Chapter 22
Delivering Cybersecurity Education Effectively

Alastair Irons
University of Sunderland, UK

ABSTRACT

This chapter draws on current research and best practice into teaching in cybersecurity in higher education. The chapter provides a theoretical and pedagogical foundation for helping tutors make decisions about what topics to include and approaches to teaching and assessing the cybersecurity curriculum. There are of course a range of potential stakeholders in cybersecurity education ranging from government, policy, and law makers to all members of society. However, for the purposes of brevity, this chapter will focus on learners and those creating and delivering cybersecurity education in the higher education (HE) sector.

INTRODUCTION

The chapter discusses the opportunities for different and innovative ways of learning about cybersecurity – designed to provide deep learning and thus a greater understanding of principles, theories and applications of cybersecurity. The purpose of the chapter is to explore the differences between the delivery of cybersecurity education and the delivery of other computing-based subjects in Higher Education. Whilst the delivery of cybersecurity will utilize good practice from the delivery of computing, computer science and other subjects in HE the discussion in this chapter attempts to emphasize and examine the issues from a cybersecurity perspective.

In recent years, computing technology and computer systems have experienced dramatic growth. The growth in the number of systems (communications, information systems, Internet systems and e-commerce) and the advances in the scale, the functionality and the usability of systems have provided opportunities for malicious users to exploit insecure and non-robust systems. The pace at which companies and their customers have embraced technologies such as cloud computing, smart devices, mobile technologies, and the Internet of Things (IoT) has created an environment that is changing faster than organizations and legislators can keep abreast of. It's not only systems that are changing – the way people use the

DOI: 10.4018/978-1-6684-3554-0.ch022

systems and the expectations of speed and convenience means that cybersecurity can often be relegated in importance. Allied to the growth in systems technologies is the growth in the amount of data that is provided and the huge variety of ways in which data is collected, manipulated and stored.

The range of systems and technologies and the speed of implementation and adoption provide opportunities for cybercriminals to exploit. In addition to chance to take advantage of vulnerabilities in systems the advances in technology give computer criminals the opportunity to conceal their activities, to cover their tracks and attempt to destroy evidence of their actions. The ability to prevent cybercrime attacks and cybersecurity breaches that have taken place and the resultant requirement to examine the cybertrail have raised the need to develop specialists in cybersecurity – a set of practitioners who have the methods, skills and techniques to prevent, detect, recover and restore systems and data in the event of an attack.

The global news headlines frequently present cybersecurity attacks, vulnerabilities or failures, illustrating that there is an increasing loss of control over the cyber-threats to business. Recent years have seen high profile attacks to major corporations such as Tesco Bank, Talk Talk, Daimler Chrysler. In 2017 the NHS in the UK (along with 160 other organizations) were rocked by the "Wannacry" attack. Other headlines have reported belief and fear that the recent U.S. elections could be manipulated by a foreign power and speculation over whether development in artificial intelligence could lead to cyber attacks perpetrated by machines, without any human motivation.

The changing technology environment and the growth in threats and potential threats means that the role of cybersecurity is increasing in importance. As society and business becomes more reliant on cybersecurity the efficiency of cybersecurity education – what we teach and how we teach it – becomes an important objective. Similarly, there is a need to consider the learners, what they need and want to learn as well as how they learn as in integral part of cybersecurity education.

McGettrick (2013) argues for the need for cybersecurity education as opposed to cybersecurity training. In this chapter the focus is on cybersecurity education – but as tends to be the case with discussion on any aspect of cybersecurity there is overlap between the categories, so some aspects of training come in to the consideration of cybersecurity education. Part of the rationale for looking at this topic is because there are so many different providers offering a range of different cybersecurity learning products claiming to deliver education and training.

It is worth asking the question as to why there should be consideration given to examining the ways in which to deliver cybersecurity education. Cybersecurity is a complex and wide-ranging topic (or series of topics) to consider. The complexity associated with cybersecurity means that there is a need to consider different teaching approaches to enable cybersecurity learning. Rashid et al (2018) argue that "the foundational knowledge on which the field of cybersecurity is being developed is fragmented, and as a result, it can be difficult for both students and educators to map coherent paths of progression through the subject". There are many topic domains in which we potentially have interest in cybersecurity including (but not limited to) information security, systems security, network security and Internet security each with a set of fundamentals and principles and different theories and applications. In addition, there is an interesting mix of technical, policy, governance, ethical and human / society subjects which require different approaches to teaching and learning. As far back as 1997, Pfleeger et al (1997) suggested a broad range of sub topics making up the cybersecurity knowledge base, including "security policy, privileges, authentication, correctness and auditing", and how these relate "trusted systems, operating systems, database management systems, distributed systems, cryptography, protocols, system correctness, intrusion detection and mobile code". Hallet et al (2018) raise questions about the number of cybersecurity