Chapter 14
Forensic-Ready Approaches to Insider Threat Mitigation and Human Behavior Analysis

Pridhi Arora
https://orcid.org/0009-0002-5790-1742
Delhi Technical Campus, Greater Noida, India

Padmesh Tripathi
https://orcid.org/0000-0001-9455-1652
Delhi Technical Campus, Greater Noida, India

Seema Verma
https://orcid.org/0000-0002-7893-671X
Delhi Technical Campus, Greater Noida, India

ABSTRACT

Insider threats are a cybersecurity risk that comes from people who already have authorized access to an organization's systems and information. This chapter provides a deep understanding of how to use cutting-edge technological tools along with the insights from human behavior that can help us to detect and stop insider threats. The chapter starts by defining insider threats and their various forms. It analyzes various internal breaches and explains why the traditional security methods are ineffective in identifying them. We further explain the need for modern frameworks that include pattern analysis of the activities, machine learning, identity and access controls, and detection of unusual activities. The chapter focuses on how the behavioral analysis can be used to identify the suspicious activity. After examining the

DOI: 10.4018/979-8-3373-4898-8.ch014

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

unusual activities, we discuss methods to prevent them by implementing the proper access control, training employees, securing the sensitive data, and adoption of a zero-trust security model. Legal and ethical concerns are also covered in this chapter.

1. INTRODUCTION

Insider threats are the risks posed by individuals within an organization who misuse their authorized access to harm the organization's information, systems, or people. Insider threat encompasses both intentional and unintentional actions by insiders that have negative effects. Insiders include current or former employees, contractors, vendors, business partners, or anyone granted trusted access to facilities or information systems. Insider incidents can take many forms such as espionage, sabotage, theft of information, fraud, workplace violence, or other policy violations (CISA, n.d.). In the cybersecurity context, common manifestations are unauthorized data exfiltration, means stealing of files or databases, misuse of authorized access e.g. an admin creating backdoor accounts, IT sabotage means destroying or altering systems or data, using systems for financial theft, and unauthorized disclosure of confidential information.

1.1 Types of Insider Threats

Organizations often categorize insider threats into a few broad groups:

1.1.1 Malicious Insiders

Malicious insiders are people who willfully use the access to do malicious activities. The bad insiders can pursue self-financial interest, vengeance over the perceived injustice, or competitive advantage with a new employer. They produce information, destroy systems or do any other damage to the organization. An IT administrator who plants a logic bomb to destroy systems after being demoted is a malicious insider, an example. The majority of famous insider cases (e.g., stealing trade secrets, information breaches) belong to this category. Research has established that by a high percentage of the insiders who engaged in IT sabotage or stole data were discontented employees who were either motivated by revenge or greed. Actually, personal financial gain is a significant factor that contributes to the occurrence of malicious insider breaches, almost 89% of this is as a result of financial gain (Smith, 2025).

28 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/forensic-ready-approaches-to-insider-threat-mitigation-and-human-behavior-analysis/401301

Related Content

A Biomedical Dataset Analysis on Predictive Modeling of Chronic Kidney Disease Using Machine Learning

G. Jeyalakshmi, F. Vincy Lloyd, K. Subbulakshmiand G. Vinudevi (2024). *Optimizing Intelligent Systems for Cross-Industry Application (pp. 175-196).*
www.irma-international.org/chapter/a-biomedical-dataset-analysis-on-predictive-modeling-of-chronic-kidney-disease-using-machine-learning/355749

Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186

Impact of Digital Technologies on Tourist Arrival in Selected Economies

Meenakshi Gupta, Bhoomika Sharmaand Ajay Kumar Singh (2025). *Harnessing AI, Blockchain, and Cloud Computing for Enhanced e-Government Services (pp. 441-474).*
www.irma-international.org/chapter/impact-of-digital-technologies-on-tourist-arrival-in-selected-economies/367027

The Future of Artificial Intelligence Quantum Neural Networks as the Next Frontier

S. Surya, D. Mahammad Rafi, Neeraj Chandnani, Prasanta Chatterjee Biswas, Mohit Tiwariand Melanie Elizabeth Lourens (2026). *Hybrid AI Architectures for Intelligent Systems (pp. 287-318).*
www.irma-international.org/chapter/the-future-of-artificial-intelligence-quantum-neural-networks-as-the-next-frontier/406935

Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186