Chapter 8
Online Calling Cards and Professional Profiles in Cybersecurity From Social Media

Shalin Hai-Jew
https://orcid.org/0000-0002-8863-0175
Kansas State University, USA

ABSTRACT

Demand is very high for people to work in various cybersecurity professions and ceteris paribus that demand may well continue into the near term. While there are more formal trails for employment, such as higher-educational pathways, performance in cybersecurity competitions, participation in professional conferences, and social media presentations may all offer less conventional paths into cybersecurity hiring. Through a convenience sample across a number of social media platforms and bottom-up coding, this work explores some aspects of cybersecurity professional profiles ("calling cards") available on the open Social Web and what may be learned about respective skills and capabilities from these glimmers of the person(s) behind the profiles. These profiles are assessed based on a 2x2 axis with focuses on (1) target skills and (2) personhood attributes. From these analyses, some tentative insights are shared about the cybersecurity calling cards and how informative they may be for recruitment and retention of cybersecurity workers.

INTRODUCTION

George Smiley: "The more identities a man has, the more they express the person they conceal." -- John Le Carré in Tinker Tailor Soldier Spy (1974, 2012)

DOI: 10.4018/978-1-6684-3554-0.ch008

"Cybersecurity," defined as "a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access" ("What is cybersecurity?" n.d.), encompasses a broad range of professional positions and skill sets. At present, there is a lack of a consensus definition about what actually constitutes a cybersecurity professional. One researcher writes:

… a literature review confirms there is no standard definition of a cybersecurity worker, associated skills, or educational requirements. The cybersecurity workforce to which we speak in this report consists of those who self-identify as cyber or security specialists as well as those who build and maintain the nation's critical infrastructure. (Wilson & Ali, 2011, p. 15) (note: original source italics)

There are some definitions from the environment. A Department of Homeland Security secretary defined cybersecurity professionals as those in charge of "... cyber risk and strategic analysis; cyber incident response; vulnerability detection and assessment; intelligence and investigation; and network and systems engineering" (Krebs, 2009, as cited in Wilson & Ali, 2011, p. 16). In terms of secure software development, there are designers, developers, and testers (Shumba, et al., 2013, p. 4). A perusal of job sites today includes a wide range of roles. In one schematic, authors mentioned red team members (who serve as network attackers to help companies strengthen their defenses), blue team members, systems administrators, computer network defense analysts, computer programmers, targeting analysts, security engineers, computer network defense forensic analysts, collection operators, and exploitation analysts (Campbell, O'Rourke, & Bunting, 2015, p. 722). According to another source, the most in-demand cybersecurity jobs include the following three, in descending order: 1) penetration testers, 2) cybersecurity engineers, and 3) CISOs (chief information security officers), according to Mondo, a company providing technical staffing (Rayome, 2017). There have been calls for as-yet uncreated positions, such as for "cyber diplomats" to work at the nation-state level to ensure there may be clearer understandings of each other's uses of cyberspace and to help with the resolution of cyber-related issues that may arise (Maller, 2013). With the advent of the Internet of Things (IoT), with cyber tools used in homes, healthcare, cars, and other spaces, the need for professionals in cybersecurity will expand further.

Currently, there is serious planning and work to try to secure the IoT (Ahlmeyer & Chircu, 2016). Additionally, for all the mentions of full-time employees, there are also interns, "gig workers" or "temps," and others who fill cybersecurity positions. In addition, with regards to cybersecurity, there is the formal job market, the freelance, and the informal black job market. Broadly, professional roles in cybersecurity may be understood in broad categories: leadership / management, policy, legal, technology, research and development, and education and training. In some cases, there may be crossover among these categories.

The cybersecurity market is projected to be a US$170 billion industry by 2020 (Morgan, 2016). In 2016, some 209,000 cybersecurity jobs in the U.S. were unfilled (Morgan, 2016), and this number is expected to rise to "6 million globally by 2019, according to the CEO of Symantec (Morgan, 2016). Organizationally, labor shortages mean that some functionalities are simply not addressed, and current staff tend to be over-worked and potentially under-attentive; also, there are pressures on wages (Wright, 2015). A number of efforts are ongoing to address the workforce shortfall in this critical and dynamic area, particularly with the onboarding of more cyber with the Internet of Things (IoT).

With the popularization of cyber, in early years, individuals with "hacker" skills were in high demand, and while the field has formalized to some degree (with internships, competitions, growing technical certifications, undergraduate and graduate degrees, post-graduate studies, cyber defense competitions, and formal modeling of cyber jobs and cybersecurity workforce frameworks), there is still room for