Chapter 7
How Can a Cybersecurity Student Become a Cybersecurity Professional and Succeed in a Cybersecurity Career?

Sandra Blanke
University of Dallas, USA

Paul Christian Nielsen
University of Dallas, USA

Brian Wrozek
University of Dallas, USA

ABSTRACT

The need for cybersecurity professionals extends across government and private industries. Estimates place the shortage of cybersecurity professionals at 1.8 million by 2022. This chapter provides aspiring cybersecurity students a clear understanding of the various educational pathways they can choose to achieve their goals. The authors describe educational categories and include an assessment of each that students will want to consider based on their own situation. The authors discuss how the study of cybersecurity can be accomplished from a computer science, engineering, and business perspective. Students with STEM skills can accomplish their goals in numerous cybersecurity roles including cyber engineer, architect, and other technical roles. Finally, students with cyber business interest can accomplish their goals with a focus on strategy, compliance, awareness, and others. Organizations need employees with all these skills. This chapter concludes with the recommendation for continual learning, the value of networking, and the encouragement for students to start creating a cyber career.

INTRODUCTION

As cybersecurity professionals and educators, the authors are often asked by students and other individuals currently in information technology and other career fields; "How Can I Become a Cybersecurity Professional"? This question is being asked because there are numerous publications reporting a very large gap in cybersecurity expertise and for those with cybersecurity skills there are six figure salary

DOI: 10.4018/978-1-5225-5927-6.ch007

opportunities. Steve Morgan (2016) the Founder and CEO at Cybersecurity Ventures and Editor-In-Chief of the *Cybersecurity Market Report* and *Forbes* contributor reported "if you are thinking about a career change in 2016, then you might want to have a look at the burgeoning cybersecurity market which is expected to grow from US$75 billion in 2015 to US$170 billion by 2020 … a career can mean a six-figure salary, job security and the potential for upward mobility."

Jeff Kauflin (2017) an author for Forbes Staff focusing on leadership and careers reports "behind every new hack or data breach, there's a company scrambling to put out the fire. That's good news for job seekers with cybersecurity security skills. Employers can't hire them fast enough." ISACA (2016) estimates a global 2 million workforce gap by 2019 and Cisco Continuum (2017) reports cybersecurity will have a workforce gap of 1.8 million by 2022.

These statistics are prompting many individuals to consider moving into cybersecurity. Some have solid backgrounds in supportive fields such as information systems administration, networking, software development, and testing. Others seek to make major career changes from largely unrelated fields such as accounting, marketing, sales, and manufacturing. A successful transition to cybersecurity promises a strong demand for these needed skills, high pay, and job stability for the foreseeable future.

This chapter was written to provide the aspiring cybersecurity professional with an overview of the initial study of Information Assurance that was introduced in May, 1988 in Presidential Decision Directive 63 (PDD 63). Prospective cybersecurity students need to understand the purpose, the complexity, and the importance of reducing vulnerabilities in our national infrastructure, risk management strategies and other important areas of cybersecurity education. This objective can only be accomplished by developing the number of cybersecurity professionals.

Prospective students will learn of the many cybersecurity job titles, skills and resources that have been created and can be used to assist the student. Numerous cybersecurity education categories are discussed and a realistic review of each are provided including advantages and disadvantages of each. Students are provided recommendations on how to prepare for either a technical or non-technical position in cybersecurity as well as recommendations to begin their cybersecurity career.

BACKGROUND

Creation of the Study of Cybersecurity Education

In May 1988 the Presidential Decision Directive 63 (PDD 63), within the Clinton Administration, created the Policy on Critical Infrastructure Protection and the initial development of the Centers of Academic Excellence in Information Assurance (IA) Education (CAE-IAE) Program. The CAE program was initially developed by the National Security Agency (NSA) in 1998 and in 2004 the Department of Homeland security joined as a partner. "The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in cyber defense and producing professionals with cyber defense expertise for the nation" (National Centers of Academic Excellence in Cyber Defense, 2016).

In 2008, the CAE in IA research was added to encourage doctoral research in cybersecurity. In 2010, Two-year institutions, technical schools, and government training centers were added (National Centers of Academic Excellence in Cyber Defense, 2016). In 2016, the CAE-Cyber Operations designation was announced and in 2017 it restructured to have two designation programs. The CAE-Cyber Operations Fundamental and the CAE-Cyber Operations Advanced (CAE-Cyber Operations Announcements,