Chapter 1
An Exploration Regarding Issues in Insider Threat

Jaeung Lee
Louisiana Tech University, USA

Md Shamim Akbar
The State University of New York at Buffalo, USA

Anu Mary Eapen
Infosys Limited, USA

H. Raghav Rao
The University of Texas at San Antonio, USA

ABSTRACT

Insider threat occurs when a person with legitimate access misuses his privileges and compromises the operations and security of a company. When an outsider tries to gain access to company data, it can often be managed or detected by having standard controls in place. However, when an insider who has rightful access to the data is involved, it can often go undetected. There has been a steady rise in the number of cases of insiders' threat related incidents in recent years. An insider could do this either for his own benefit or might be acting as an espionage to profit another individual or organization. Insider threat is prevalent in various forms across various disciplines and is a serious cause of concern for the operation of an organization and maintenance of trust of the customers. In this chapter, we will look at various forms of insider threats, some well-known insider threat cases, factors causing this kind of behavior, some of the key indicators and what organizations can do to deter the theft of intellectual property.

DOI: 10.4018/978-1-5225-1941-6.ch001

INTRODUCTION

In an organization when a person is endowed with trust and s/he uses his/her position to violate the rules in the organization's security policy, that person is considered as an "insider threat". The insider usually has legitimate access to various company documents or network and misuses his/ her privileges to get into the system resulting in potential compromise of the operations and security of a company. An insider can be involved in such harmful behavior either for his/her own benefit or might be acting as a spy in order to profit another individual or organization (Federal Bureau of Investigation, 2014).

Duncan, Creese, and Goldsmith (2012) defined a malicious insider as a person who abuses or intentionally goes beyond their rightful access in a way that endangers the integrity, confidentiality, or availability of an organization's resources. Insiders are highly familiar with the company and its surroundings, which is unlikely for an outsider. A malicious insider can adversely damage an organization and its resources. Insiders can be classified into the three following categories: advanced, persistent and threat (Duncan, Creese, & Goldsmith, 2012).

An advanced insider has very high technical capability with good knowledge of computer systems and skilled. S/he is capable of developing custom tools to carry out the motives. A persistent insider is determined to accomplish his goals. They receive directives and work towards accomplishing a specific mission. These types of insiders continuously look for opportunities until their goal is met. A threat is most dangerous as the insider might be receiving monetary support from other individuals or organization to carry out the breaches of sensitive information. To understand the psychology of an insider and the framework for insider threat, it is crucial to understand the motivation, capability, and opportunity for an insider to successfully abuse a particular vulnerability or compromise a system (Sarkar, 2010).

In recent years, there has been an increase in the number of insider attacks in US companies such as government organizations, as well as the banking and finance industry (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). In addition, concerns about insider threat also have increased. For example, the Global Information Security Survey (GISS) conducted by Ernst and Young (2014)) showed that 1,040 organizations out of 1,825 (57%), perceive insiders as the most likely source of a security incident. Figure 1 (adapted from Silowash et al., 2012) shows that financial institutions were the most highly attacked sector, in terms of fraud, compared to other infrastructure sectors.