Countering Insider Threats in Personal Devices

Luk Boral, Maria Disla, Shivraj Patil, Jari Williams, and Joon S. Park, Member, IEEE

Abstract—The Information Age is a time when organizations are networked back and forth with multiple wires, different communication channels, many sophisticated information systems, and most importantly through the almighty Internet. This project focuses on responses that are most beneficial to organizations in regards to the internal threats. Mainly, it addresses the issues connected to the broad use of laptops, desktops, and other personal devices such as flash drives. During research there were thought different ways of mitigating the issue of insider threats. The result of this analysis is the Diamond Theory. It ties four methods of increasing the security of personal devices: software design, information retrieval, detection technology design and information policy design. All four corners of the diamond are represented by four different techniques that increase the security of personal devices and thus the defense against insider threats. These techniques are described as theoretical premises that shall be fulfilled in order to have the security raised to the maximum. Additionally, these methods are interdependent of each other and must work together to meet the overall goal of the theory.

I. INTRODUCTION

Due to the seriousness of the problem of internal incidents, there are various research works done on insider threats and ways of mitigating this risk within a company. This project is focusing on personal devices as a group of machines that are inseparably tied with every organization’s processing, but which expose a serious threat to be attacked internally.

II. METHODOLOGY

In order to collect and validate our research findings we conducted personal interviews with professionals who face the problems of internal securities (Lockheed Martin, DOD, Rapid Response Monitoring, KPMG, and Ernst & Young). We followed that up with retrieving both quantitative and qualitative data from articles, magazines, case studies and information security publications. Analyzing this problem required the collaborative effort and different ideas from the four members of our group. During our research, we concluded that we each thought of different ways of mitigating the issue of insider threats. Therefore, we divided the project into four different parts that represented our different views and interests on this topic. Individual research was conducted according our interests and a scheduled was set up to meet twice a month for updates and progress. Then as a group, we integrated our four different parts into one big solution.

III. DIAMOND THEORY

As a result, we came up with a Diamond Theory that ties four methods of increasing the security of personal devices: software design, information retrieval, detection technology design and information policy design.

All four corners of the diamond are represented by four different techniques that increase the security of personal devices and thus the defense against insider threats. These techniques are described as theoretical premises that shall be fulfilled in order to have the security raised to the maximum. Additionally, these methods are interdependent of each other and must work together to meet the overall goal of the diamond theory.

The Diamond Theory does not introduce new technology, software, or policies to fight against insider threats; instead it introduces the characteristics that we feel the four designs of the Diamond Theory should consists of in order to be effective. This theory was developed based on past research and type of incidents on this issue.

IV. CONCLUSIONS

There are multiple ways of increasing the security of personal devices against insider threats within the company. This project analyzed many of them and combined the most efficient ones into a net of interdependencies. Sorted and linked together they created the Diamond Theory. This theory consists of four independent parts: software design, information retrieval design, detection technology design, and policies design, that become interdependent when implemented together in the organization. Those, applied accordingly to the theory and in a cohesive manner provide the best security for personal devices.