Securing Physical Protection System against Insider Threat

Jeong-ho Lee, Hyung-min Seo, Sung-woo Kwak
KINAC Exp-ro 573 Yusung-gu,Deajeon Korea
{friend25kr, rickyseo, swkwak}@kinac.re.kr

1. Introduction

A Physical Protection System is intended to provide security to an applied facility including a nuclear facility against inner and outer threats. It is, unfortunately, a well-known fact that it focuses on threats more from outside than from inside. Even though regulations and guidelines emphasize that a physical protection system should be designed to have arrangements or measurements prepared for insider threats. However, it is difficult to find well-prepared physical protection system for both inner and outer threats in the fields. In this paper, we present characteristics of insider threat based on incidents to critical infrastructures in United States. Based on that, also, we propose several methods to enhance the effectiveness of the system against insider threat.

2. Characteristics of Insider Threat

Adversaries to a facility may be categorized as follows [1]:

1. **Class I (clever outsiders):** They are often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment. They often try to take advantages of an existing weakness in the system, rather than try to create one.
2. **Class II (knowledgeable insider):** They have substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.
3. **Class III (funded organization):** They are able to assemble teams of specialist with related and complementary skills backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced tools. They may use Class II adversaries as part of the attack team.

The above criteria itself might be the proof on the fact that assistance from insider might greatly increase possibility to succeed malicious attempts. It will helpful to understand characteristics of insiders from various aspects in order to establish effective plan against it. Statistics presented in this paper is based on the analysis [4] of the forty-nine incidents that occurred across the critical infrastructures in United States between 1996 and 2002.

2.1 Insider's Employment Status

It will be helpful to identify potential insiders among employees by taking a close look at insider's employment status at the moment incidents took places. The majority of the insiders were former employees. When the incidents were occurred, fifty-nine percent of insiders were former employees or contractors to the affected organizations, and the rest were current employees or contractors. Among the former employees or contractors, insiders were left their positions due to being fired (52%), resigning (41%), and being laid off (7%).

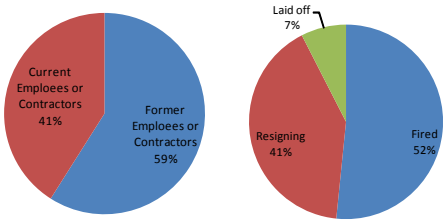

Figure1. Employment Status

Most of insiders were previously or currently employed full-time in their organization. Over seventy-five percent of insiders were full-time employees before or during the incidents. Eight percent of them worked part-time, and another eight percent were hired as contractors or consultants. Four percent worked as temporary employees, and two percent as subcontractors. In addition, most of insiders (86%) were in technical position. The rest were in professional position (10%) such as editors, managers or in service position (4%).

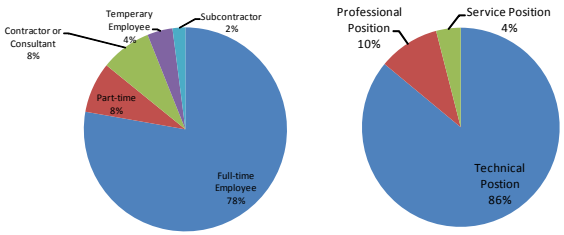

Figure2. Position Status

2.2 Insider's Motive

It also is worth to take a close look at reasons why the insiders took malicious actions. Before the incidents, there happened a specific event or series of events that triggered insiders' actions. These events included employ termination (43%), dispute with a current or former employer (19%), and employment related demotion or transfer (12%). The majority (over 80%) of insider's motives were a desire to seek revenge. Forty-one percent of the incidents were motivated by addressing a grievance or issue that the insiders had. Another twelve percent happened in order to drag attentions. Another twenty-four percent were took place by reason of addressing dissatisfaction with company policies and culture.

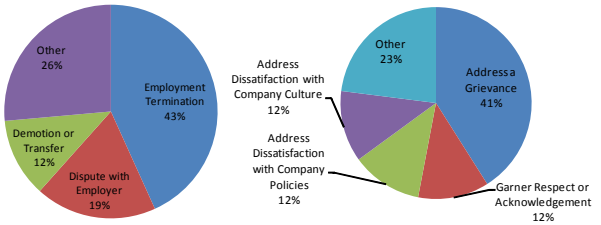

Figure3. Motive

2.3 Pre-attack Behavior and Planning

Before the incident took place, the insiders' actions could be anticipated by various ways. Sixty-two percent of the insiders established plans to harm the organizations. In thirty-seven percent of events, their planning activities could be noticed. Among those cases, they were noticeable online (67%) or offline (11%). In thirty-one percents of cases, there were people who had information about the insiders' plans, intentions, or their activities. In these cases, there were coworkers (64%), friends (21%), family members (14%), and someone involved with the incident (14%). Over half of the insiders (58%) were expressed their negative feelings, grievances, or interest in causing harm to others. In twenty percent of incidents, surprisingly, the insiders mentioned clearly their intention to harm the organization.

3. Prevention of Insider Threat

Analysis on the characteristics of the insiders indicates that it is possible to develop strategies to prevent such incidents. First of all, it is required to pay attention to employees who experience negative work-related events. Negative work-related events includes employment termination, demotion, or conflicts with coworkers and managements. In addition, organizations need to establish grievance procedures and additional forums where employees can express their concerns or dissatisfactions. This will help to reduce insiders' motive by addressing their grievance other than harming the organization. Furthermore, it is required to set up formal process for reporting and sharing information implying any malicious actions. With the formal process, organizations need to document those reports of suspicious behaviors and develop procedures to response to such reports.

With those administrative efforts, it is also important to take measures to enhance security of Physical Protection System against tamper or manipulation, highly by insiders, into account. [5] Functional measures that protect the system from those threats by using designated devices such as seals or tags should be considered as a part of the Physical Protection System (MPC&A). As well, standards need to be developed to detect tamper and manipulation with a reliable and practical program that assess vulnerability to those behaviors. Also, it is necessary to research and develop effective technology to remotely monitor the system protecting from tamper or manipulation.

4. Conclusions

In this paper, we provide valuable information on characteristics of the insiders based on analysis of the past incidents. This information will help organizations to identify their potential inner adversaries. Also, we present the reasons of insiders' attack and the triggers of their behaviors. It might give management an insight on how to prevent malicious behaviors by insiders. In addition, we propose several strategic approaches to deal with employees' concerns or complaints. This will enhance organizations' security culture resulting in mitigating insider's motive. Also, we advise the way to enhance their security systems.

REFERENCES

[1] DG Abraham, GM Dolan, GP Double, JV Stevens, "Transaction Security System", in IBM System Journal v30 no 2 (1991) pp 206-229.
[2] Anderson, R.H. Research and Development Initiatives Focused on Prevention, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. Santa Monica, CA: RAND(CF151); Department of Defense. DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team. Washington, DC, 2000.
[3] Shaw, E., Post, J., and Ruby, K. Final Report: Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations, 1999.
[4] Michelle Keeney, J.D. et al. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, US. Secret Service and CERT Coordination Center, 2005.
[5] Roger G. Johnston. Tamer Detection for Safeguards and Treaty Monitoring: Fancies, Realities, and Potentials, The Nonproliferation Review, 2001.