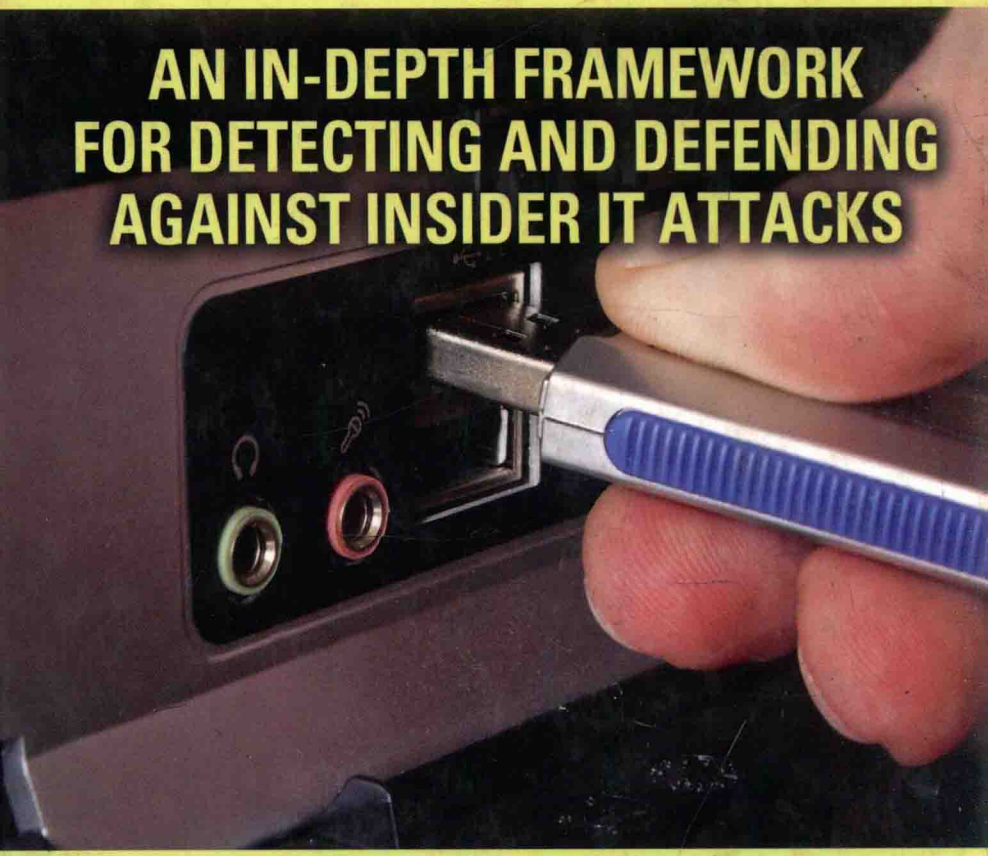
INSIDER COMPUTER FRAUD

AN IN-DEPTH FRAMEWORK FOR DETECTING AND DEFENDING AGAINST INSIDER IT ATTACKS



Kenneth C. Brancik

Auerbach Publications
Taylor & Francis Group

INSIDER COMPUTER FRAUD

AN IN-DEPTH FRAMEWORK FOR DETECTING AND DEFENDING AGAINST INSIDER IT ATTACKS

Kenneth C. Brancik

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Auerbach Publications is an imprint of the
Taylor & Francis Group, an **informa** business

The fundamental research and writing of this book preceded my employment at VerizonBusiness. The opinions, analysis, and writings are my own and were based on my computer science research as a former Doctoral student at Pace University, New York.

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-4659-5 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Brancik, Kenneth C.
Insider computer fraud : an in-depth framework for detecting and defending against insider IT attacks / Kenneth Brancik.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4200-4659-5 (alk. paper)
1. Computer security . 2. Computer crimes. I. Title.

QA76.9.A25B725 2007
005.8--dc22 2007017696

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

INSIDER COMPUTER FRAUD

AN IN-DEPTH FRAMEWORK FOR DETECTING AND DEFENDING AGAINST INSIDER IT ATTACKS

Dedication

This book is dedicated to my Mother, who took care of four young adults; when my Father passed away early in my life, she was suddenly forced to reenter the job market, while still providing her family the care and support we all needed during our growing years through adulthood. I owe my strong work ethic and dedication to my personal goals to her and the good example she has demonstrated over many years as a supportive parent.

