Controlling Premise Liability by Real-World Risk Assessments/Security Practices

By Mark Pickett, CPP, Managing Director for Pinkerton's Consulting & Investigations

In today's business world of growing pressures and expansion, every enterprise faces the challenges of growth, profitability and survival. Businesses fail every year, some because of poor management and others due to economic or quality issues. Today, more and more businesses are failing due to financial devastation caused by liability losses. These losses can be caused by any of the following:

- Theft, either internal or external
- Interruption of business operations caused by natural or man-made disasters, or personnel liability such as incidents of workplace violence

Providing adequate levels of security is also important in mitigating negligent security court cases, which are becoming more prevalent. A common theme for these liability lawsuits is loss resulting from lack of security or safety measures – based on premise liability rulings.

Plaintiffs argue that premise owners have a duty to protect against potential criminal acts, and recent court cases are substantiating their claims. This equates to an increase in liability for the enterprise, and in a sense, a threat to the long-term well being of the company.

The first step in planning for the prevention or mitigation of these types of losses is to understand what you face in the form of risk. In other words, how do you determine what to protect and what methods you use to prevent loss if you don't fully understand where the risk comes from?

To help prevent these and other losses, the enterprise must take a proactive approach in protecting assets and reducing risks. Security and risk managers must develop proactive security measures that meet the many threats facing their businesses, and an enterprise's senior management must adopt the measures and practices. Very few will debate the concept that security management's first step is to conduct a security risk assessment.

Risk

In simple terms, risk is the value of threat plus vulnerability. A quantitative risk analysis is a tool for measuring the compliance of an organization with applicable security requirements, and is a standardized methodology that can be used to analyze a system or function and identify vulnerabilities that potentially result in losses. This standardized methodology is based on the interrelationships of four key factors: Assets, Threat, Vulnerability and Safeguards.

Using a Software Tool

Measuring risk requires a standardized methodology or approach. The best method or application of standardizing an approach to a risk analysis is the use of a software tool. The purpose of the risk analysis is to identify the vulnerability of the assets of the enterprise to a variety of threats, establishing overall risk, and to recom-

Mark Pickett, CPP

Mark Pickett, CPP, is a Managing Director for Pinkerton Consulting and Investigations (C&I). Pickett has over 20 years of experience in the security industry including risk evaluation, security program development, system design and evaluation, information protection and business continuity planning. He studied economics at Brigham Young University, is a Certified Protection Professional and a member of ASIS. Pickett is based out of C&I's Napa, California, office.

mend safeguards, or revisions to current practices, that could reduce or eliminate the vulnerability of these threats. A software tool, and there are several on the market, provides some definite advantages that enhance the value of assessment to an enterprise. Let's look at some of these advantages:

Bias – the use of a good software tool will help eliminate bias by establishing a uniform method of evaluation.

Standardized approach – there are variances between industries, and surveyors have to take into consideration the variations of vulnerability found in the industries they are assessing. A software tool provides standardized methodology in the determination of threats, risk factors, vulnerability exposures and potential losses.

Benchmarking – because a software tool provides so much analytical information, the elements that can be compared or benchmarked from site to site are significantly increased.

Measurements – quantifiable findings are possible with software tools and can be shown in a variety of graph formats.

Risk assessments consist of four major elements

- *Assets*. Defined as the resources you are trying to protect, the identification and valuation of the assets of the enterprise should be a major focus of the risk assessment.

- *Threats*. Threats must be identified and frequency rates assessed. Measuring the seriousness of the threat and the vulnerability to the threat is the real task of the assessment.

- *Vulnerabilities*. Vulnerability has been defined as weaknesses in the systems that create opportunities for threats to occur. Safeguards are implemented to offset or mitigate vulnerabilities.

- *Safeguards*. These are the recommended systems, policies and procedures that eliminate, reduce or mitigate vulnerability and the impact of a threat occurrence.

A successful assessment incorporates the evaluation of all four of these elements. A software tool is currently the best method of identifying threats that could affect assets, discover vulnerabilities that enable threats to occur and identify safeguards that can eliminate potential losses.

The Assessment Scope and Process

Assessment scope, or scope of work, will vary with management's needs and objectives. The following scope of work is an example that may be helpful in initiating a security assessment using a software tool.

