International Journal of Smart Education and Urban Society
Volume 11 • Issue 4 • October-December 2020

Perspectives in Talent Management Strategies for Cybersecurity Job Roles in Public Safety and Health in Government Organizations

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

Delores Springs, Regent University, USA
https://orcid.org/0000-0003-0940-1225

Sharon L. Burton, Grand Canyon University, USA

Maurice Dawson, Illinois Institute of Technology, USA
https://orcid.org/0000-0003-4609-3444

Jorja B. Wright, University of Charleston, USA

Rajanique Modeste, Capella University, USA
https://orcid.org/0000-0002-6446-7502

ABSTRACT

US government organizations struggle to broaden an entire of government approach to recruit and keep younger cybersecurity talent at a time when national security and intelligence organizations and emergency response agencies are extremely concerned that threats to federal structures and networks from cyber-attacks have never been higher for the state, local, and federal agencies. This study looks to explore innovative options for these agencies to address these employee talents and retention shortages for young information security and information technology professionals.

KEYWORDS

Cybersecurity, Employee Engagement, Employee Motivation, Employee Retention

INTRODUCTION

Technology is changing the nature of many industries. Consider how tremendous technological advances have changed the transportation of healthcare records, specifically through health information technology or health IT (McCoy & Perlis, 2018). As a result, public health-oriented agencies like the Center for Disease Control and National Institutes have new challenges concerning analysis and

DOI: 10.4018/IJSEUS.2020100101

protections of sensitive data from cyberattacks; hence, cybersecurity has become extremely important. These organizations have sensitive public health-oriented missions and require information technology and cybersecurity expertise to carry out these missions effectively. The Center of Disease Control's (CDC, 2019) mission "is to collaborate to create the expertise, information, and tools that people and communities need to protect their health – through health promotion, prevention of disease, injury and disability, and preparedness for new health threats" (CDC, 2019). Table 1 displays the eight concepts that comprise the CDC's mission.

Table 1. The mission of the Centers for Disease Control (CDC, 2012)

Monitor health;
Detect and investigate health problems;
Conduct research to enhance prevention;
Develop and advocate sound public health policies;
Implement prevention strategies;
Promote healthy behaviors;
Foster safe and healthful environments;
Provide leadership and training;

Evidence shows the CDC is a vital agency to the health and well-being of the American population and warrants competent personnel to handle such sensitive data. Consequently, human resource management factors such as "talent hunting, hiring of specialized personnel, employee training and motivation and execution of various policies" (Soomro, Shah, & Ahmed, 2016, p. 219) are a company's responsibility, so asserting that a more "holistic approach should be adopted" for talent management strategies. The preceding statement further corroborates with the CDC's mission. "Each of CDC's component organizations undertakes these activities in conducting its specific programs. The steps needed to accomplish this mission derive from scientific excellence, requiring well-trained public health practitioners and leaders dedicated to high standards of quality and ethical practice" (Centers for Disease Control, 2019).

Like the CDC, the NIH is another essential agency to our society's health in that it is a leading medical research center (National Institute of Health, 2019). NIH's medical discoveries are vital to the health of American citizens because their work has been life-saving (2019) Table 2 displays the goals of the National Institute of Health (NIH) (2019). NIH's mission "is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce the burdens of illness and disability" (2019).

The goals of the agency are shown in Table 2.

Since public health-oriented government agencies collect personal medical information, store information, and analyze personal health-related data, it is imperative to prevent cyberattacks on these organizations because such attacks can be catastrophic. A report from the Center for Strategic and International Studies states, "The damage from cyber-attacks is real. In 2007, the Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities" (Langevin, McCaul, Charney, Raduege, & Lewis, 2008, p. 12). $(ISC)^2$, a top IT and cybersecurity professional organization, substantiates that government agencies are at a higher risk of cybersecurity attacks compared to other sectors (($(ISC)^2$, 2018). Federal agencies reported 43,889 cyber intrusions to the Department of Homeland Security fiscal year 2011 (Johnson, 2012). The U.S. Federal Government employment market for information

Civic Crafting in Urban Planning Public Consultation: Exploring Minecraft's Potential

Lisa Ward Matherand Pamela Robinson (2016). *International Journal of E-Planning Research (pp. 42-58).*

www.irma-international.org/article/civic-crafting-in-urban-planning-public-consultation/158037