Chapter 11
Model Course Syllabus: Management of Security Issues in Wearable Technology

Michelle C. Antero
Zayed University, UAE

ABSTRACT

This chapter briefly introduces some historical and contemporary context before proposing a model course syllabus to implement a course in Management of Security Issues in Wearable Technology. The course syllabus is developed in line with the IS2010 curriculum recommended by the peak bodies (ACM and AIS) for a degree in Information Systems, Computer Information Systems or Management Information Systems. The design further follows the guidelines developed by the Accreditation Board of Engineering and Technology (ABET) that advocates that Course Learning Outcomes (CLOs) be developed for the list of topics covered by the material. In addition, the syllabus provides a basis for enterprise training relevant to managers and security specialists. The chapter also provides some general pedagogical guidelines on how each topic can be discussed and activities appropriate to the learners. It also uses Gluga et al.'s (2013) assessment criteria, based on Bloom's (1956) taxonomy to measure the depth of knowledge.

INTRODUCTION

Technological advances in microchips, mobile technology, wireless networks, sensors, location-based services, and the prevalence of mobile applications have made possible the widespread availability of a whole range of wearable technology.

DOI: 10.4018/978-1-5225-1016-1.ch011

Early applications of wearable technologies were conceived in 1955 and developed in 1961 when Thorpe and Shannon developed a shoe-mounted roulette wheel prediction system (Thorpe, 1998). The mass production of the microchip in the 1980s made it possible to increase computing capabilities and opened up opportunities to develop wearable technology. Pioneering work by Steve Mann in the 1980s and early 1990s (Mann, 1995s) introduced the "wearable wireless webcam" to the world and, in 1996, the USA's Defense Advanced Research Project Agency (DARPA) launched a wearable technology workshop looking towards "Wearables in 2005" (Rhodes & Mase, 2006).

A year later, in 1997, the first head-mounted display (DARPA, 1997) was developed for tactical military purposes. By the late 2000s, we began to see the availability of consumer wearable technology and the ability to sync information between the wearable technology and mobile phones. For example, the collaboration between Nike and Apple in 2006 created Nike+iPod (Apple, 2006). Nike+iPod was the first product to synchronize information collected from sensors in Nike shoes with an iPod application, and it ultimately changed a runner's experience. By 2014, the Consumer Electronic show in Las Vegas was showcasing smart watches, activity trackers, head-mountable cameras and a whole range of other wearable technology for the mass market (Gibbs & Arthur 2014).

The spike in the demand and growth of the availability of wearable technologies in recent years provides motivation to understand the security risks associated with these devices. As these devices become pervasive, individuals and organizations need to be made aware of the security and privacy risks posed by wearable technology. As a new academic discipline focused on this particular research agenda has emerged, there is a corresponding need to develop a model curriculum to guide academics as they discuss these issues in the classroom or in enterprise-wide training courses.

WEARABLE TECHNOLOGY AND ITS SECURITY AND PRIVACY RISKS

Wearable technology builds on the vision that body-worn technology augments a human's physical and analytical capabilities with computing power to engage in superhuman activities (Pedersen, 2014). Wearable technology refers to clothing or accessories that utilize the power of computing and electronics to enable the exchange data between objects without human intervention. The interoperability of these devices with existing technologies has made it possible to have a seamless exchange of data and a push toward connectedness.