IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB13047

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos© 2006, Idea Group Inc.

Chapter XIV

Training the Cyber Investigator

Christopher Malinowski, Long Island University, USA

Abstract

This chapter considers and presents training possibilities for computer forensic investigators. The author differentiates between civil service and industry needs for training, as well as cites differences in considerations for providing such training. While each organization has its own requirements, different paradigms and forums for training are offered allowing the reader to develop a training plan which may be unique to his/her organization. Those common subject matter areas which are felt critical to all organizations and needs are identified as well, providing a "core" knowledge and skill base around which to plan a training strategy.

Overview

Maintaining operations in an investigative environment is a time-consuming task. The process is exacerbated with the addition of technology, either in performing the investigations, or when technology is the subject of the investigation. When one considers the rate at which technology is constantly advancing, the burden is exponentially aggravated.

The issues concerned in this chapter fall into the realm of training, and affect staffing and budgeting. These issues, particularly in a civil service environment, are tightly bound. The manager of any unit, and the administration structure of the organization in which that unit is embodied, determines the likelihood at every level of such a cyber unit's success. This chapter applies therefore not solely to the manager of the unit itself, but also to those administrative managers involved in any decision-making process affecting the budgeting, training, and staffing of any cyber unit.

While this author's experience deals with the command structure of the NYPD (New York City Police Department), many of the issues will apply to both public agencies as well as many private institutions.

The reasons for training properly are obvious: efficient and adequate job performance depends on training levels commensurate with the tasks to be performed. A failure to provide adequate training will leave individuals and organizations vulnerable to court actions (either civil or criminal). The failure to process electronic evidence may result in a failure to exculpate an individual, or may result in failure to protect an organization in the event of a dispute. This impact will affect the individuals who are the subjects of the investigation as well the organizations for which they work.

Budgeting concerns are not part of this chapter other than to state that equipping and training on an ongoing basis are required. The justification for budgeting is rarely demonstrated in the public sector as a return on investment (ROI); instead, the justification is a negative one. The negative justification of risk avoidance and mitigation includes the cost of training individuals and properly maintaining the digital investigative environment.

The intended purpose of this chapter therefore, is to consider training paradigms and determine the applicability of any training models which meet job performance requirements.

Examination of typical tasks (as well as those not-so-typical tasks) can indicate the range of knowledge, skills, and abilities (KSA) required fulfilling cyber investigative roles. If possible, the categorization of these functional roles may allow a manager to better compartmentalize training requirements to a particular role (eventually assigned to a staff member), and thereby better plan training needs.

An alternate method of determining training possibilities is to survey training programs currently in place: the caveat here is that current offerings are designed to fit a "common" need, which may in fact not suit a unit's specific needs.

Still another technique of finding training topics is to examine course offerings in formal education institutes, both on the undergraduate as well as the graduate level. The distinction between the two should be the level and depth of expertise as well as the quality of research requirements in a course of study.