Chapter 9
Insider Threats: Detecting and Controlling Malicious Insiders

Marwan Omar
Nawroz University, Iraq

ABSTRACT
Malicious insiders are posing unique security challenges to organizations due to their knowledge, capabilities, and authorized access to information systems. Data theft and IT sabotage are two of the most recurring themes among crimes committed by malicious insiders. This paper aims to investigate the scale and scope of malicious insider risks and explore the impact of such threats on business operations. Organizations need to implement a multi-layered defensive approaches to combat insider risks; safeguarding sensitive business information from malicious insiders require firstly, an effective security policy that communicates consequences of stealing or leaking confidential information in an unauthorized manner. Secondly, logging and monitoring employee activity is essential in detecting and controlling system vulnerabilities to malicious insiders. Thirdly, conducting periodic and consistent insider vulnerability assessments is critical to identifying any gaps in security controls and preventing insiders from exploiting them. And lastly, but certainly not least, taking extra caution with privileged users is important to proactively protecting information infrastructure from insider risks.

INTRODUCTION AND BACKGROUND
Recent security research studies have clearly shown that insider threats are posing a major security risk to organizational information assets. In fact; about 70% of threats to an organization’s network and network-based infrastructure originate from inside (Sugata, 2010). While many business organizations invest their most dear computational as well as monetary resources to fortify their network against outside malicious attacks; they forget or rather fail to pay close attention to the great threats posed by insiders who can advertently abuse or exceed their authorized access to organizational information systems and ultimately steal or modify sensitive business data for financial gains and other malicious goals. Fur-
Insider Threats

Insider threats have become a common and popular trend targeting private sector companies as well as government agencies for reasons that range from financial gains and IT sabotage to business advantage and industrial espionage (Barrios, 2013).

The insider threat challenge continues to receive increasing attention by both industry experts and scholars alike due to its devastating consequences which usually result in theft of sensitive business data and cause privacy, credibility, and reputation issues. A root cause of the insider threat issue stems from the fact that business organizations, and government agencies alike, do not seem to have adequate security defenses in place to detect and prevent insider attacks. This coupled with the fact that insiders have access to the “crown jewels” and valuable information assets that are inaccessible by outsiders; this certainly entices insiders to abuse their privileged access to those data and commit attacks. Organizations typically rely on security policies, auditing and log monitoring tools, and traditional access control mechanisms to combat insider threats; unfortunately those techniques cannot withstand emerging insider threats which are becoming highly sophisticated and usually remove their foot prints after committing insider attacks.

What Is Insider Threat and Who Are Malicious Insiders?

According to CERT, a malicious insider is a current or former employee, contractor, or business partner who has or had legitimate and authorized access to organization’s information systems and advertently misused or abused that privilege to compromise the confidentiality, integrity, and availability of organizational information assets (CERT, 2009). Employees with malicious intentions represent the insider threat to business organizations and government agencies and they usually commit deliberate acts for a variety of reasons such as job dissatisfaction, employment termination, workplace conflicts with co-workers and managers, or it could be due to influences by outsiders who have their own malicious objectives and want to exploit insiders’ authorized access to confidential business information which in turn could be for industrial espionage or IT sabotage or business advantage.

It’s important to note that insider threats may fall under two main categories: intentional insider threat and unintentional insider threat; as it’s equally important to acknowledge that both are a problem and both can have devastating consequences on organizational information resources. Nonetheless; both threats are exploited by the same entity which is organization’s personnel (current or former employees, contractors, business partners, etc.) whom are considered the source of greatest threat because they are usually entrusted with valuable and confidential business data which can entice them to exploit and exceed this privilege for their own personal advantage (Carroll, 2006). Unintentional insider threat is usually manifested in non-adherence or lack of security policy and non-conformance to security awareness and training programs. Intentional insider threat, on the other side, usually originates from malicious intentions and seeks to harm organization’s information assets. This kind of threat is certainly more dangerous and more consequential since it deliberately accesses information in an unauthorized manner; malicious insiders are usually technically capable and may use a combination of social engineering techniques along with sophisticated technical expertise to gain unauthorized access to organization’s valuable information resources.
Related Content

Speech Content Authentication Scheme based on High-Capacity Watermark Embedding
www.igi-global.com/article/speech-content-authentication-scheme-based-on-high-capacity-watermark-embedding/179277?camid=4v1a

A Novel Pixel Merging-Based Lossless Recovery Algorithm for Basic Matrix VSS
www.igi-global.com/article/a-novel-pixel-merging-based-lossless-recovery-algorithm-for-basic-matrix-vss/182460?camid=4v1a

Legal Issues: Security and Privacy with Mobile Devices
www.igi-global.com/chapter/legal-issues/131399?camid=4v1a

A Biologically Inspired Smart Camera for Use in Surveillance Applications
www.igi-global.com/article/biologically-inspired-smart-camera-use/46043?camid=4v1a