Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

The professionalisation of information security: Perspectives of UK practitioners

R.P. Reece*, B.C. Stahl

Centre for Computing and Social Responsibility, De Montfort University, The Gateway, Leicester LE1 9BH, United Kingdom

ARTICLE INFO

Article history:
Received 7 June 2014
Received in revised form
11 September 2014
Accepted 14 October 2014
Available online 28 October 2014

Keywords:
Security professional
Status
Qualification
Certification
Socio-technical
Graduate

ABSTRACT

In response to the increased "cyber" threats to business, the UK and US Governments are taking steps to develop the training and professional identity of information security practitioners. The ambition of the UK Government is to drive the creation of a recognised profession, in order to attract technology graduates and others into the practice of cyber-security. Although much has been written by state bodies and industry commentators alike on this topic, we believe this qualitative study is the first empirical academic work investigating attitudes to that professionalisation amongst information security workers. The results are contextualised using concepts from the literature in the fields of professionalisation and social topics in information security.

Despite the movement to establish professional status for their industry, these practitioners showed mixed levels of support for further professionalisation, with a distinctly wary attitude towards full regulation and licensing and an explicit rejection of elitist and exclusive models of profession. Whereas the UK Government looks to establish "professional" status in order to attract entrants, such status in itself was seen to be of little import to those already working in the area. In addition there are significant tensions between managers embracing business- and human-centred security and those more interested in the technical practice of executing policy.

While these tensions continue, the results suggest that state attempts artificially to catalyse the professionalisation process for this group would be precipitate. Historically such projects have risen from the front line; ambitions to move the industry in that direction might see more success by identifying and delegating control to a single regulatory body, founded and respected by the people it aims eventually to regulate.

1. Introduction

The market for information security skills is the focus of much current attention. The number of entrants to the occupation is rising and its recruitment paths and qualification schemes are changing (Alderbridge Consulting, 2013). According to one report, demand for information security staff grew by 74% between 2007 and 2013, with over half of advertised positions requesting at least one certification (Burning Glass, 2014).

Having identified a significantly increased need for trained security staff, the UK Department for Business, Innovation

* *Corresponding author*. Tel.: +44 1438 773786, +44 7711 603258 (mobile); fax: +44 1438 773715.
E-mail address: rpreece@dmu.ac.uk (R.P. Reece).
http://dx.doi.org/10.1016/j.cose.2014.10.007

and Skills [BIS] (2014) is engaging directly in the training and organisation of the occupation. It aims to create a cyber-security "profession", with sufficient status to compete for talent with more established career options (Cabinet Office, 2011; BIS, 2014). In the US, the Department of Homeland Security [DoHS] (2012) is also active in developing "cyber skills" however the National Research Council [NRC] (2013) appears more cautious than the UK Government towards formal professionalisation. Alongside noting the effects of artificially manipulating labour markets, it cites the lack of a single body of knowledge to define such a profession (Burley et al., 2014). Yet references are already commonly made to information security "professionals" and a number of credentials exist to certify this professional status. To take one example, there are now nearly 95,000 holders of the Certified Information Systems Security Professional [CISSP] certification ((ISC)^2, 2014). So do these people already consider themselves qualified members of a recognised profession, and if not is achieving that status their ambition?

The objective of this study was to investigate whether efforts to promote an information security profession resonate with the priorities of workers within the industry. Whilst professionalisation may increase its allure to potential entrants, it is this current generation of practitioners who must assent to its progress. The study examines their basic concept of "profession", alongside their attitude to professional status as a motivator and the value of certification. In addition, it investigates practitioner perspectives towards the heterogeneity of professional identity noted by Burley et al. (2014) and others, examining whether those who implement technical controls and those who manage, educate, instil a security culture and issue policies represent a single occupation.

2. Prior work

To provide context to the analysis, several key concepts from two bodies of literature are highly relevant. Firstly, the "social" strand of security research is briefly reviewed, which rebalances the emphasis between technical and non-technical aspects of practice. From this it is shown that there is a theoretical and substantive basis for differentiation between management and technical enforcement roles in security; it is upon this distinction that claims of a new and distinct profession (separate from the computing sciences) might be founded. Secondly, from the substantial sociology of professionalisation it is seen that the formation of professions is a dynamic and competitive process, where both new and existing areas of knowledge are the subject of rival claims for control. This provides a conceptual basis for framing the analysis.

2.1. *Socially-informed security practice*

It is well-established in the literature that information security does not rely solely on the implementation of technical controls. Modern security is a human-centred process, fully informed by both technical and social aspects (Stanton et al., 2005; Von Solms, 2001; Brocaglia, 2005; Siponen and Oinas-Kukkonen, 2007; Bunker, 2012; Von Solms, 2006; Johnson and Goetz, 2007; Kayworth and Whitten, 2010). This shift is most strikingly seen in the recent conceptual challenges to the long-established *confidentiality-integrity-availability* ("CIA") model. Once so fundamental to orthodox computer security texts, this triad is now seen as *incomplete*, since it emphasises technical continuity of individual systems over the human elements of managing security within an organisation (Dhillon and Backhouse, 2000; Kolkowska et al., 2009; Ashenden, 2008). Many writers see this fuller consideration of the human user as vital for a comprehensive or "holistic" approach (Dhillon and Backhouse, 2000; Bunker, 2012; Fink et al., 2008; Brocaglia, 2005; Dlamini et al., 2009).

This socially-informed work does not seek to minimise the significance of technical policy enforcement, but rather to bring more equal consideration to the processes whereby policy is communicated and its acceptance negotiated. Although a consistent minor theme (Dhillon and Backhouse, 2001; Hitchings, 1995; McFadzean et al., 2006), such topics now appear under-represented in earlier work, relative to more even modern treatment (Furnell and Clarke, 2012). Such balance is essential; policy without the ability to enforce it technically is often toothless. However, conceptualising security in purely technical terms leads to its reification. Whilst one can source firewalls and software, one cannot purchase *security* as an alternative to making necessary behavioural and cultural adjustments in an organisation (Stahl et al., 2008; Ashenden and Sasse, 2013). Instilling a proper security culture is a particularly rich area of research, emphasising the centrality of human issues in information security.

2.2. *Translating security policy into culture*

All well-accepted models for security management stress the fundamental importance of an effective policy (Blakley et al., 2001; Von Solms, 2001; Doherty and Fulford, 2006; Stanton et al., 2005), however the mere existence of a policy does not inherently create security (Doherty and Fulford, 2005). Several studies have concluded that where readers regard security requirements as impossible or unnecessary they will either ignore or attempt to circumvent them (Wood, 1997; Post and Kagan, 2007; Adams and Sasse, 1999; Renaud, 2012; Renaud and Goucher, 2014; Barlow et al., 2013; Siponen and Vance, 2010).

Education programmes must therefore move beyond simple awareness. An aware user who does not also understand and accept the security message may wilfully ignore anything inconvenient to their own tasks, particularly where is little compulsion to comply (Furnell and Clarke, 2012; Furnell and Thomson, 2009; Von Solms and Von Solms, 2004). They must be persuaded of a threat to their interests and that their action might be effective against it (Herath and Rao, 2009; Besnard and Arief, 2004; Siponen, 2000; Al-Awadi, 2009; Fulford and Doherty, 2003). To enable this, policies must be the product of dialogue rather than artefacts of diktat (Albrechtsen, 2007; Albrechtsen and Hovden, 2010; Gagné et al., 2008).

Without suitable social awareness and empathy, these cultural efforts will not be effective. Staff with a purely technical outlook may assume that resource priorities for staff throughout the enterprise mirror those of the information security function. Such staff when attempting to impart the