Chapter 17
Retaining Generation Z Cybersecurity Talent in Government and Beyond

Jennifer Ferreras-Perez
Marymount University, USA

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA

Calvin Nobles
https://orcid.org/0000-0003-4002-1108
Illinois Institute of Technology, USA

Amalisha Sabie Aridi
https://orcid.org/0000-0002-7869-5530
Capitol Technology University, USA

Kevin Richardson
https://orcid.org/0009-0002-3212-8669
Capitol Technology University, USA

Katrina Khanta
Marymount University, USA

ABSTRACT

As the world becomes more interconnected, business competition becomes increasingly fierce, making it critical for companies to stay ahead of the curve in the current era of globalization. With a forecasted turnover of 50-75% higher than in previous years and a timeline 18% longer to fill roles than pre-pandemic, employee retention has become essential for organizations. Employee satisfaction is a critical factor for organizational success, as it not only increases perceived productivity but also has a positive impact on overall organizational performance. The introduction of Generation Z (Gen Z) into the workforce has ushered a shift in job requirements, expectations, and needs as Gen Z approaches employment with an outlook different from previous generations. This qualitative study aims to identify the factors that influence recruiting, retention, and job satisfaction in the cybersecurity field with reference to Gen Z in the federal workforce.

DOI: 10.4018/978-1-6684-7207-1.ch017

INTRODUCTION

The increasing prevalence of cyber threats has created a growing need for qualified cybersecurity professionals to help protect government organizations from malicious activities. However, recruiting these individuals can be a difficult and complex process, and the challenges associated with doing so can put these organizations at great risk.

The first challenge facing government organizations when attempting to recruit cybersecurity workers is the lack of qualified professionals in the field. According to Purcell and Puthiyamadam (2017), "the shortage of skilled cybersecurity professionals is a major challenge for organizations." This is especially true for government organizations, which often have more stringent requirements for their cybersecurity personnel than do private sector organizations. Therefore, it can be difficult for these organizations to find individuals who have the necessary qualifications for the position. Additionally, because of the shortage of skilled professionals in the field, those with the necessary qualifications often command higher salaries than what organizations can afford to pay (Purcell & Puthiyamadam, 2017).

The second challenge is the rapidly changing nature of the field. The field of cybersecurity is constantly evolving, making it difficult for government organizations to keep up with the latest developments. Additionally, the technology used in the field is also constantly evolving, making it difficult for organizations to ensure that their cybersecurity personnel have the necessary skills and knowledge to work with the latest technology (Brown, 2017). As a result, it can be difficult for government organizations to recruit and retain cybersecurity personnel who are up to date on the latest trends in the field.

The third challenge is the lack of available resources. Government organizations often lack the resources necessary to recruit and retain qualified cybersecurity personnel. According to Brown (2017), "many government organizations are unable to offer competitive salaries and benefits to attract and retain top-level cybersecurity personnel." Additionally, these organizations may lack the resources necessary to provide the necessary training and development opportunities to their cybersecurity personnel. As a result, these organizations may struggle to find and retain qualified personnel.

The fourth challenge is the lack of institutional knowledge among cybersecurity personnel. Cybersecurity personnel often have a limited understanding of the internal workings of the organization for which they are working. This lack of knowledge can make it difficult for these individuals to effectively protect the organization from cyber threats. Additionally, it can be difficult for government organizations to ensure that their personnel have the necessary knowledge and skills to identify and respond to cyber threats in a timely and effective manner (Brown, 2017).

The fifth challenge is the difficulty in obtaining security clearances for cybersecurity personnel. Obtaining security clearances is a time-consuming and costly process, and government organizations often lack the resources necessary to obtain the necessary clearances for their personnel (Brown, 2017). Furthermore, the process of obtaining security clearances can be especially difficult for individuals with a criminal background or foreign nationality, making it difficult for government organizations to recruit individuals with the necessary qualifications.

The demand for cybersecurity professionals is increasing, and the skills gap is widening. As a result, organizations are struggling to find qualified cybersecurity workers. Recruiting and retaining Generation Z employees is an important strategy for addressing this challenge.

Generation Z is defined as individuals born between 1997 and 2012 (Joshi et al., 2020). This generation is characterized by their "prolific use of digital technologies," which "has shaped the way they interact with the world" (Joshi et al., 2020, p.3). As such, Generation Z is often referred to as "digital