Chapter 9
Innovative Legitimate Non-Traditional Doctorate Programs in Cybersecurity, Engineering, and Technology

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA & Capitol Technology University, USA

Calvin Nobles
https://orcid.org/0000-0003-4002-1108
Illinois Institute of Technology, USA

Maurice Dawson
https://orcid.org/0000-0003-4609-3444
Illinois Institute of Technology, USA

Eugene J. M. Lewis
https://orcid.org/0000-0002-2956-0760
Capitol Technology University, USA

S. Raschid Muller
https://orcid.org/0000-0002-1742-7575
Capitol Technology University, USA

Kevin Richardson
Edward Waters University, USA

Amalisha S. Aridi
Capitol Technology University, USA

DOI: 10.4018/978-1-7998-9430-8.ch009

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

ABSTRACT

According to the US Federal Bureau of Investigations (FBI) the number of complaints about cyberattacks to their cyber division is up to as many as 4,000 a day. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cybersecurity-related roles. Colleges and universities have created certificate, undergraduate, and graduate programs to train professionals in these job roles. The challenge to meeting the cybersecurity workforce shortage through degree programs is intensified by the reality of the limited number of cybersecurity and engineering faculty at colleges and universities. This chapter explores the essential need to develop more doctorate faculty in technology-related areas and explains some unique and non-traditional paths to doctoral completion that allow professionals with significant real-world work experience to complete a doctorate without career interruption and relocation from highly respected and established universities in the US and the UK.

INTRODUCTION

According to the US Federal Bureau of Investigations ([FBI] 2021) the number of complaints about cyberattacks to their Cyber Division is up to as many as 4,000 a day. That represents 400% increase (FBI, 2021). The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack (FBI, 2021). According to Newman (2016), the cybersecurity threat landscape is continually evolving as malicious cyber actors pursue new vectors to target and capitalize on newly discovered or known vulnerabilities. In 2017 a hacking group known as the Shadow Brokers, claiming to have breached the NSA-linked operation known as the Equation Group. The Shadow Brokers provided samples of the stolen data and attempted to auction off other stolen data (Newman, 2017).

In May of 2017, a strain ransomware virus call WannaCry attacked a series of public and private organizations including temporarily crippling technology-driven operations of several hospitals and medical facilities in the United Kingdom (Newman, 2017). In 2017 there where new revelations about hacking vulnerabilities cell phones, Windows, and the ability to turn some smart TVs into listening devices (Newman, 2017). The top industries targeted by cybercriminals are (1) healthcare, (2) manufacturing, (3) financial services, (4) government, and (5) transportation (Morgan, 2016). These industries are targeted for sensitive information primarily in the healthcare and financial services sectors. Researchers are forecasting the global cost of cybercrime in 2019 to reach over 2 trillion dollars (Morgan, 2016).

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/innovative-legitimate-non-traditional-doctorate-programs-in-cybersecurity-engineering-and-technology/311377

Related Content

Vulnerability Assessment and Malware Analysis of Android Apps Using Machine Learning

Pallavi Khatri, Animesh Kumar Agrawal, Aman Sharma, Navpreet Pannuand Sumitra Ranjan Sinha (2021). *Handbook of Research on Machine Learning Techniques for Pattern Recognition and Information Security (pp. 255-277).*

www.irma-international.org/chapter/vulnerability-assessment-and-malware-analysis-of-android-apps-using-machine-learning/279915

A Comprehensive Study of Data Analytics in Social Perspectives

Arram Sriram, Prasanth Rao Adhiraju, Praveen Kumar Kalangiand Sathiyamoorthi V. (2021). *Challenges and Applications of Data Analytics in Social Perspectives (pp. 257-274).*

www.irma-international.org/chapter/a-comprehensive-study-of-data-analytics-in-social-perspectives/267250

Using Machine Learning to Predict Women at Risk Having a Child With Congenital Heart Defects

Amany Abdo, Asmaa Mostafa Mosallamand Laila Abdel-Hamid (2025). *International Journal of Artificial Intelligence and Machine Learning (pp. 1-19).*

www.irma-international.org/article/using-machine-learning-to-predict-women-at-risk-having-a-child-with-congenital-heart-defects/373196

Rule Extraction in Trained Feedforward Deep Neural Networks: Integrating Cosine Similarity and Logic for Explainability

Pablo Ariel Negroand Claudia Pons (2024). *International Journal of Artificial Intelligence and Machine Learning (pp. 1-22).*

www.irma-international.org/article/rule-extraction-in-trained-feedforward-deep-neural-networks/347988

Early Warning System Framework Proposal, Based on Big Data Environment

Goran Klepac, Robert Kopaland Leo Mrsic (2019). *International Journal of Artificial Intelligence and Machine Learning (pp. 35-66).*
www.irma-international.org/article/early-warning-system-framework-proposal-based-on-big-data-environment/233889