Chapter 63
An Exploration of the Cybersecurity Workforce Shortage

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
The Florida Institute of Technology, Melbourne, USA

ABSTRACT

There is a colossal cyber security workforce shortage. Global estimates state there are over 1 million unfilled cyber security jobs. As everyone becomes increasingly hyper-connected and cybercrime intensifies in both scale and complexity, the need for experts in the field is dire. Innovative organizations are realizing that they need to tap into new talent pools of minorities and woman that have historically been overlooked. This article explores nature of this this workforce shortage and how to find new sources of talent.

INTRODUCTION

The underrepresentation of women and minorities in computer science has been a concern to government, industry, and academia for more than 10 years. Researchers are indicating that within the Science, Technology, Engineering, and Mathematics (STEM) domain, computer science is expected to experience the extensive growth through 2020 in the U.S.; yet, the pipeline struggles to produce enough college graduates to meet the demand. The shortage of computer scientists becomes more cumbersome when women and minorities remain significantly underrepresented, which means that women and people of color need more initiatives for inclusion in the equation. Organizations with Information Technology Departments have challenges with hiring cybersecurity professionals in this hypercompetitive environment due to a talent shortage. Considering the complexity of acquiring engineering and technical talent for organizations, highlights a deficiency in strategic initiatives aiming to hire more women and minority computer scientists and computer engineers. Diversity promotes differences in thinking and perspectives,

DOI: 10.4018/978-1-7998-2466-4.ch063

enabling organizations to discover new vectors for problem solving, which have a dramatic impact on operational successes. Social scientists indicate that socially diverse groups and people with various specialties are more advantageous than a homogeneous group at solving complex, emergent problems. This is not only because people with different backgrounds provide different perspectives. Diversity can enhance the bread of knowledge and incite new practices by adding to an organization's intellectual capacity and innovative ideology. A diverse workforce is a core capability that provides organizations with a strategic advantage by approaching problems, projects, and strategies with holistic viewpoints such as minority computer scientists and engineers providing critical cultural and gender-based perspectives on engineering problems that are stymied due to shortsighted vantage points.

LITERATURE OVERVIEW

Recently, Uber CEO, Dara Khosrowshahi, acknowledged a 2016 data breach in which the personal data, including phone numbers, email addresses, and names of 57 million Uber consumers. At the time of the data breach, Uber paid the hackers $100,000 to destroy the data and intentionally neglected to inform regulators or consumers of the incident until November of 2017 (Stump, 2017).

According to Larson (2017), 48 states have security breach notification laws. These laws require companies to disclose cyber incidents or theft of consumers' privacy information and critical human resource information (Larson, 2017). The Uber cybersecurity incident is one in a series of corporate and government security breaches that highlight the need for proven and effective cybersecurity security controls as well as personnel with the expertise to execute these objectives (Morgan, 2016a). According to Morgan (2016d) the five most cyberattacked industries in 2015 were:

- Healthcare
- Manufacturing
- Financial Services
- Government
- Transportation

Information security analysts (ISA) positions are expected to grow 18% through 2024 because ISAs are involved in mitigating cyber vulnerabilities in corporate networks (Morgan, 2016b). Crimes related to cyber costs businesses upwards of $400 billion annually accompanied by the rapid integration of technology, electronic communications, and digitalization efforts project the cost of cybersecurity breaches to $2.1 trillion globally by 2019 (Morgan, 2016b)

Magid (2014) states that cybersecurity is an organizational-wide responsibility. Information technology companies and merchants have complex responsibilities to protect customers' payment information and personal private information (Magid, 2014). Government organizations have a role in law enforcement and the deployment of public education programs (Magid, 2014). Global and local companies need to have effective business strategies in place that focus on information security (Magid, 2014). Cybersecurity crime forecasts indicate a need for more information security employees (Morgan, 2016b). The demand for more cybersecurity professionals is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million cybersecurity professionals (Morgan, 2016a). The median pay for information