Journal of Cybersecurity Education, Research and Practice

Volume 2016
Number 2 *Two*

Article 1

December 2016

From the Editors

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Carole L. Hollingsworth
Kennesaw State University, chollin2@kennesaw.edu

Recommended Citation

Mattord, Herbert J.; Whitman, Michael E.; and Hollingsworth, Carole L. (2016) "From the Editors," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2016 : No. 2 , Article 1.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2016/iss2/1

From the Editors

Abstract

Welcome to the second issue of the Journal of Cybersecurity Education, Research and Practice (JCERP).

Keywords

editorial, cybersecurity defined

FROM THE EDITORS

Welcome to this issue of the Journal of Cybersecurity Education, Research, and Practice (JCERP). 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.

For this issue's editorial, we thought we would share some thoughts on where cybersecurity comes from and what a cybersecurity graduate should know. Cybersecurity is a computing-based discipline involving technology, people, information, and processes to enable assured operations. It draws from the fields of information systems, information technology, computer science, criminal justice, law and business, and began with computer security.

The need for cybersecurity arose when the first mainframe computers were developed. During the early years, cybersecurity as practiced, even if not specifically identified as such, was a straightforward process composed predominantly of physical security and document classification. The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage.

In the early 1980s, the development of TCP (the Transmission Control Protocol) and IP (the Internet Protocol) led to the emergence of the Internet brought the networking aspects of Cybersecurity to the fore. The Internet eventually brought pervasive connectivity to virtually all computers where integrity and confidentiality were a lower priority than the drive for availability where many problems that plague the Internet today result from this early lack of security.

The Internet brings millions of unsecured computer networks and billions of computer systems into continuous communication with each other. The security of each computer's stored information is contingent on the security level of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve cybersecurity, as well as a realization that cybersecurity is important to national defense. The growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure. Another growing concern is the threat of nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

Though it may be known by other names, such as information security, information assurance, IT security or data security, cybersecurity is perceived by most in the information technology industry as a critical discipline on par with software development, networking, database management and the many other disciplines that made up the modern computing ecosystem. Each of these disciplines requires practitioners to be thoroughly grounded in the theoretical aspects of each specialty, learned skills to implements sound practices and ongoing professional education to maintain currency.

Cybersecurity is emerging as an identifiable discipline due to the need for specialists that are focused on the objectives of integrity, confidentiality and non-repudiation. The cybersecurity discipline has arisen since other computing disciplines have not been able to prepare specialist for the complexities and specific understanding of those complexities required to assure secure operation of cybernetic systems.

Cybersecurity as an identifiable degree field is still in its infancy. It has developed from the disciplines of information security, computer security and information technology security. Driven by significant workforce needs, educational programs are being developed nationwide. That workforce demand is acute and immediate. Findings from the International Information Systems Security Certification Consortium (ISC)^2 workforce survey predict that by 2020 there will be a global shortage of 1.5 Million cybersecurity professionals (National Institute of Standards and Technology / National Initiative for Cybersecurity Education (NIST/NICE) Workforce Demand Report, 2015).

We believe that each graduate of a program of study identifying itself as a cybersecurity program should have a core cybersecurity curriculum that includes: (1) cybersecurity's inherent adversarial mindset, (2) an information technology and computer science foundation, (3) core cybersecurity knowledge and skills, (4) a range of specializations meeting the in-demand domains identified in the NIST/NICE Cybersecurity Workforce Framework, and (5) a strong legal and ethical approach to the responsibility for information protection.

The mission of JCERP is to be the premier outlet for high-quality information security and cybersecurity related articles of interest to teaching faculty and students.

The JCERP Editorial Team:

Michael E. Whitman, Ph.D., CISM, CISSP, Co-Editor in Chief
Herbert J. Mattord, Ph.D., CISM, CISSP, Co-Editor in Chief
Carole Hollingsworth, DBA, 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 JCERP Web site at digitalcommons.kennesaw.edu/jcerp/