Chapter 12
Diversity Leadership Development for Cybersecurity Managers in Healthcare Organizations

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA & University of North Carolina at Chapel Hill, USA

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

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

ABSTRACT

Attacks in the U.S. on Asian American professionals during COVID-19, the #MeToo anti-sexual harassment movement, and the Black Lives Matter protests have led more U.S. cybersecurity organizations to realize the importance of diversity and inclusion training and leadership coaching for their managers. This analysis applies an action research and action learning technique of a multicultural leadership development program leveraging ZOOM. Specifically, this approach was chosen because it fits well for real-world organizational interventions. The relevance of this real-world case study lies in the fact that it could serve as a model for other cybersecurity firms that, due to their limited resources, need help determining how to get started with diversity and inclusion initiatives. This research has significance as cybersecurity firms and departments are attempting to recruit diverse employees to compensate for workforce shortages.

DOI: 10.4018/978-1-6684-7207-1.ch012

INTRODUCTION

In 2020, the worldwide cybersecurity workforce had over 1.5 million open jobs. In order to close this widening gap, companies are looking for candidates with various educational histories, professional experiences, and career trajectories (Burrell & Nobles, 2018). In order to meet the demand, it is necessary to implement talent management and recruitment strategies that can source potential employees from various nations and cultures (Burrell, 2021). Organizations must be more inclusive to do this effectively, and managers must be more culturally competent (Burrell, 2021). As job tasks grow more virtual and technology-driven to incorporate more cross-functional engagement on teams, collaborative activities have become a key element in the design of modern workspaces (Burrell, 2019). As a consequence of this, the cultures of healthy and productive workplaces will continue to be those that become more inclusive and varied on the religious and cultural fronts. This transformation in talent management calls for new abilities to be had by managers and further training for all staff (Burrell, 2019=).

A striking phenomenon is that cybersecurity supervisors and hiring managers are counterbalancing two competing quandaries, a technical one and a people one (Burrell, 2018, 2019, 2021). Many organizations promote technical personnel into management positions believing that technical expertise transfers directly into leadership competencies (Burrell, 2018). However, the professional capacities required of high-performing technical experts might be different from the skills required in leadership roles (Burrell, 2018, 2019, 2021). Technical competence does not transfer into managerial competence as technical skills involve analytical and design, whereas the managerial role requires people skills, decision-making, and teambuilding competencies (Burrell, 2018; Hladio & Edwards, 2017; Burrell, 2019; Burrell, 2021).

Organizations frequently hire computer scientists, information technology professionals, and cybersecurity experts for their technical expertise; however, a current trend is that when personnel, as mentioned above, are promoted, most lack the leadership training and background required to motivate staff, manage performance, and direct and drive change (Burrell, 2018, 2019). Most organizations are only willing to invest in information technology-related training, often focusing on developing managerial and leadership skills for information technology and cybersecurity professionals (Burrell, 2018).

Given that performance is a vital feature of a successful organization, leadership development programs can aid in improving the leadership skills that drive performance. Effective leadership development programs can serve as tools to strengthen the abilities and skills of leaders (Hladio & Edwards, 2017). Leadership development should not be left to chance because effective leadership is critical in implementing organizational transformation (Hladio & Edwards, 2017; Burrell, 2018, 2019, 2021).

The return on investment for leadership development programs is incalculable, given that cybersecurity and information security professionals work tirelessly to prevent cyber-attacks, data breaches, and ransomware attacks from occurring (Burrell, 2018). The average cost of a cyber incident is from 4-6 million dollars, and lack of consumer trust, defaming, and shareholders' loss of confidence; therefore, the actual cost is damaging (Burrell, 2018).

Current research asserts that the current organizational leadership landscape is continually evolving (Hladio & Edwards, 2017; Burrell, 2018, 2019, 2021). It is more complicated, volatile, unpredictable, and challenging for organizations and leaders today (Burrell, 2018, 2019, 2021; Hladio & Edwards, 2017). The skills needed to be an effective organizational leader continue to evolve, requiring strong collaborative thinking, thought leadership, and problem-solving skills that are more innovative and more adaptive; yet, leadership development curriculums and strategies continue to lag behind the advancing business environment (Hladio & Edwards, 2017; Burrell, 2019).