Chapter 1
Modeling Processes and Outcomes From Cybersecurity Talent Gaps in Global Labor Markets

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

Many experience cybersecurity talent gaps at a local level. They see positions that go unfilled or filled with people without the requisite skills; they see data and identity compromises, projects that are stymied, and heightened risks. They have to address this gap locally by educating individuals through the talent pipeline, supporting learning and training programs, cross-training employees into cybersecurity endeavors, placing classified ads/head-hunting and hiring ever-more-expensive talent, and so on. They go to outside vendors to support the work. For those in the proverbial trenches, understanding this global labor market challenge at the 30,000-foot level may be helpful. This work models the projected processes and outcomes of the cybersecurity talent gap through multiple means: a review of the literature, general systems theory, social network analysis, game theory, and abductive logic, and up-to-date data.

INTRODUCTION

In a typical workday, the cybersecurity talent gap in the global labor markets is patently clear. There are news reports of various data compromises in cities that have had their data encrypted and controlled by ransomware. There are data spills with private data shared broadly. On the Dark Web are businesses selling people's credentials for others to exploit. And within work places are smaller fires—phishing attacks, malware attacks, disappeared memory devices, misplaced laptops with sensitive data, and others. Those who can afford to hire top-flight talent and purchase top-shelf technologies attempt to create a secure cyber-environment. Those who cannot afford to do so are left exposed and must focus on lower-cost methods for recovery. In many senses, the "cyber-technological haves" are also the most vulnerable because of the wiredness of their societies and their early adoptions of cybertechnology.

DOI: 10.4018/978-1-5225-5927-6.ch001

A Broad Vulnerability

"Cyber," broadly speaking, touches virtually every aspect of modern life. In a typical day, people may use resources on the Internet and Web for the following: intercommunications, work, news consumption, entertainment, banking, library services, health management, research, and others. The Internet of Things (IoT) stands to broaden the reliance on cyber in people's homes, healthcare, transportation, commerce and shopping, and other systems. Less obviously, they rely on infrastructure that relies on cyber (cyber-physical systems): electricity, transportation (e.g., GPS, scheduling, sensor networks), manufacturing, commerce, military systems, and others. The deep integration of cyber in contemporary lifestyles means that the potential cyber "attack surface" is wide and deep, and cyberattacks based on found and created vulnerabilities may be high-impact, disruptive, and even potentially devastating.

Cybersecurity

Cybersecurity may be conceptualized as the so-called "security value chain," which includes five elements:

Deter -> Protect -> Detect -> Respond -> Recover

Each step of the chain is important to strive for a holistic context of security. Therefore, security is created through a mix of policies, laws, law enforcement, technologies, surveillance, and social norms, among others. These various elements provide actual defense-in-depth (the uses of various defensive lines at all levels for a stronger collective defense), and they challenge any nation-state, criminal organization, hacker collective, or individual to really consider cost-benefit calculations before they would take actions to compromise cybersystems or cyber elements in systems.

The Definition of Necessary Skills

Information security professionals, based on the 2013 Global Information Security Workforce Study, do well to have the following skills to be successful in the field (in descending order): "broad understanding of the security field (92%), communication skills (91%), technical knowledge (88%), awareness and understanding of the latest security threats (86%), security policy formulation and application (75%), leadership skills (68%), business management skills (57%), project management skills (55%), and legal knowledge (42%) (Caldwell, 2013, p. 7).

The required skills are often cross-disciplinary:

The pivotal significance of cyber and computer networks to the security of critical infrastructure has contributed to raising awareness about how the comprehension of cyber and cyber security issues necessitates a complex skill-set. This skill-set includes competence within a variety of disciplines, ranging from engineering and computer technology, to law, diplomacy and management. (Røislien, 2015, p. 23)

Another critical capability is to think and innovate creatively, since so much of the field is ambiguous and undefined, and since cyberattacks are constantly being innovated by people.