Chapter 57
A Case for Using Blended Learning and Development Techniques to Aid the Delivery of a UK Cybersecurity Core Body of Knowledge

David A Bird
https://orcid.org/0000-0002-5953-7107
Learning and Performance Institute, Coventry, UK

John Curry
Bath Spa University, Bath, UK

ABSTRACT

This article explores the UK's current approach in addressing the cybersecurity skills gap championed by the National Cyber Security Strategy. There have been progressive and elaborate steps taken in the UK toward professionalization of the cybersecurity field. However, cybersecurity knowledge has been labelled as inconsistent when a cybersecurity Chartered status is being proposed. The objective of this analysis was to apply an academic lens over the UK's voyage towards the establishment of a cybersecurity profession. It has been an ambitious but complex endeavor that at times has had alterations of course. Learning from this experience, a blended learning and development approach is now recommended underpinned by an overarching core knowledge framework. Such a framework could join up the existing silos of learning and development activities to benefit from, and build upon, a coherent core knowledge-base for the community. It is argued that this will provide a more satisfactory outcome to enhance the UK's cybersecurity capability on the road to a cybersecurity profession.

DOI: 10.4018/978-1-7998-2466-4.ch057

1. INTRODUCTION

In 2011, the United Kingdom (UK) Government set out their stool by predicting the need to increase cybersecurity skills and expertise in line with their Cyber Security Strategy. It was also decreed that education and training providers should heed this prediction. The main aim then was to counter the effects of cyber-crime, which required specialist training in order to meet an increased skills demand (Cabinet Office, 2011). In 2013, the Harvard Business review stated that education was a catalyst, and enabler, for cybersecurity and called upon academic institutions to share cybersecurity best practices and curricula (Viveros, 2013).

The comprehensive International Information Systems Security Certification Consortium ((ISC)^2) survey of 2015 stated that 63% of private sector organizations did not have enough cybersecurity staff in the UK (Grout, 2015). In the same year the Chancellor laid out the cyber-crime threats to the UK economy (Osborne, 2015). He labored the point that cybersecurity should be embedded at every stage of the education and training process, so the next generation will be able to keep Britain safe in cyberspace. By the next iteration of the Cyber Security Strategy in 2016, it was stated that there were still insufficient skills in cybersecurity and that the public lacked cyber awareness. The UK Government subsequently set their intention for collaboration in training and education across the target audience in the public and private sectors (Cabinet Office, 2016). This was a part of the continuing agenda taken by UK Government to make Britain the safest place in cyberspace championed by the Department for Digital, Culture, Media and Sport (DCMS) (2017) and the National Cyber Security Center (NCSC) which is a part of the Government Communications Headquarters (GCHQ). A number of approaches to enthuse adolescents were spawned and aimed at refocusing of attitudes leading to a cybersecurity curriculum (Williams, 2017).

There is a myriad of certifications categorized by the Institute of Information Security Professionals (IISP) ranging from vendor-based, those aimed at role competencies, broad certifications and those provided by academia (Finch & Furnell, 2018). However, there are advantages and disadvantages with professionalization. From a USA perspective, Schneier (2013) has discussed openly that popular certifications used as a form of entry into cybersecurity run the risk of becoming obsolete; and need to be maintained using Continuous Professional Development (CPD). Interestingly, Nepal (2018) has stated that in Australia cybersecurity tools have not reduced the demand on cybersecurity experts, but actually increased demand for more cybersecurity specialists. In tandem, the cybersecurity skills shortage in the UK increased to 66% by 2017 (Cox, 2017). The 2018 edition of Information Systems Audit and Control Association (ISACA) ‘State of Cybersecurity’ report stated that of the 60% of organizations who had open jobs in cybersecurity, 54% of positions took over three months to fill (GoCertify, 2018); it was suggested that the skills gap was actually widening (ISACA, 2018). Consequently, demand for expertise and skills is driving up cybersecurity salaries in the UK (McDonald, 2018) and making them comparative to more established and recognized professions.

Additionally, there have been endeavors to increase cybersecurity awareness in organizations (Palmer, 2016) and the wider populace of the UK; this follows a similar agenda to the USA (Morgan, 2017). However, awareness should only be the start of making people mindful about the cybersecurity risks (Beyer et al., 2015). There are other diverse and relevant skillsets within the Information Technology (IT) industry such as system designers and developers along with system managers and system administrators who are also important in cybersecurity. All these roles require better cybersecurity awareness and the right culture to ensure that security is an important criterion in the development, implementation and