Preface

The insider threat has for too long been overlooked by many organizations in conducting their risk assessments and threat analysis processes. The financial and reputation risks may be high for organizations who fall victim to nefarious activities of an insider involving current or former employees, contractors, or perhaps trusted clients who are afforded similar access rights to applications, systems, and data as an employee; and the cost of ignoring preventative security solutions could become comparatively even higher in the long-term.

Information security concerns do not typically evaporate over time, but rather can evolve from what appears to be an isolated problem, to a systemic risk that has enterprise-wide implications. The enterprise-wide information security risks can be created by both external and internal threats; however, the latter risk is typically overlooked by many organizations. In an organization, the absence of evaluating the risks posed by the insider threat can have a deleterious effect on the information security governance process and can cause many negative consequences, including an increased level of risk to operations, finance, reputation, and strategy.

The absence of an effective information security governance process may lend itself to increased regulatory oversight, particularly when the risk involves the need for ensuring the safeguarding of sensitive nonpublic private information (NPPI) data. The need to safeguard NPPI data from both internal and external threats is also the focus of numerous states imposing breach notification laws and the pending federal legislation (Data Accountability and Trust Act [DATA]), which will mandate customer breach notification involving unauthorized access to NPPI data.

All roads within *Insider Computer Fraud: An In-Depth Framework for Detecting and Defending against Insider IT Attacks* point to the importance of maintaining strong security controls first. Then, using completed comprehensive and integrated data flow diagrams, the transactions transmission and storage life cycle (critical path) will be traced. The critical path will show the transmission and ultimate storage of NPPI and critical core transaction data elements, which will be useful for determining the assigned control points throughout the critical path where access controls, data origination and input, processing, and output controls exist.

Kenneth C. Brancik, PhD, CISA, CISSP, ITIL

Key Features

The primary goal of this book is to introduce the reader to the topic and problem of insider computer fraud (ICF), and to suggest a practical framework or methodology that can be used by any private-sector organization or government agency for identifying, measuring, monitoring, and controlling the risks associated with the insider threat. This book is not intended to offer a prescriptive process that requires a series of steps, which absolutely must be performed in order to benefit from any one step or process that is discussed in the ICF framework. The layers within the "Defense in Depth Model" used to mitigate ICF risks will be management's decision based on the results of their risk and privacy assessment; threat modeling; and decision to accept, transfer, or mitigate that risk. This book is not intended to provide exhaustive controls assessment for applications, systems, or any separate component of the information technology (IT) infrastructure of an organization. However, a horizontal analysis of application and system related risks is provided, and the interrelationships between an application and the IT infrastructure components it uses to transmit, process, and store the data will be demonstrated.

The book is process driven, to help in understanding both management and technical controls and how the two operating in concert have a positive synergistic impact in reducing ICF activity as well as reducing the risks over external threats. Although the primary thrust of the book focuses on the insider threat, many of the risks and controls apply equally to both internal and external threats in varying degrees. There is a symbiotic relationship that exists between the risks, controls, threats, and action plans that should be deployed to enhance overall information security governance processes.

The material presented will be beneficial to not only management, but the audit and compliance community as well. Where appropriate, the integrated risk assessment approach used to identify, measure, monitor, and control risks will aid auditors, compliance and privacy officers, regulatory examiners, and others who seek sound and best practices over the risk management process.

Based on the minimal amount of data available within the public domain on the insider threat and computer fraud, one of the primary goals of this book is to provide an orientation on an elusive topic for which the information is either not

readily available or the data may lack the credibility to justify the development of a risk management strategy and action plans. The mitigation and prevention of financial losses associated with the insider threat can be mitigated or, hopefully, prevented if management deploys the appropriate safeguards based almost exclusively on deploying the *Defense in Depth* concept, with its foundation based on logic, cost effectiveness, and management's appetite or tolerance for risk.

The reader of this book will gain a familiarity with the following concepts that are all related to understanding the risks and controls surrounding ICF activity:

