River Publishers

Cybersecurity Leadership for Healthcare Organizations and Institutions of Higher Education

Authors:

Bradley Fowler, Member of National Cyber Watch Association, USA

Bruce G. Chaundy, Southern New Hampshire University, USA

Healthcare organizations and institutions of higher education have become prime targets of increased cyberattacks. This book explores current cybersecurity trends and effective software applications, AI, and decision-making processes to combat cyberattacks. It emphasizes the importance of compliance, provides downloadable digital forensics software, and examines the psychology of organizational practice for effective cybersecurity leadership.

Since the year 2000, research consistently reports devasting results of ransomware and malware attacks impacting healthcare and higher education. These attacks are crippling the ability for these organizations to effectively protect their information systems, information technology, and cloud-based environments. Despite the global dissemination of knowledge, healthcare and higher education organizations continue wrestling to define strategies and methods to secure their information assets, understand methods of assessing qualified practitioners to fill the alarming number of opened positions to help improve how cybersecurity leadership is deployed, as well as improve workplace usage of technology tools without exposing these organizations to more severe and catastrophic cyber incidents.

This practical book supports the reader with downloadable digital forensics software, teaches how to utilize this software, as well as correctly securing this software as a key method to improve usage and deployment of these software applications for effective cybersecurity leadership. Furthermore, readers will understand the psychology of industrial organizational practice as it correlates with cybersecurity leadership. This is required to improve management of workplace conflict, which often impedes personnel's ability to comply with cybersecurity law and policy, domestically and internationally.

TABLE OF CONTENTS

Acknowledgements
Introduction
Author's BIO

Chapter One Current Trends in Cybersecurity Leadership
Summary
Case Study
Discussion Questions
Glossary

Chapter Two Cybersecurity Leadership for Healthcare Organizations
Summary
Case Study
Discussion Questions
Glossary

Chapter Three Cybersecurity Leadership for Institutions of Higher Education
Summary
Case Study
Discussion Questions
Glossary

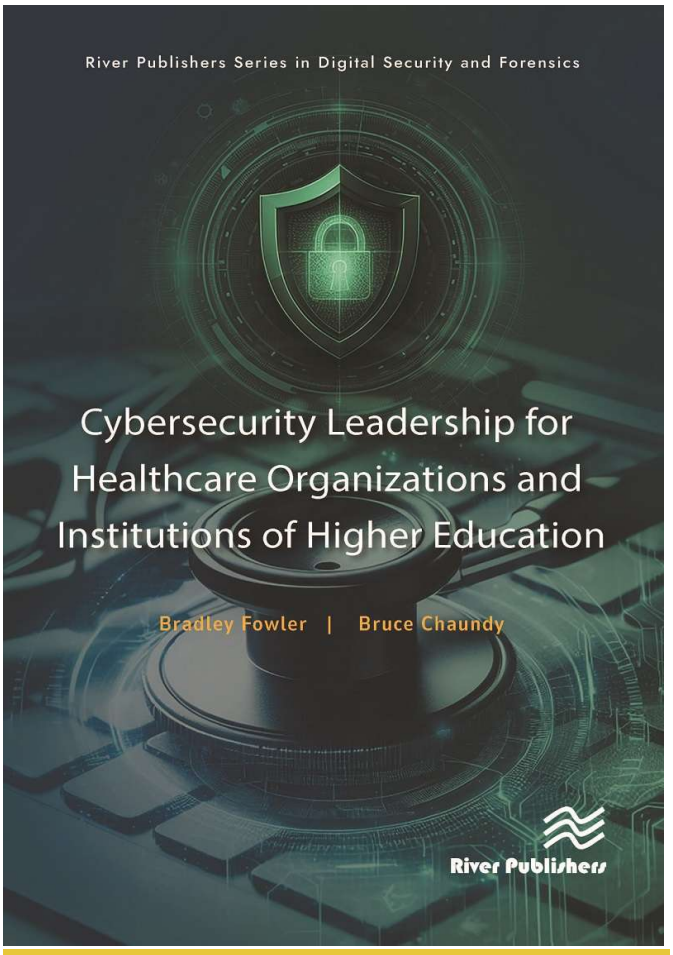
Chapter Four Penetration Testing
Summary
Case Study
Discussion Questions
Glossary

Chapter Five Cybersecurity Forensics Tools and Usage Techniques
Summary
Case Study
Discussion Questions
Glossary

Chapter Six Artificial Intelligence for Cybersecurity Leadership
Summary
Case Study
Discussion Questions
Glossary

Chapter Seven Psychology of Industrial Organizational Cybersecurity Leadership
Summary
Case Study
Discussion Questions
Glossary

References
Index



River Publishers Series in Digital Security and Forensics

ISBN: 9788770042345
e-ISBN: 9788770042338
Available From: February 2025
Price: $ 140.00

KEYWORDS:
Cybersecurity leadership, artificial intelligence, machine learning, natural language processing, Brain virus, executable code, Morris worm, Sputnik, distributed denial of service attack, ransomware attacks, phishing, whaling, social engineering, Bugs, CIA Triad, dark web, interface engines, service level agreements, interoperability, use case, algorithm, man-in-the-middle, cryptology, Continuous Internal Penetration Testing, white-hat hacker, ethical hacker, black-hat hacker, grey-hat hacker, war driving, brute force attack, dictionary attack, Digital forensics, inculpatory, exculpatory, packet sniffing, pharming, generative artificial intelligence, Intellectual property, maliciousness, Managed Detection and Response, and negligent insider.

www.riverpublishers.com
marketing@riverpublishers.com