Chapter 6
Introducing Psychological Concepts and Methods to Cybersecurity Students

Jacqui Taylor
Bournemouth University, UK

Helen Thackray
Bournemouth University, UK

Sarah E. Hodge
Bournemouth University, UK

John McAlaney
Bournemouth University, UK

ABSTRACT

This chapter begins with a brief review of the literature that highlights what psychology research and practice can offer to cybersecurity education. The authors draw on their wide-ranging inter-disciplinary teaching experience, and in this chapter, they discuss their observations gained from teaching psychological principles and methods to undergraduate and postgraduate cybersecurity students. The authors pay special attention to the consideration of the characteristics of cybersecurity students so that psychology is taught in a way that is accessible and engaging. Finally, the authors offer some practical suggestions for academics to help them incorporate psychology into the cybersecurity curriculum.

WHAT CAN PSYCHOLOGY OFFER TO CYBERSECURITY EDUCATION AND TRAINING?

There is a symbiotic relationship between the disciplines of computing and psychology: psychologists have helped in many ways to understand the way that computer systems are developed and used, but also an understanding of computers has helped psychologists to model and investigate human cognitive and social processes. This chapter will focus on the former; over the past 60 years, psychologists have

DOI: 10.4018/978-1-5225-4053-3.ch006

tracked and researched the development and impact of computers and they have also been instrumental in their design and evolution. To design, develop, implement and evaluate secure sociotechnical systems students need to understand concepts and research methods in psychology. To understand the potential risks of sociotechnical systems, cybersecurity students need to understand and consider how people perceive, remember, feel, think and solve problems, i.e. the domain of cognitive psychology. It is also important for students to consider individual differences and social behavior if effective interaction between people and computer systems is to be achieved, i.e. the domain of social psychology and individual differences. An understanding of these psychological topics enables students in cybersecurity to consider the potential capabilities and limitations of computer users and helps them to design computer systems that are more effective (usable) for a variety of user types. In addition to covering the foundation areas of Psychology, it is also important that cybersecurity students are taught evaluation methods and that they are able to consider the social impacts and ethical issues regarding the implementation and use of computer systems in organisations and society.

A review of the literature and media commentary on cybersecurity attacks shows that increasingly they involve social engineering techniques; where psychological principles are used to manipulate people into disclosing sensitive information or allowing others to access a secure system (Tetri & Vuorinen, 2013). For example, phishing emails and phone scams utilize many psychological principles relating to social influence to persuade users to open a link, such as appeals based on fear or invoking a sense of scarcity or urgency (Cialdini, 2008). However, despite the psychological nature of such cybersecurity attacks, research into the role of psychology in cybersecurity is still limited (McAlaney, Thackray and Taylor, 2016). Also, often research into the closely linked area of social engineering is conducted from the discipline of computing rather than psychology. Indeed, the call for papers for a recent conference organized in the UK by the Higher Education Academy on learning and teaching in cybersecurity listed relevant disciplines as 'STEM' and 'Computing' and the eventual program of abstracts contained no mention of psychology. Similarly, curricular guidance for the field of cybersecurity education produced by the ACM (McGettrick, 2013), contained just two uses of the word psychology and no further detail. However, within the last year the importance of psychology has begun to be recognized in the academic literature (McAlaney, Thackray and Taylor, 2016). For example, a recent article (Hamman, Hopkinson, Markham, Chaplik & Metzler, 2017) suggests the teaching of game theory in cybersecurity courses and links this to the psychological nature of many incidents. Hamman et al. propose that one of the benefits of game theory is that it fundamentally alters the way students view the practice of cybersecurity, and state that it helps to sensitize them to the human adversary element inherent in cybersecurity in addition to technology-focused best practices (p1).

The majority of psychological research that has been conducted so far in this area has focused on prevention and mitigation strategies for the targets of cybersecurity incidents with little focus on the motivation of the perpetrators (Rogers, 2010). Psychology can offer much in helping to understand the motivations of individual hackers or scammers, for example drawing on the research into individual differences, looking at factors such as self-esteem, introversion, openness to experience and social anxiety (Fullwood, 2015). Other work has shown that individual's motivations are not always related to financial gain but can be purely for entertainment or social status reasons (Rogers, 2010). In contrast, large scale cybersecurity incidents are often instigated by groups, as opposed to individuals acting alone. As such these incidents can be regarded as the result of group actions and group processes; theories from Psychology are used to help understand the formation, operation and influence of groups on their