- *Strategic Planning Process*: The Insider Threat Strategic Planning Process is discussed in detail.
- *Risk Governance Process*: How an effective risk governance process for identifying ICF activity should be implemented is discussed.
- *Risk Categorization and Assessment*: The differences and similarities in determining inherent, residual, and net residual risk and how to integrate the threat assessment process into the risk assessment process are presented.
- *Risk and Threat Assessment Processes*: The interrelationship between the risk assessment and the threat assessment processes is covered.
- *The Defense in Depth Model and Security Efficiency Calculation*: Using Bayes' Theorem, the efficiency and effectiveness of each layer of protection in the Defense in Depth Model are quantified to assist management in their information security (InfoSec) strategic planning and risk reduction processes for both internal and external threats.
- *Application Security*: Industry sound and best practices are discussed in context with interrelated risks found within other IT infrastructure components and software (optimizers).
- *Penetration Testing*: Penetration testing criteria for Web-based applications, which could leave those applications vulnerable to both internal and external threats, are addressed.
- *Web Services Security*: Web services and supporting applications introduce security risks for internal and external threats. The knowledgeable insider can have greater access to and internal knowledge of the Service Oriented Architecture of an enterprise, which supports the use of Web services and the development activities of the applications and systems used to transmit data and messaging, leaving those applications and systems with an increased vulnerability.
- *Insider Computer Fraud Identification*: The importance of using various diagnostic tools for assessing ICF misuse detection using key risk indicators is discussed in detail. The key risk indicators include key fraud indicators (KFIs), key fraud metrics (KFMs), and key fraud signatures (KFSs), based on performing macro and micro taxonomies of a critical application.

- *Control Point Identification and Forensic Foto Frames*: Based on the critical path of nonpublic private information (NPPI) and core data elements of transaction data of critical applications, control points (access controls, data origination and input, processing, and output) can be identified, measured, monitored, and controlled through data capture activity and other means. The data capture activity will be performed through the execution of the Forensic Foto Frame process that will collect key data by taking a "snapshot" of that data at stated control points. The snapshot of the data will be collected by the continuous Forensic Foto Frame process, and over time it will provide the necessary data to conduct an analysis of the normalcy of the captured data's behavior. The primary goal of the Forensic Foto Frame process is the profiling of the data versus the initial profiling of the behavioral characteristics of the insider. The behavioral characteristics or data profiling process will take the absolute values of each Forensic Foto Frame captured and begin the process of analyzing data normalcy in the context of a given set of variables. The variables may include but not be limited to the name of the insider who executed the transaction or processed the data. The metadata will also be analyzed for normalcy based on its description of various characteristics about the data, such as the time of day that the data was entered into the system and other relevant information. The data analysis can then assess the behavior of the captured data and metadata for negative patterns or trends (such as spikes) in absolute value changes and conclude on suspected insider misuse detection.
- *Application Journaling*: The importance of application and IT infrastructure journaling is addressed in terms of its importance in the detection of ICF activity, the collection of computer forensics evidentiary data and metadata for event correlation purposes, root cause analysis, and strengthening the software engineering processes to "Bake" InfoSec journaling criteria and requirements within the software engineering and application development life cycle. In general, journaling is an important component of the eDiscovery process, which became law at the end of 2006.
- *Privacy*: The increasing emphasis on regulatory compliance through the Sarbanes–Oxley Act, section 404 (SOX 404), Gramm–Leach–Bliley Act (GLB), Health Insurance Portability and Accountability Act (HIPAA), and other legislation and guidance have placed growing attention on ensuring the confidentiality, integrity, and availability of NPPI and core transaction data. A discussion of the importance of performing a privacy impact assessment, and data flow diagramming the critical path of NPPI and core transaction data between critical systems internally and externally is also examined.
- *ICF Anomaly Detection*: The use of emerging technology through artificial intelligence, such as a novelty neural network that learns through neural associative memory (NAM), which can profile the behavior of data and metadata to flag anomalies in the behavior of data, which is instrumental in

determining day zero insider threats involving data and metadata manipulation, is explored.

- *Information Security Pattern Analysis*: The use of security patterns has been gaining some level of traction in recent years. A discussion on how the use of these security software design and procedural patterns may assist in the identification and resolution of enterprise-wide high-risk threats is presented. The pattern development and analysis will be partly based on management's clear problem definition, context identification, forces determined, and finally a viable solution that can be used to mitigate both insider and external security threats.

Unfortunately, the insider threat topic, even though it is significant in terms of its impact on an organization's operational, financial, and reputation risk areas, has not yet reached critical mass in terms the public's awareness of insider risks and mitigating controls. Although there may be varying degrees of research into the insider threat problem, the absence of a large volume of credible writing on this topic and the general absence of a significant number of solution providers who offer a means for identifying, measuring, monitoring, and controlling risks associated with the insider threat remains a concern.

