



BEST PRACTICE No. 2: FORENSIC METHODOLOGY

Table of Contents

Position Statement..... 2

Evidence Review 2

Risk Assessment..... 3

Threat Assessment 3

Vulnerability Assessment / Security Survey..... 4

Analysis and Opinions..... 6

Bibliography..... 7

The International Association of Professional Security Consultants has issued this consensus-based and peer-reviewed Best Practice for the guidance of and voluntary use by businesses and individuals who deal or may deal with the issues addressed in the context of third-party premises security litigation.

POSITION STATEMENT

The International Association of Professional Security Consultants does hereby recognize that its members will be called upon to perform as “Forensic Consultants” and serve as Expert Witnesses in a court of law or other legal proceeding. The purpose of these guidelines is to meet the need for a standardized methodology used in the evaluation of premises security cases.

It is recognized that the task of the Forensic Consultant is one of education. Forensic Consultants will provide their opinion(s) to the client, to opposing counsel during deposition, in response to written interrogatories, in reports, and to the judge and jury at trial or any other lawfully convened hearing. This is done with the goal of making others aware of the security issues and contributing to a just and proper conclusion on the litigation.

The responsibility of the Forensic Consultant lies within our system of justice and the ethics of the security profession. The opinions so offered are made as an objective expert witness/consultant, without any financial or other interest in the outcome of the litigation.

Forensic Consultants will, at all times, be forthright, honest and precise in evolving the ultimate conclusion(s) and opinion(s). The opinion(s) will be the result of a review of all available documentation and discovery material presented by all parties to the litigation. Site inspections and analytical procedures generally followed by the “Forensic Consultant” are described in these guidelines.

The following methodology is to be used in a typical premises security case. It is reasonable to expect variations of the steps, with some steps deleted and others added as the facts and circumstances of the case being analyzed warrant. The Forensic Consultant is expected to exercise diligence in requesting and/or obtaining information that the Consultant reasonably believes is relevant to the facts and circumstances of the case.

EVIDENCE REVIEW – THE PROCESS

In the context of this Guideline, the Forensic Consultant will review and analyze various information, whether produced during the discovery process of the litigation or otherwise obtained through research, common knowledge, investigation, and/or other legal means which allows the Consultant to identify factors leading to an understanding of the crime risks present at the time of the criminal event.

Types of evidence generally available to the Forensic Consultant include, but are not limited, to the following:

1. Complaint/Petition
2. Police Report
3. Site and Immediate Vicinity Crime History
4. Interrogatories and Responses
5. Requests for Production of Documents and Responses
6. Requests for Admissions and Responses
7. Affidavits, Witness Statements and Interviews
8. Depositions
9. Expert Witness Reports
10. Medical Records Relating to the Facts of the Case
11. Photographs, Video and Audio Recordings, etc.
12. Other Related Evidence

RISK ASSESSMENT

A risk assessment is the general process of identifying and prioritizing risks. It is a qualitative, quantitative, or hybrid assessment that seeks to determine the likelihood that criminals will successfully exploit a vulnerability or compromise a security countermeasure.

There are two main components to a risk assessment: a threat assessment and a vulnerability assessment. The threat assessment is an evaluation of the various sources for crime threats. The vulnerability assessment, which includes a security survey, is an analysis of the weaknesses in a security program.

The security survey, along with documented evidence, is the means by which security measures utilized and/or available at the facility at the time of the incident leading to the incident that is the subject of the litigation are identified and analyzed.

A risk assessment provides the foundation for effectively implementing countermeasures.

THREAT ASSESSMENT

A threat assessment is an evaluation of events that can adversely affect operations and/or specific assets. Historical information is a primary source for threat assessments, including past criminal and terrorist events. A comprehensive threat assessment considers actual, inherent, and potential threats.

1. Actual Threats

- a. The crime history against an asset or at a facility where the asset is located. Actual threats are a quantitative element of a threat assessment.
- b. Relevant crimes on the premises (three to five years prior to the date of the incident)
- c. Relevant crimes in the immediate vicinity of the facility (three to five years prior to the date of the incident)

2. Inherent Threats

Threats that exist by virtue of the inherent nature or characteristics of the facility or nature of the operation. For example, certain types of facilities or assets may be a crime magnet or prone to loss, damage or destruction (e.g., assaults among patrons in nightclubs, infant abductions from hospital nurseries, etc.).

3. Potential Threats

Threats which exist by virtue of vulnerabilities around the asset or weaknesses in the security program which produce opportunities for crime to occur.

VULNERABILITY ASSESSMENT / SECURITY SURVEY

The vulnerability assessment is an analysis of security weaknesses and opportunities for criminal activity. A security survey is the fundamental tool for collecting information used in the vulnerability assessment.

A security survey is a physical survey of the scene of the incident and areas/functions that are applicable to the incident to achieve a meaningful understanding of information that has potential application to the matter in litigation.

