Chapter 9
Understanding Personality and Person-Specific Predictors of Cyber-Based Insider Threat

Joyce S. Pang
Nanyang Technological University, Singapore

ABSTRACT

The chapter aims to provide an opinion on major challenges for ongoing personality research on cyber security, especially in the area of insider threat. While research on the prevention and perpetuation of insider threat activity within cyberspace has grown substantially in the recent decade, there remain many unanswered challenges and unchartered territories of knowledge in the field. Specifically, compared to the amount of work done on algorithmic modelling approaches, much of the psychological data is scant and focuses on correlations between the so-called Big Five personality traits (i.e., extraversion, openness to experience, agreeableness, emotional stability, conscientiousness) or demographic variables (e.g., gender, age) with insider threat activity. Thus, the focus of this article is to articulate the major challenges for understanding insider threat in the context of cyber security, particularly from a personality and person-specific perspective that emphasises internal characteristics of the individual actor as explanations of actions and events.

INTRODUCTION AND GENERAL APPROACH

The aim of this chapter is to provide an opinion on the major challenges for ongoing personality research on cyber security, especially in the area of insider threat. Cyber security refers to the field involved in the monitoring of criminal activities in cyberspace, in order to maintain a safe environment for the transfer of resources and for the dissemination and protection of information. Insider threat refers to the presence of trusted individuals who are either members of an organisation or who have privileged access to organisation resources, and who engage in activities from within the organisation to threaten the interests of that organisation (cf. Probst, Hunker, Gollmann, & Bishop, 2010). In relation to cyber security, the major categories of insider threat are IT sabotage, fraud, theft of intellectual property (IP

DOI: 10.4018/978-1-5225-5634-3.ch009

theft), and espionage. While research on the prevention and perpetuation of insider threat activity within cyberspace has grown substantially in the recent decade, there remain many unanswered challenges and unchartered territories of knowledge in the field. Specifically, compared to the amount of work done on logging software and algorithmic modelling approaches, relatively less work has been carried out to clarify the important psychological and sociological factors for cyber security and for insider threat. Importantly, much of the psychological data is scant and focuses on correlations between the so-called Big Five personality traits (i.e., extraversion, openness to experience, agreeableness, emotional stability, conscientiousness; John & Srivastava, 1999; see Axelrad, Sticha, Brdiczka, & Shen, 2013, for an example of a Bayesian network model of insider threat using the Big Five traits) or demographic variables (e.g., gender and age; see Chang & Lim, 2014) with insider threat activity. Thus, the focus of this chapter is to articulate the major challenges for understanding insider threat in the context of cyber security, particularly from a personality and person-specific perspective.

By a 'personality and person-specific perspective', I am referring to a perspective that emphasises internal characteristics of the individual actor as explanations of actions and events. These internal characteristics can come from personality dimensions – which are a system of thoughts, feelings, and behaviours that an individual exhibits consistently across time and over situations – or they can come from person-specific dimensions that are externally ascribed to an individual usually because of his or her social category. Examples of personality dimensions are traits (e.g., extraversion), explanatory styles (e.g., pessimism), motives (e.g., power motivation), skills and competencies (e.g., intelligence, creativity), and values (e.g., benevolence). Individuals differ on these personality dimensions because of biology, influence from social contexts, upbringing, and exposure to significant others, as well as through a combination of learning experiences and interaction with social and physical environments. Examples of person-specific dimensions include gender, age, and socioeconomic class.

There are two major decisions for a behavioural scientist who is trying to understand person-specific characteristics of cyber-based insider threat; these involve the questions of what and how to study cybercrime and insider threat. In considering the question of what should be studied, I will make use of the excellent groundwork carried out recently by researchers in the fields of cyber security and insider threat. I will conduct a targeted review of recently published frameworks for understanding insider threat, specifically the models of Nurse et al. (2014) and Moore et al. (2011).

Whilst Nurse and colleagues did an admirable job of summarising main themes in the field, their framework is relatively general and thus allows for much more categories of study to be uncovered. Hence, Nurse at al.'s (2014) model can be a jumping off point, from which I will discuss more context-specific areas for future research inquiry, such as regarding the motivation of offenders.

I will also discuss offender profiles and types of cyber-insiders, using recent work by Moore and colleagues. Moore, Cappelli, and Trzeciak (2008) and Moore et al. (2011) have provided some insight into offender profiles in insider crime, specifically in the areas of fraud and IP theft. Using research in the related fields of organisational psychology and personality psychology (e.g., Murphy & Dacin, 2011), I suggest some extensions of Moore and colleagues' work by identifying some other promising variables and/or productive dimensions for categorising cyber offenders of insider attacks.

For the question of how to study cyber-based insider attacks, in the latter part of the chapter, I will discuss some methodological considerations, such as how to derive an approach for the field that is both theory and data driven, and how psychological and behavioural data should be collected and/or treated for validation purposes and for application purposes.