My goal in writing this book was to increase the awareness and importance of understanding the associated risks and controls involving the insider threat. By writing this book, I am confident that the volume of credible research and security solutions will occur in the near future and will incite an increased level of research, funding, and solution development activities. This book, together with other research available in the public domain, may serve as a stimulus for creating both public- and private-sector partnerships between corporations and state, local, and federal governments and the academic community. The INFOSEC Research Council (IRC) in their 2005 Hard Problems lists ranks the insider threat problem as number two, which I am hoping will spur an increased level of academic and professional research into this area. In 2007, I have observed a significant increase in interest for the topic of the insider threat. This year, I have been involved two workshops on the insider threat problem. The workshop participants include both the public and private sectors, along with academia involvement.

Organization of the Book

The following chapter summaries provide abstracts for each of the chapters within this book to allow the reader to focus on key chapters; however, it is highly recommended that the chapters be read in sequence, because the structure of the book is designed such that each chapter serves as a building block to each of the subsequent chapters in the book.

Chapter 1: Insider Computer Fraud

This introductory chapter provides an overview of insider computer fraud (ICF) and discusses the interrelationships between various chapters and related content contained throughout the book. There is discussion regarding the importance of developing and maintaining a robust risk assessment methodology, which serves as the prerequisite bedrock needed for developing *Insider Computer Fraud: An In-Depth Framework for Detecting and Defending against Insider IT Attacks.* The chapter provides a high-level synopsis of key chapters within the book which relates to and has a connection with an integrated risk assessment process. The Defense in Depth concept is a vital component within this book in context to its relevance and importance to other related topics discussed throughout the book.

Chapter 2: Related Research in Insider Computer Fraud and Information Security Controls

This chapter provides a high-level survey of key research and writing conducted on the topic of the insider threat. One of the more significant contributions to bringing increased attention to the insider threat was achieved in the Insider Threat Study prepared by the U.S. Secret Service and Carnegie Mellon's Software Engineering Institute. A previously unpublished article by Thomas Kellerman also provides insight into the insider threat problem and discusses authentication, privileges, physical security issues, and various warning signs.

Chapter 3: The Insider Threat Strategic Planning Process

This chapter provides a comprehensive review on a number of different areas related to the insider threat. The topic of strategic planning is broken down into a number of different processes and practices, which are woven together within this extensive chapter. The content provides the foundational knowledge needed to understand and apply the concepts presented within all the subsequent chapters. The sections of this chapter include, but are not limited to the following key areas: defining security objectives; understanding the security governance and risk management governance processes; the tailored risk integrated process (TRIP); application criticality determination and security; qualitative and quantitative risk ratings; inherent, residual, and net residual risk ratings; threat modeling; the Risk Assessment Heatmap and InfoSec Scorecard; industry sound and best security practices; data privacy legislation and the privacy impact assessment; data flow diagramming and determining the critical path of data; control point determination and key risk indicators (KRI); the Defense in Depth Efficiency Calculation; the strategic planning process for the insider threat; the Web-based application penetration testing process; utilizing software security design and procedural patterns for problem identification and solutions; determining the strategic, legal, and operational risk assessment; and developing strategies for implementing software engineering InfoSec process and product improvements.

Chapter 4: Information Technology Architecture and Insider Computer Fraud Prevention

This chapter focuses on the importance of a Risk-Based Information Technology Architecture for Threat Mitigation. An introduction to the components of a typical information technology infrastructure is also presented. Specifically, a high-level introductory discussion of typical IT infrastructure components include firewalls, packet filters, application gateways, routers, hosts, servers, PC workstations, and intrusion detection systems. The Zachman Architectural Framework is discussed in the context of preventing and detecting insider computer fraud activities. Also provided is an introduction to the types of systems and architectural designs for information processing, which includes Service Oriented Architecture (SOA) and Centralized Processing and Distributive Systems Architecture including Client–Server Architecture. Particular emphasis is placed on SOA, given its significance to illustrating how the Forensic Foto Frame concept works for ICF detection.

Chapter 5: Protection of Web Sites from Insider Abuse and the IT Infrastructure

This chapter describes insider attacks and the importance of developing an ICF taxonomy identifying the types of attacks that may exist. Based on the completed taxonomy, management can determine which category of attack would be most relevant to a particular organization. Also discussed are intrusion detection systems, vulnerability assessments, and other network testing. A comprehensive overview identifies the strengths and weaknesses of network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A detailed discussion of the penetration testing process is provided. This chapter continues the discussion of firewalls and gateways introduced in Chapter 4, given their significant role in protecting Web sites from insider abuse.

