Chapter 69
An Exploration of the Critical Need for Formal Training in Leadership for Cybersecurity and Technology Management Professionals

Darrell Norman Burrell
Florida Institute of Technology, USA

ABSTRACT

For many cybersecurity professionals it is often their technical skills, certifications, and technical academic education that gets them hired and even promoted from a line employee to a management role in technical departments and technical organizations. Being in management roles requires the development of new leadership soft skills that include personality traits, attitudes, habits, and behaviors you display when working with leading, coaching, empowering and developing others. While good soft skills are also important for employees, they are critical for managers - and for those who want to be managers. This article explores that nature of those skills and approaches to help organizations develop leaders in these areas.

BACKGROUND

A striking phenomenon is that cybersecurity leaders and professionals are counterbalancing two competing quandaries, a technical one and a people one (McGettrick et al., 2014; Tasdo, 2016). The skills it takes to engage in cybersecurity Ransomware breach analysis is different than the skills it takes to mentor a new employee in their first job fresh out of an undergraduate program in Cybersecurity or Computer Science. The organizational challenge is that recruiting and developing the talent of current cybersecurity personnel often takes precedence on developing effective supervisory leaders of people (Tsado, 2016). Advanced persistent threats, cyber-attacks, and data breaches are monopolizing the focus

DOI: 10.4018/978-1-5225-8356-1.ch069

on recruiting and hiring over managerial training and development for technical managers. Researchers indicate that executive-level education lags behind the business environment and practices (Arbaiza, 2016), which reflects the lack of leadership development programs specifically for cybersecurity leaders that are transitioning from technical roles to management.

Lester and Parnell (2006) and Brockett (2007) state that many organizations promote technical personnel into management positions believing that technical expertise transfers directly into leadership competencies. However, the professional capacities required of high performing technical experts might not be the same skills required in leadership roles (Lester and Parnell, 2006). 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 (Goldberg, 2006; Rothenberger, 2016; Dzameshie, 2012).

In a recent study, data indicated that 62% of organizations fail to provide sufficient training to maintain situational awareness on business and information technology risks (Oltsik, 2017. According to (Oltsik, 2017), another disquieting data point is that cybersecurity and information technology professionals need more business training to enhance the technicians' career and business development.

Based on the above suppositions, transitioning from a technical role to a leadership role has many challenges, particularly for information technology (IT) and cybersecurity professionals (Lester & Parnell, 2006; Rothenberger, 2016; Dzameshie, 2012). These challenges include having the social capital (people and soft skills) and leadership competencies to manage and lead employees that are non-technical (Brokett, 2007; Lester & Parnell, 2006). A technical manager might have superb expertise but struggle with transitioning from managing in the technical space to leading people in a complex organization (Dzameshie, 2012; Evans, 1992; Rothenberger, 2016). Often, information technology managers lack adequate leadership experience, skills, and preparation, particularly in communication and delegation (Dzameshie, 2012; Rothenberger, 2016) as well as the business savviness to drive information security practices for the enterprise. With evolving changes to risk management and regulatory enforcement, many companies are task saturated with cybersecurity requirements that were once channeled into offices of senior cybersecurity and information technology leaders; consequently, keeping these leaders directly involved in technical operations rather than directing cybersecurity operations for the enterprise. Hansib (2014), a cybersecurity expert, articulates that cybersecurity is a business strategy; therefore, requiring an organizational-wide approach to execute efficiently. Now that cybersecurity is widely being accepted as a business strategy, senior information technology and cybersecurity leaders are engaging in executive-level functions; however, at the cost of not developing, training, and mentoring aspiring subordinates—due to task saturation.

According to Lester and Parnell (2006) and Brokett (2007), the underlying dilemma with IT professionals is that fundamental aspects of their jobs pertain to working on computers, computer networks, and technologies, which often afford limited opportunities to interact with sizeable contingencies of personnel on a daily basis. Frequently, organizations hire computer scientists, information technology professionals, and cybersecurity experts for their technical expertise; however, a current trend is when aforementioned personnel are promoted most lack the leadership training and background required to motivate staff, manage performance, and to direct and drive change. Often most organizations are only willing to invest in information technology related training often neglecting the development of managerial and leadership skills for information technology and cybersecurity professionals.

Technical supervisors and leaders require an in-depth understanding of leading and managing employees (Rothenberger, 2016; Dzameshie, 2012). Watkins (2013) and Gabarro (2007) note that managers