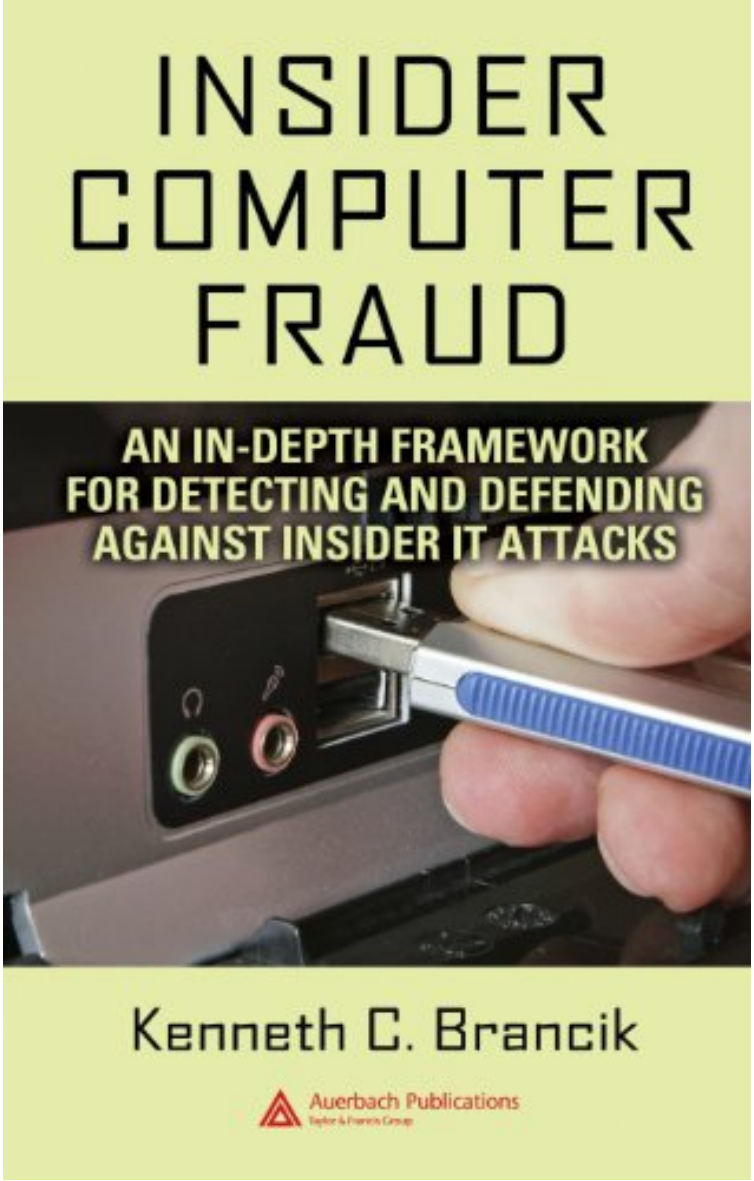
Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks

Kenneth Brancik
**Download PDF | ePub | DOC | audiobook | ebooks*



#4190318 in eBooks 2007-12-06 2007-12-06File Name: B00A8SLS7I | File size: 73.Mb

Kenneth Brancik : Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks before purchasing it in order to gage whether or not it would be worth my time, and all praised Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks:

2 of 2 people found the following review helpful. Highly recommend - well written and must readBy ISCI really

enjoyed reading this book. It provides a comprehensive framework for understanding insider threats and Risk management.The author integrates a lot of components like Risk Assessment, Threat Modeling, Privacy assessment, Cyber security, Application security, Web services and Computer architecture as it relates to insider threat identification and prevention. If you deal with any of these components - you must read this book. You will learn so much - all in one place.This book is logically arranged; the author does an excellent job building from one topic to another. It is an eye-opening and fascinating book as it presents the methods, safeguards, and techniques that help protect an organization from insider computer fraud.I really liked Chapter 3 which covered Risk Assessment very well. It walks the reader with a step by step risk assessment methodology, which is very critical in any environment.As a IT Security professional this book has become an invaluable resource for me.Bottom line: Must read and well worth the price.0 of 0 people found the following review helpful. Inside the Insider ThreatBy GoldBrancik covers computer fraud from every angle imaginable. It's precise, thorough and methodical. The index is detailed and specific in getting the exact information you need quickly. This book can be used as a reference for looking to tighten security and also as a textbook in the classroom. I specifically liked Chapter 6 that covered web services, which is the most widely missed security flaw in companies today.Brancik put together a fraud taxonomy that also can be used by professionals to measure how secure they are. This goes beyond most classroom lectures because this is the kind of information you need in real life work scenarios. What I liked mostly about this book was that the chapters flow into one another and while it covered a wide range of topics it did not feel like I was reading just another computer textbook. The book covers security and audit like no other book on the market and I have read most of them being in the banking sector for a number of years. I recommend this book highly.2 of 2 people found the following review helpful. Great textbook without the "textbook" feelingBy B. H. Edington"Insider Computer Fraud" is a comprehensive overview that gives anyone, even computer novices, a solid framework of the topic. A topic of such breadth could overwhelm many individuals, but Brancik manages to divide the material into edible chunks that inform without drowning the reader in excess. If you scan the contents you can easily identify the area you want to focus on -- the well thought out design of the book is a real plus.For professors looking for a textbook on this subject, "Insider Computer Fraud" is a good option. Each topic adds onto the prior chapter and gives a logic sequence to the material.Interesting sub-topics such as the Novelty Neural Network and The Brain will capture the reader's attention. A good mix of theory and application makes this book a good choice for anyone interested in increasing their knowledge of a highly complex subject.

An organizationrsquo;s employees are often more intimate with its computer system than anyone else. Many also have access to sensitive information regarding the company and its customers. This makes employees prime candidates for sabotaging a system if they become disgruntled or for selling privileged information if they become greedy. Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks presents the methods, safeguards, and techniques that help protect an organization from insider computer fraud. Drawing from the authorrsquo;s vast experience assessing the adequacy of IT security for the banking and securities industries, the book presents a practical framework for identifying, measuring, monitoring, and controlling the risks associated with insider threats. It not only provides an analysis of application or system-related risks, it demonstrates the interrelationships that exist between an application and the IT infrastructure components it uses to transmit, process, and store sensitive data. The author also examines the symbiotic relationship between the risks, controls, threats, and action plans that should be deployed to enhance the overall information security governance processes. Increasing the awareness and understanding necessary to effectively manage the risks and controls associated with an insider threat, this book is an invaluable resource for those interested in attaining sound and best practices over the risk management process.

About the AuthorInformation Security Consultant, New York