Chapter 6: Web Services Security and Control Considerations for Reducing Transaction Risks

The goal of this chapter is to introduce the importance of Web services in conducting electronic commerce and its use internally within organizations as a means of facilitating interoperability between different applications, systems, and platforms. The chapter was included in this book because of the evolving and maturing nature of security risks and controls that could lead to heightened security risks for an enterprise. Specifically, a trusted insider who presumably has the greatest access to enterprise applications beyond the firewall in an organization, coupled with the greater potential to understand inside information about organizations and the IT infrastructure and business, could make Web services a prime target for potential insider abuse.

The chapter extends the discussion of the importance of architecture, particularly as it relates to SOA, as graphically illustrated in Chapter 4. The topic of Web services is featured in context of its growing importance and use within the financial services sector, major groups involved in establishing standards, current uses of Web services, and industry concerns relative to the surrounding security risks and controls. Security controls used within Web services and some of the problems associated with their use are also highlighted.

Chapter 7: Application Security and Methods for Reducing ICF

The discussion of application security in this chapter is significant. Overall, there is only a minimal amount of guidance in the marketplace for industry and government

sound and best practices over application security. The current state of application security and the prevention and detection of the insider threat are provided. Application security is presented in the context of the Insider Threat Study that was introduced in Chapter 2.

In this chapter, a few of the key concepts discussed in Chapter 3 are reinforced. The importance of software engineering processing in ensuring application security is considered throughout the software development life cycle. The Threat Assessment Matrix and companion Threat Assessment Rating Reference Table that were developed in Chapter 3 can now be used to complete the insider computer fraud threat assessment (ICFTA), which is used for evaluating the level of net residual risk. Included within this chapter is a table that can be used to determine what application journaling could be captured and used for computer forensics purposes in providing some type of trace-back mechanism to determine the root cause of the insider threat. Finally, developing application-specific acceptable and unacceptable use policies are discussed with regard to their importance in preventing ICF activities.

Chapter 8: Insider Computer Fraud Taxonomy and the Art of the Key Fraud Indicator (KFI) Selection Process

The content of this chapter is significant because it introduces the concept of the KFI, which is really the nucleus of insider computer fraud identification and detection. The nexus between software vulnerabilities, application security, taxonomy, and insider computer fraud is explored. The trusted insider may have access to the source code of various programs used within an organization, which may introduce a point of risk. Application security and ICF are also addressed. For the first time in this book and discussed in detail are the problems surrounding the lack of secure authentication and access control features within applications and overreliance on the potential for organizations to place an overreliance on client-side validation.

Understanding the source of security problems is a fundamental first step toward achieving a viable solution, whether it involves insider computer fraud or other problems. As such, one of the primary goals of this chapter is to reinforce the importance of understanding the concept of ontology, which in the world of computer science is a data model that represents a domain and is used to reason about objects in that domain and the relationships between them. There is an obvious interrelationship between the results from performing an ontology and a taxonomy. The taxonomy, which classifies various components into various categories, aids in determining a KFI.

Upon completion of the ontology, taxonomy (macro and micro), the concept of *Forensic Foto Frame*, is introduced, which is a term used to symbolize a point within an organization's architecture where data are being collected at a defined control

point (that is, access control, data origination or input, processing, and output). The Forensic Foto Frame takes a snapshot of the real-time data during transmission of the data and metadata within an application or system or in the transmission of data to another application. This chapter builds upon the topics discussed in previous chapters, most notably in Chapter 3, which discusses the topics of control point identification, KFI, and identifying and tracking the critical path of the transmission of data both internally within an enterprise and externally.

Chapter 9: Key Fraud Signature (KFS) Selection Process for Detecting ICF

One of the primary goals of this chapter is to inculcate the knowledge gained from previous chapters. A new concept of KFS builds upon the concepts discussed throughout the book, particularly as it relates to KFI, key fraud metrics (KFM), and finally the development of a KFS. The KFS is analogous to the intrusion detection system (IDS) signature that is commonly used within IDS for known network intrusion detection systems (NIDSs) and host-based intrusion detection system (HIDS) attacks. The concept of KFS is significant, because over time through system journaling of a KFI and perhaps other significant data elements, computer forensic analysis, the results of event correlation, and the results of the integrated risk assessment are important in understanding the threat vectors for known insider attacks.

