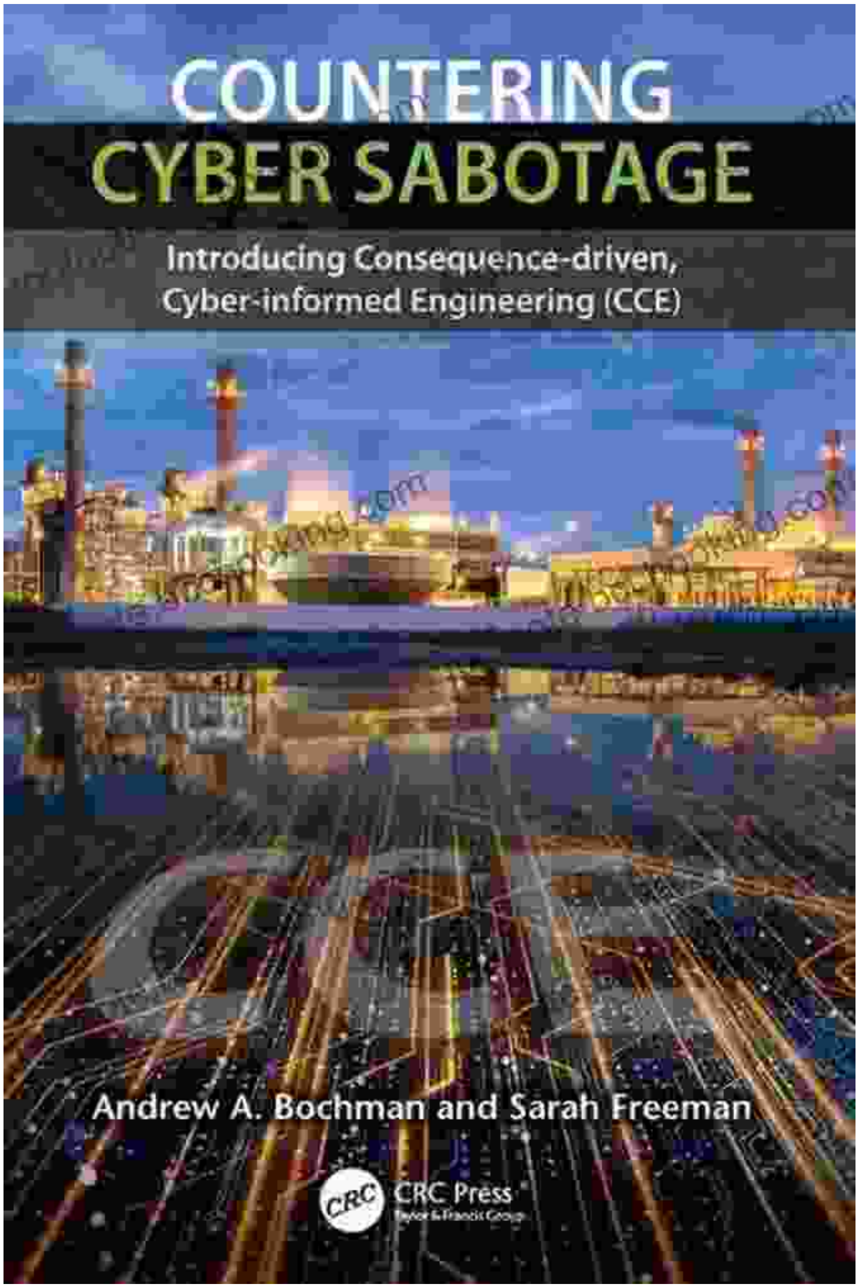
Introducing Consequence Driven Cyber Informed Engineering (CCE): Transforming Cybersecurity Through Human Factors and Systems Engineering


COUNTERING
CYBER SABOTAGE
Introducing Consequence-driven, Cyber-informed Engineering (CCE)
Andrew A. Bochman and Sarah Freeman
CRC Press
Taylor & Francis Group

Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)

by Mohammed Hamed Ahmed Soliman

★★★★☆ 4.8 out of 5

Language	: English
File size	: 36844 KB
Print length	: 314 pages
Screen Reader	: Supported

Table of Contents

Chapter 1: to Consequence Driven Cyber Informed Engineering (CCE)

In the rapidly evolving landscape of cybersecurity, organizations face unprecedented challenges in protecting their critical systems and data. Traditional approaches to cybersecurity have focused primarily on technical solutions, such as antivirus software and firewalls, which are often reactive and ineffective against sophisticated cyber threats.

