The Business of Teaching Cyber Security

Alysyn Harvey-Green, Edgar Maldonado, Vickie Seehusen
Metropolitan State University of Denver
August 2021

Abstract:

Evidence suggests that all employees who are uninformed in basic cyber security threats, vulnerabilities and counter measures can pose real dangers to an organization's information technology resources. Nevertheless, there appears to be little to indicate what type of cyber security education students in non-computer related programs are exposed to in their respective majors. Universities and colleges have responded with a plethora of cyber security degrees and certificate programs across the country and throughout the world. Higher education is a major player in this arena.

In AACSB schools, students in business majors are generally required to take one or more information systems or information technology courses as a part of their degree. The authors of this paper reviewed the catalog descriptions of 542 AACSB accredited colleges core information systems/technology courses. Specifically, the authors looked for indicators or security training, security awareness or security topics in general. Upon identifying a list of words, each catalog description was categorized as having included or not having included some form of cyber security training. The authors found that 16% of AACSB schools mention security awareness or training in the catalog descriptions for their core IS/IT courses. Given the exponential growth of cyber security dangers, the authors contend that a more formalized approach to training and awareness is required for all business majors. Future research will look at complete syllabi from participating AACSB programs focusing on whether security is taught in the core courses, regardless of catalog description.