SECURITY
BUSINESS PRACTICES REFERENCE
6

Physical Security
Investigations
Emergency Planning
Safeguarding Proprietary Information
Personnel Security
Security Management

ASIS International

Industry	Employees	Yearly Revenue
Retail	62,000	$8.2 billion

Achieving Return on Investment from Crime Analysis

The Problem

In late 2001, a retail chain implemented a program to assess the risk at each of the company's stores so appropriate security measures and levels could be deployed. The company's security team decided that the most accurate way to assess risk was to use its internal security reports and actual crime data from each police department where company stores are located. Because the company's stores are often the anchor stores in strip centers, many crimes were reported from the stores that did not actually occur there. To resolve the issue of over-reported crime, the security team had to find a method that would differentiate between two types of crimes: those that occurred at the store and those that were simply reported from the store.

The Response

In 2002, the security team began using a crime analysis software application. The software contains a crime database for each of the company's stores and verifies the nature and occurrence location of each serious crime, using police offense reports. The database includes the time, date, and specific nature of each crime. The database also reflects where violent crimes occurred on the property and identifies the victim. That information enables the security team to determine (1) whether a store is high, medium, or low risk, and (2) who is being targeted (customers or the store itself). Armed with store-specific data and the analytical tools in the software, the security team deployed appropriate security measures to reduce the risk at each store specifically.

The Outcome

By the end of 2002, a sizable return on investment was realized. An annual savings or cost avoidance of $9.2 million, 41 percent of the security budget, was gained in the first year since implementation of the new program. This savings reflects a number of changes to the security program, but the main change was the deployment of security personnel during higher-risk times. Before the use of the program, security personnel were used haphazardly, with no regard for actual risk levels. By deploying personnel only during peak risk times, the company saved over $9 million. It expects to retain a similar savings level in the years to come.

There is another category of cost avoidance that cannot yet be measured. That category consists of reduced crime and avoidance of security litigation—two benefits that the security team believes will accrue in the future. Over time, the company will build up enough data pertaining to settlements and judgments to determine if that hypothesis is correct.

With the software application, the security team is now able to select and implement appropriate security measures and justify its budget by allocating security resources based on empirical crime data. The savings to the company's bottom line has made the security department a favorite with

upper management, which now allows the team the flexibility to experiment with other security technologies.

Karim H. Vellani, CPP Security Consultant	Threat Analysis Group, LLC P.O. Box 16640 Sugar Land, TX 77496	(281) 494-1515 kv@threatanalysis.com