Cyberforce Education Pipeline – A U.S. Department of Defense Solution

Andre Slonopas, Warren Thompson, and Kenneth L. Williams
Center for Cyber Defense
American Public University System (APUS)

Abstract
Cybersecurity training and education is a major concern at all levels of the modern organization. This concern is especially amplified within government due to the evolution of risk from the use of physical to cyber capabilities. The typical government employee is increasingly expected to achieve levels of awareness, education, and training to amplify skills, knowledge, and abilities that are profoundly different from those found in the private section. Organizational leadership's daily decisions are bookended by risks from the use of cyberspace. – In prior years employees were equipped to assist at a fraction of the cost - whereas now greater level of awareness, education, and training is desired. The key question is how to achieve security in modern organization especially in those with a government mission The requirements for increased level of awareness, education, and or training can be kept internal or turned over to traditional organizations such as universities and others to assist. The solution to these challenges materializes through the actions of the organization, the individual employee, and the educating and training entities such as universities and trade schools. The effectiveness of these efforts by the various entities on risk mitigation is explored. This leverages search of the literature and reports from the popular culture to examine the efficacy of current efforts. The paper narrows its focus on the typical governmental organization and its associated risks from the use of the cyberspace. The paper presents recommendations to the government organization and assists in the achievement of risk reduction related to the use of the cyberspace and the management of the cyber-force pipeline.

References


