*.

Krol, K., C. Papanicolaou, A. Vernitski, and M. A. Sasse (2015a): "'Too taxing on the mind!" Authentication grids are not for everyone'. In: *HCI International 2015, HAS*.

Krol, K., E. Philippou, E. De Cristofaro, and M. A. Sasse (2015b): "'They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking'. In: *USEC 2015*.

Molotch, H. (2013): 'Everyday Security: Default to Decency'. *Security & Privacy, IEEE*, vol. 11, no. 6, pp. 84–87.

Sasse, A. (2015): 'Scaring and Bullying People into Security Won't Work'. *Security & Privacy, IEEE*, vol. 13, no. 3, pp. 80–83.

Steves, M., D. Chisnell, M. A. Sasse, K. Krol, M. Theofanos, and H. Wald (2014): 'Report: Authentication Diary Study'. National Institute of Standards and Technology (NISTIR) 7983.

Wash, R. (2010): 'Folk models of home computer security'. In: *SOUPS 2010*.