Information Security Education Journal Volume 2 Number 1 June 2015

Contents

FROM THE EDITORS

What Should We Teach? Everything!!

Welcome to the third issue of the Information Security Education Journal (ISEJ). On behalf of the editorial team, we thank you for taking the time to read this issue and strongly encourage you to consider submitting an article to be considered for upcoming editions.

In April of this year Kennesaw State University hosted the annual Southeast Collegiate Cyber Defense Competition. This was preceded a month earlier by a virtual qualifying round since 23 teams were interested in competing on site. The top 8 teams from the qualifying round made their way to our northern most campus during our Spring break. We take great pride in promoting information security education through one of our two marquee events (the other one being the Information Security Curriculum Development Conference). For the past couple of years, part of the competition involves students meeting with recruiters from the public as well as the private sector. In our opinion this is an opportunity for recruiters to meet with what we consider to potentially be the top information security talent in the Southeast.

This year we saw more recruiters explicitly stating that they would like the future "cyber warriors" to be trained in offensive skills. Of course, this statement is always a little strange since we are at a cyber "defense" competition. We understand the interest in students with offensive capabilities, since most of the individuals interested in these "cyber warriors" are mostly TLAs (Three Letter Agencies) - U.S. Federal Agencies, Department of Defense military or civilian defense contractors, authorized to conduct such actions. However, we also understand that demand for offensively trained or at least capable is not without merit. Some also argue that the offensive mindset is the domain of a more technical information security degree. Should we teach more offense in our curriculum? If so, what should we remove? As a degree granting institution, we are limited to a certain number of credit hours that students need to take. An unlimited option would be great, but it's not feasible.

In our undergraduate information security and assurance program, the closest we come to an offensive course is an elective on penetration testing. Even in that course, students learn to write reports and look at things strategically. Why do that? Let's consider the information security climate. We have very popular technical conferences such as Black Hat, Def Con, and BSides. We agree that it's important to have students who have mastery over "in the weeds" technical aspects of network security. However, we also believe in assisting with developing a more mature and balanced workforce. It is important to consider both the vertical and technical, and the more horizontal and strategic aspects of information security. This is reflected in our curriculum, which is a balance between technical (e.g. network security, systems security etc.) and managerial (incident response, management of security etc.). We have been positively reviewed by folks in industry, which has also culminated in students being recruited at a higher than average rate at a very young stage of their academics. But we continue to have conversations at the industry and academic levels to ensure that we remain relevant to what the field requires. That is something we believe everyone should be doing.

We hope you enjoy the latest issue.

Michael E. Whitman, Ph.D., CISM, CISSP, Editor in Chief
Herbert J. Mattord, Ph.D., CISM, CISSP, Senior Editor
Humayun Zafar, Ph.D., Senior Editor
Kennesaw State University, GA, USA
infosec@kennesaw.edu

For a complete listing of the Associate Editors, or to submit a manuscript please visit the ISEJ web site at: http://socio.org.uk/isej/

Editors