1. Incident Review

- a. Police incident and investigation report
- b. Proprietary incident report
- c. Medical records (emergency room and/or autopsy as it relates to information about the occurrence of the incident)

- d. Other sources of information about how the incident occurred
2. Site Inspection - Inspect site where the incident occurred and the surrounding relevant area. (Note that not all cases will require site inspections, nor is it always possible to conduct site views - e.g., if the site has been altered substantially or no longer exists). Further, the facts of some cases and potential liability issues are not related to the site/property layout, design, or other physical attributes. As such, a site inspection may be unnecessary.
- a. Determine layout of the premises
 - b. Evaluate relevant factors (lighting, lines of sight, places of concealment, remoteness, accessibility, security measures, conditions, etc.)
 - c. If and when appropriate and as allowed by local rules of evidence, interview those with knowledge of the incident and/or the premises/surrounding area (this is often covered in depositions, police interviews and private investigators' investigations)
 - d. Review relevant documentation (lease, contract, diagram, map, etc.)
 - e. Assess the characteristics of the surrounding area
3. Security Personnel
- a. Review security officer(s) actions, staffing levels, post orders, duty hours, equipment provided, tours, evaluations, training, hiring procedures and supervision
 - b. Review law enforcement presence and actions (e.g., on-duty, police details, etc.)
 - c. Review roles and actions of non-security related persons who may have participated in the security program and/or incident
 - d. Assess the qualifications and performance of owner/management personnel overseeing the security program
4. Security Program
- a. Review security related policies and procedures
 - b. Review risk assessments performed prior to the date of the incident

- c. Review daily activity reports, job descriptions, incident reports and internal correspondence
 - d. Review security services contract
 - e. Review security manuals
 - f. Review training manuals and materials
 - g. Interview parties and/or review depositions regarding employees' understanding of their duties, and all customs and undocumented practices
 - h. Review changes to security prior to the incident
 - i. Evaluate the qualifications and experience of security management and supervisory personnel
5. Security Equipment
- a. Review building design and site plans
 - b. Inspect all security devices related to the incident
 - c. Inspect all structural security features
 - d. Determine the position, function and maintenance status of the relevant security equipment and features
 - e. Determine levels of illumination, if relevant

ANALYSIS AND OPINIONS

The security expert will determine the level of adequacy of security at the location of the incident on the date and at the time the incident occurred. This will be based on the information obtained in the previous steps, and the application of a qualitative analysis based on experience, education and training.

Based upon the analysis, the expert will reach conclusions on the issues of foreseeability, preventability and causation (i.e., terms as used in the security profession). At this point the expert has formed opinions and is prepared to provide a written report, be deposed and/or testify at trial. Those opinions will state the detailed bases for the findings, including evidence, standards, best practices and guidelines, where applicable.

BIBLIOGRAPHY / REFERENCES

The process of evaluating the risk of crime at a specific location or geographical area is widely recognized and has been adopted nationwide by private industry, public law enforcement, municipalities, and other governmental agencies. The following published sources reference the process used to perform a crime risk analysis. *This is not all-inclusive, but a representative sampling of available references.*

This bibliography is not to be construed in any way as an endorsement by the International Association of Professional Security Consultants of the publications or the respective authors.

ASIS International (2003). *General Security Risk Assessment Guideline*. Alexandria, VA.

Bates, Norman D. (1997). "Forseeability of Crime and Adequacy of Security", Accident Prevention Manual for Business & Industry, Security Management, National Safety Council.

Broder, James F. (2006). Risk Analysis and the Security Survey, Boston, MA: Butterworth-Heinemann.

Crowe, Timothy D. (2000). Crime Prevention Through Environmental Design, National Crime Prevention Institute, Boston, MA: Butterworth-Heinemann.

Department of the Navy, Naval Facilities Engineering Command, (1983). Physical Security Design Manual 13.1, Washington, DC: Government Printing Office.

Eck, John E. and Weisburd, David (1995). Crime and Place. Monsey, NY: Criminal Justice Press (Police Executive Research Forum).

Gottlieb, Stephen, Sheldon Arenberg, and Raj Singh (1998). Crime Analysis: From First Report to Final Arrest. Montclair, CA: Alpha Publishing.

International Association of Crime Analysts (2004). Exploring Crime Analysis. Overland Park, KS: International Association of Crime Analysts.

Miethe, Terance D. and Richard McCorkle (1998). Crime Profiles: The Anatomy of Dangerous Persons, Places, and Situations. Los Angeles: Roxbury Publishing Company.

National Crime Prevention Institute (2001). Understanding Crime Prevention, Boston, MA: Butterworth-Heinemann.

U.S. Army Corps of Engineers (1990). Security Engineering Manual, Missouri River Division/Omaha District.

U.S. Department of Justice, Federal Bureau of Investigation, “UCR: Uniform Crime Reporting Handbook” Revised 2004, U.S. Government Printing Office, Washington, D.C.

U.S. Department of Justice (1995). Vulnerability Assessment of Federal Facilities, Washington, DC: Government Printing Office

Sennewald, Charles A. (2003). Effective Security Management. 4th Edition. Woburn: Butterworth-Heinemann.

Vellani, Karim H. (2006). Strategic Security Management: A Risk Assessment Guide for Decision Makers. Woburn: Butterworth-Heinemann.

FORENSIC SECURITY COMMITTEE MEMBERS

Norman D. Bates, Esq., Committee Chairman; President, Liability Consultants, Inc.

John Case, CPP, John Case & Associates

James H. Clark, CPP, Managing Partner, Clark Security Group, LLC

Lance Foster, CPP, CSC, Security Associates, Inc.

William A. Hawthorne, CPP, CSC, William A. Hawthorne Associates, Inc.

Steve Kaufer, CPP, CSC, Inter/Action Associates, Inc.

Robert Shellow, Ph.D, CSC, Fellow, APA, President, IMAR Corporation

Ira S. Somerson, BCFE, CPP, CSC, Loss Management Consultants, Inc.

Karim Vellani, CPP, CSC, Threat Analysis Group, LLC

Ralph W. Witherspoon, CPP, CSC, Witherspoon Security Consulting

CASES CITING THE METHODOLOGY

Childress v. Kentucky Oaks Mall, 2007 WL 2772299 (W.D. KY) 2007

DOCUMENT REVISION HISTORY

Initial Release: June 2000 approved by the IAPSC membership in attendance at the annual meeting.

Revised: May 2, 2005 with approval by the IAPSC membership in attendance at the annual meeting.

Revised: November 2008 with approval of the Board of Directors