Incorporating Social Trust into Design Practices for Secure Systems

Piotr Cofta, BT (British Telecom), UK
Hazel Lacohée, BT (British Telecom), UK
Paul Hodgson, BT (British Telecom), UK

ABSTRACT

Companies are increasingly dependent on modern information and communication technology (ICT), yet the successful adoption of ICT systems stubbornly hovers at only around 50%, adding disappointment to business losses. Trust (both inter-personal and technology-related) has significant explanatory power when it comes to technology adoption, but only as part of a systematic methodology. Therefore, understanding more fully the interaction between human process and technology by adding the richness of socio-technical considerations to the design process of ICT systems should significantly improve adoption rates. At the same time, trust-based design has to demonstrate the (often neglected) business value of trust. ‘Designing for trust’, discussed in this chapter, is a design framework that consolidates trust governance and security management. Trust governance is a complete proposition that makes trust relevant to business practices, including the design and deployment of ICT systems. Trust governance incorporates the business justification of trust with an analytical framework, and a set of relevant tools and methods, as well as a maturity model. This chapter discusses how ‘designing for trust’ leverages trust governance into the design practices of ICT systems by complementing security-based methodologies, demonstrating the value of this approach.

1. INTRODUCTION

Throughout their industrial experience, the authors have seen several examples of systems where security suffered due to a lack of proper consideration for the complexity of an inter-play between technical systems and their social environment. Further, the authors can see that even within the confines of a large technical system, its security depends not only on purely technical measures or mastery of technical designs, but also on the ability and willingness of design and support personnel to engage at a deeper level. The authors’ current work concentrates on improving industrial practices, using elements of a proposition presented here.

In the continuous fight to improve on offerings and decrease costs, companies are increasingly dependent on complex information and communication technology (ICT) systems. While the design and deployment of such systems represents a challenge in itself, the fact is that up to 50% of those systems do not live up to their original expectations (Lippert & Davis, 2010).
adding frustration and damaged reputation to lost investment and missed revenues.

While analysing the reasons for such a lack of success, it is apparent that failures can often be attributed to the lack of social adoption of such new systems. This lack of adoption often originates in inappropriately designed and applied security measures (Cranor and Garfinkel, 2005), that are either too lax (so that they expose vulnerabilities) or too stringent (so that they inspire creative rejection), or finally, they may be appropriate in strength but entirely ignore established practices. Note that quite often such security measures are designed in full accordance with requirements or specifications, yet they miss the importance of the social context of practical application (Lippert & Davis, 2006).

A system that fails to achieve adoption represents a business loss, but a system that is not fully or willingly adopted represents a significant security vulnerability, specifically if users of such a system are set to circumvent security controls by means of creative social practices. For example, even the most sophisticated access control does not provide security if users choose to use their access cards according to their perception of social relationships (and value systems) rather than according to security policies (Collins, 2007), or if a PIN code for a credit card is shared (Lacohée, Cofta, Phippen, and Furnell, 2008).

This phenomenon of ‘unintended consequences’ can be best described in terms of affordance, coined by Gibson (1986) and popularised in the field of HCI and design by Norman (1988) who applied the concept to everyday artefacts. Norman defined affordance as “the perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used.” Affordance, therefore, determines what an ICT system can be used for, following the intentions of its users, while specification and design concentrates on how the system is intended to be used by its original designers. The disparity between both intentions creates tension that eventually undermines system adoption.

While the ‘answer’ to such ‘user challenges’ of ‘unintended consequences’ may lie partly in better education, improved usability or more stringent supervision, the underlying truth is that the deployment of an ICT system is a cause and enabler of a planned change (Lippert & Davis, 2006) that should be designed with its immediate social environment in mind. Successful technologies owe a large part of their success to the fact that they fulfil or enhance an existing human need, or fit well into an already well established social context. In common with other types of change, any unsubstantiated demand that requires a radical change of social practices will be met with rejection and creative re-use or even abuse. Therefore, a successful socio-technical approach to design should take into account social relationships and practices that surround a given system, leading to improvements in acceptance rates.

Considering established software development practices, best design practice (Anderson, 2001) stresses that features such as security should be designed into the system as early as possible. This is corroborated by general observations that changes in the design stage can be made easier, faster and cheaper than changes undertaken later in the system’s lifetime (Boehm, 1981). Such approaches are well accepted and there are existing tools and methodologies to support them (e.g. Mouratidis & Giorgini, 2007). However, addressing security alone does not allow for the proper modelling of relationships between social agents and relationships between such agents and technology, where assurance can be resolved by means other than control.

Adding the richness of social considerations (specifically the notion of affordance) to the design process of ICT systems should therefore significantly improve design considerations, thus decreasing potential security vulnerabilities as well as improving system adoption. It has been identified that trust (both inter-personal and technology-related) has significant explanatory power when it comes to technology adoption (Lippert & Davis, 2006).
Technology: A Bane or Boon for Cross-National Levels of Generalized Trust?
Blaine G. Robbins and Maria S. Grigoryeva (2010). *Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives*  (pp. 123-144).
www.igi-global.com/chapter/technology-bane-boon-cross-national/42904?camid=4v1a