The five phases of KFS selection are described, which include Phase I—Asset Risk Prioritization; Phase II—Data Criticality; Phase III—A Macro Taxonomy of ICF; Phase IV—A Micro Taxonomy of ICF; and Phase V—The Creation of Key Fraud Signature Association Rules (KFSAR). The concept of neural networks is introduced as a preview of what will be described in greater detail in Chapter 11. In the context of this chapter, there is a brief discussion on how the data collected and analyzed for developing a KFS can also be used for training and testing a neural network. The chapter continues into a discussion of KFSAR, which decomposes the topic down to its functional primitive state by describing the KFS format with associated examples.

In this chapter, a Data Definition Table is provided that presents realistic examples of how various data attributes (data and metadata) can be captured in a real-time manner using the concept of the *Forensic Foto Frame* given a particular business application (such as loans). A snapshot of one Forensic Foto Frame is used as an example to show the linkage between completing the ontology of information security concerns, the macro taxonomy of general categories of ICF, and the micro taxonomy of a business application (such as loans), showing each KFI that should be journaled, and finally how all this information can be used in developing a KFS.

Chapter 10: Application and System Journaling and the Software Engineering Process

This chapter discusses strategies for application and system journaling for the software engineering process using the SOA diagram, which was developed to illustrate how the Forensic Foto Frame can be used in capturing each KFI and other useful data, which might reflect the behavior of data within an application or transmission to other internal and external applications. Many of the data collection information that are being described in terms of the KFI and the development and analysis of each KFM and KFS may not necessarily be available within many internally developed applications or systems or commercially available third-party vendor software packages. Consequently, in order to collect the aforementioned information within applications and systems, the KFI will need to be identified and documented as described in detail in Chapters 8 and 9. Once the KFI selection process has been determined, the software development and engineering process needs to ensure that the journaling requirements are built into the applications and systems development. Consequently, if the journaling requirements for capturing KFIs are not identified within the business or user requirements and technical specifications phases of the software development life cycle (SDLC), the likelihood of that information being journaled is unlikely. Therefore, interrelationships exist between all phases of information security from the highest level of information security governance, the Defense in Depth Model and Efficiency Calculation, computer forensics, the KFI, KFM, and KFS, and finally to the software engineering process that emphasizes the importance of melding the journaling requirements of KFIs into an organization's SDLC processes.

Further described are various industry sound and best practices over journaling, which include but are not limited to the *National Industrial Security Program Operating Manual* (*NISPOM*). A cursory review is outlined for illustration purposes, the various components of an IT infrastructure that should include journaling and should be considered to better understand user activity. The illustrated IT infrastructure components included within the chapter to illustrate components that generate journaling activity, which could be captured and analyzed for ICF activity, involve Web servers, networks, the UNIX operating system, Windows NT, and mainframe computers using ACF2. Finally, a Journaling Risk/Controls Matrix for documenting KFI and KFM direct and indirect fraud scenarios is included. Direct risk scenarios are those situations where data and metadata elements can be directly attributed to fraud risks, versus indirect risks where monitoring the behavior of data is not indicative of potential ICF activity. Determining direct and indirect risk scenarios can only occur when the ICF framework has matured over time and when such distinctions can be made with some degree of accuracy.

Chapter 11: The Role of Neural Networks in the ICF Framework

This final chapter takes the next and last phase of the Defense in Depth Model, by moving beyond the misuse detection capabilities as provided and described in detail within the previous chapters. The last layer in the Defense in Depth Model involves considering the use of a neural network as potentially one layer in the Defense in Depth Model, to be used for anomaly detection. Until now, the discussion in the book has centered exclusively on identifying, measuring, monitoring, and controlling misuse detection involving trusted insiders, but it has not touched upon detecting day zero attacks or anomaly detection. The use of KFS is principally rule-based, and although the use of KFI is important, it has limited capability in detecting new ICF attack vectors perpetrated by the insider.

The use of neural networks for the purpose of fraud detection is relatively new and certainly not pervasive within the industry; however, its importance cannot be understated, and its benefits could someday be substantial, even though its use in the marketplace has not yet hit critical mass for fraud detection. The purpose of this chapter is to explore the possibilities and potential benefits for future use of neural network technology or some other type of artificial intelligence to explore methods and means of determining the holy grail of fraud detection, which is predicting the event in real-time or perhaps preventing the attack based on continuous monitoring of the behavior of data.

The basics of neural networks are discussed in terms of designing the neural network, learning the laws, supervised training, unsupervised training, neural associative memory, memory creation, the role of neurons, and the novelty neural network. The discussion of novelty detection is significant because abnormal or nonrandom behaviors are identified, and are the bedrock for ICF anomaly detection.