Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Power to the people? The evolving recognition of human aspects of security

Steven Furnell, Nathan Clarke*[1]

Centre for Security, Communications & Network Research, Plymouth University, Plymouth, United Kingdom

ARTICLE INFO

Article history:
Received 18 March 2012
Accepted 15 August 2012

Keywords:
Human aspects
Security awareness
Usability
Antivirus
User authentication

ABSTRACT

It is perhaps unsurprising to find much of the focus in IT and computer security being drawn towards the technical aspects of the discipline. However, it is increasingly recognised that technology alone cannot deliver a complete solution, and there is also a tangible need to address human aspects. At the core, people must understand the threats they face and be able to use the protection available to them, and although this has not been entirely ignored, it has not received the level of attention that it merits either. Indeed, security surveys commonly reveal that the more directly user-facing aspects such as policy, training and education are prone to receiving significantly less attention than technical controls such as firewalls, antivirus and intrusion detection. The underlying reason for such disparity is that the human aspects are in many ways a more challenging problem to approach, not least because they cannot be easily targeted with a product-based solution. There is also a direct overlap into the technical area, with issues such as the usability and acceptability of technology solutions having a direct impact upon the actual protection that they are able to deliver.

This paper explores these themes, highlighting the need for human aspects to form part of a holistic security strategy alongside the necessary technologies. Taking the specific examples of security awareness and two user-facing technical controls (user authentication and antivirus), the discussion examines how things have evolved to the present day and considers how they need to be positioned for the future.

1. Introduction

In spite of the implied focus upon technology, achieving IT security is more than just a technical problem, and increasingly involves the active participation of people in order to securely design, deploy, configure and maintain systems. Whilst the level and sophistication of this interaction may vary, anyone who is engaged with technology, from administrators of the most complex of IT systems to owners of simple devices, all need to make decisions that have an impact on the security and privacy of their device and information.

Unfortunately, while people represent a key element in achieving security, they are often the point of failure. With security now impacting all aspects of society, from young to old, from organisation to individual, it is imperative that systems are designed and policies are put in place that assist people in ensuring the security of their systems. Although the security scene is still dominated by attention towards technological solutions, we are now seeing an increasing

* *Corresponding author*. Tel.: +44 1752 586222.
E-mail addresses: sfurnell@plymouth.ac.uk (S. Furnell), nclarke@plymouth.ac.uk (N. Clarke).

[1] Tel.: +44 1752 586222.

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.08.004

emphasis on human aspects. This article takes a reflective stance to examine how the situation has changed over the years, to the point we are now seeing today, with human issues receiving far more explicit recognition than they did in the past. It also identifies that further developments are still required, in terms of both the security culture that is created amongst users and the tools that they are given to support it.

2. The evolving importance of human aspects

It has long been recognised that security is a human issue and that people can represent a significant part of the problem. Indeed, numerous surveys across the years have highlighted that user actions, both deliberate and accidental, are often ranked closely alongside the more readily recognised threats of malware and hacker attacks. However, what has only started to receive more widespread recognition more recently is the role and importance of people as part of the *solution*.

In order to address the human aspects of security it is necessary to consider both the related threats (such as IT misuse and social engineering), as well as people-focused safeguards (such as the establishment and promotion of policy, security awareness and education, and the usability of security technology). Some of the categories decompose further. For example, usability will encompass a range of further issues (such as interface design, software performance, the level of task automation, and cognitive demands placed upon the user), all of which will influence the resulting ease-of-use that is perceived by the user.

Of course, many of the human factors are by no means completely distinct from the technology, and in many cases can represent the deciding factor in whether or not it is actually used *effectively*. Continuing with the usability theme, factors such as the user interface and the performance of related technology are both likely to have a clear influence upon whether users can understand and make practical use of them. If an interface is ridden with technical terminology, or conceals relevant functionality too far from view, then it increases the chances of features remaining unused. Similarly, if the operation is overly intrusive or noticeably degrades the system, then users may well elect to manage without it.

A key issue is that the human aspect matters more now than it used to, as security fundamentally affects more people. Indeed, thanks to the range of devices and services they use, and the extent of the online connectivity that they enjoy, individual users have many more security-related choices to make and more data to protect. Moreover, a greater volume and proportion of threats are now actively targeting end-users and their systems. Whatever way you look at it, today's users are, by default, more exposed than their counterparts of the past and it would not be unreasonable to suggest that the user community of security is now effectively everyone. Thus, a broader view of human aspects recognises the need for a wider societal understanding of security and related threats (encompassing both organisations and individuals), and the need to foster an effective information security culture to support this.

3. A growing need for security awareness

An area in which there has been a significant (and ongoing) shift in responsibility and onus. Users must have some level of awareness and capability to protect themselves, as the threat landscape is too wide for technology to provide a complete answer, and the threats exist in too many contexts to be able to rely upon a system administrator or similar to act as the guardian angel. However, many currently find themselves living a society in which they are ill equipped to operate. Many still lack an understanding of the technology, and so find it even harder to relate to the associated threats. Meanwhile, the very same individuals find themselves using the security technology that in previous generations would have been the preserve of the system administrator (e.g. with firewall, backup and, most notably, Intrusion Detection Systems (IDS) all being examples of technologies that have started in the IT department but progressively crept out to face the desktop user). This leads to a significant requirement to raise awareness.

Unfortunately, when considering the attention directed towards different forms of security control, awareness and training has historically lagged significantly behind the technology-oriented safeguards such as firewalls, IDS or other more product-focused approaches. While in no way suggesting that such investments are unimportant, it is fair to say that they only represent part of the picture, but are often the easier decisions to justify on the basis that they target a defined threat and deliver a more easily measurable return. As an example, we can consider the 2010 results from the CSI's annual computer crime and security survey. Although most respondents claimed to have some form of awareness activities, approximately two thirds claimed to be spending 5% or less of their security budget on these activities. Moreover, half of the respondents considered the level of investment to be too little. By contrast, when it came to security technologies, almost 70% were directing more than 10% of their budgets towards it and the vast majority considered this level of expenditure to be adequate (Richardson, 2010).

In terms of addressing security awareness in the workplace, there is the easy rationale that the organisation ought to handle it, and that it's their own fault if they have not done so. While this view may have sufficed in the past, the need for such awareness now extends into the wider populous, and while one might reasonably have expected organisations to take care of themselves, the same expectation cannot be applied to households. Nonetheless, it is important that we address them because of the risk they *face* and the risk they *pose*. For example, not only do individuals run the risk of coming to personal harm as a result of the threats that they may encounter (e.g. malware, phishing, etc), but they can also end up amplifying the problem for other people (e.g. if a home user system gets infected by malware, then many thousands of other users – and indeed organisations – may be affected if that system then starts sending out spam mails or participating in Denial of Service attacks as part of a botnet). In fact, the potential unawareness of home users means that their systems are often more exposed than those sitting under the administrative umbrella of an organisation, and so they