Consequence Driven Cyber Informed Engineering (CCE) emerges as a revolutionary approach that bridges the gap between cybersecurity and human factors engineering. It recognizes that human behavior plays a significant role in cybersecurity incidents and that understanding the consequences of cyber events is crucial for effective risk management.

This chapter introduces the fundamentals of CCE, including its key principles, benefits, and the critical role it plays in enhancing cybersecurity posture and resilience.

Chapter 2: Foundations of Human Factors and Systems Engineering in Cybersecurity

CCE draws upon the well-established principles of human factors engineering and systems engineering. This chapter provides a thorough grounding in these disciplines, exploring their application in cybersecurity and highlighting their importance in understanding human behavior, system vulnerabilities, and organizational processes.

Through case studies and real-world examples, this chapter demonstrates how human factors and systems engineering principles can enhance cybersecurity practices, such as user interface design, risk assessment, and incident response.

Chapter 3: Applying CCE to Cybersecurity Risk Management

Risk management is at the heart of cybersecurity. CCE provides a structured framework for identifying, analyzing, and mitigating cyber risks. This chapter explores the application of CCE principles to cybersecurity risk management, guiding organizations in developing a comprehensive risk management program.

Readers will gain practical insights into risk assessment techniques, threat modeling, and the development of effective risk mitigation strategies that consider both technical and human factors.

Chapter 4: CCE in Practice: Case Studies and Implementation

This chapter brings CCE into the real world through a series of in-depth case studies. Cybersecurity professionals and engineers will delve into real-life examples of CCE implementation in diverse industries, covering sectors such as healthcare, finance, and energy.

Through detailed analysis of these case studies, readers will witness the practical benefits of CCE and gain valuable insights into its effective implementation and integration with existing cybersecurity practices.

Chapter 5: The Future of CCE in Cybersecurity

As the cybersecurity landscape continues to evolve, CCE is poised to play an increasingly vital role in shaping the future of cybersecurity practices. This chapter explores the emerging trends and advancements in CCE, including the integration of artificial intelligence, machine learning, and cognitive computing.

Readers will gain a glimpse into the future of CCE and its potential to transform cybersecurity, empowering organizations to proactively manage cyber risks and achieve unprecedented levels of resilience.

Consequence Driven Cyber Informed Engineering (CCE) is a game-changer in the world of cybersecurity. By integrating human factors and systems engineering principles into cybersecurity practices, organizations can achieve a holistic and proactive approach to risk management and resilience.

This comprehensive book provides an indispensable resource for cybersecurity professionals, engineers, and anyone seeking to enhance their organization's cybersecurity posture. Through its in-depth exploration of CCE principles, case studies, and future trends, this book empowers readers with the knowledge and tools to implement this transformative approach and safeguard their organizations against the ever-evolving cyber threats.

Buy Now

Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)

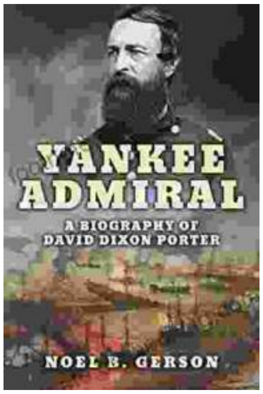
by Mohammed Hamed Ahmed Soliman

★★★★☆ 4.8 out of 5

Language	: English
File size	: 36844 KB
Print length	: 314 pages
Screen Reader	: Supported

Unveiling the Enchanting Realm of "Skyhunter" by Marie Lu: A Literary Odyssey into an Unseen World

A Literary Odyssey: Journey to an Unseen World Prepare yourself for an extraordinary literary journey as you delve into the pages of...



Heroes and Villains from American History: The Biography of David Dixon Porter

David Dixon Porter was an American naval officer who served during the Civil War. He was a skilled commander and strategist, and he played a key...