The objective of a security assessment is to provide management with a written report identifying the assessment findings, recommendations and possible threat-mitigating factors. The risk assessment should enhance the focus of a new or existing security program by providing a clear definition of the threat and vulnerability of the enterprise, and present cost-efficient measures to reduce risks to personnel and assets. Additionally, the assessment should provide budget estimates for recommended actions.

The deliverables of an assessment should provide:

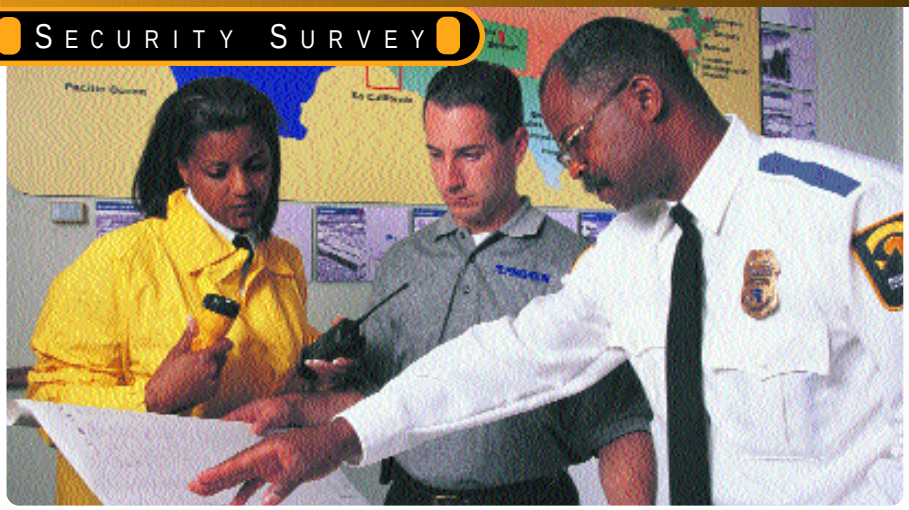
- The ability to measure policy and operational standards from an automated compliance evaluation process that can be conducted on a regular basis.

- Quantifiable return-on-investment (ROI) evaluations.

- A comparative analysis of the current threat and vulnerability base at each assessment site.

- Illustrations of how specific safeguards affect the vulnerability of specific assets of the corporation.

- A quick method of evaluating the financial effects of postpon-



ing the implementation of given safeguards.

Physical Security – The assessment should review physical security aspects of each building and location contained in the proposed scope and each of the elements listed below should be reviewed:

- *Physical building* – examine the physical elements of security for each facility including doors, locks, windows and other exterior openings. Assess parking lots and any current method of vehicle/truck parking control, including shipping, receiving and distribution methods. Examine the elements of the buildings' interior areas to assess the level of security at restricted or sensitive areas, financial offices, executive offices, locations of high-value articles, information control areas, tool cribs, etc.

- *Perimeter security* – examine the pedestrian and vehicular perimeter control of each facility including access to the overall property and building.

- *Fencing, landscaping, clear zones* – review and assess the value and/or need of any applicable fencing. Assess landscaping, including shrubbery near walk paths, fence lines, open areas and the appropriate use of clear zones as applicable.

- *Property lighting* – review and measure the current lighting at critical locations throughout the facility.

Security-related Operational Procedures – Security policies and procedures should be evaluated with recommendations documented as necessary. Specific site survey findings and recommendations for operational procedures should be offered within the framework of existing security policies. The security procedure evaluation process should include the following:

- Employee, visitor and contractor identification/badging
- Personnel security practices
- Facility access control
- Utilization of security officers
- Existing workplace violence program
- Crisis management planning
- Incident reporting
- Alarm reporting and response
- Security awareness programs

Security Electronic Systems – Evaluate and make recommendations regarding existing electronic security systems and/or the need for security systems. The assessor should evaluate whether any cost reductions or increased safety, convenience or asset protection are likely to result from the implementation or expansion of security electronics and provide justification for the expenditure. Systems that should be included in this evaluation process are:

- Closed-circuit television systems (CCTV)
- Electronic access control systems
- Alarm and intrusion detection systems
- Intercom/communications
- Vehicle gate control and truck traffic control
- Security monitoring and response

Security Officers – An assessment should be made of the use, effectiveness and operation of the security officer force. It should be measured against the objectives of the security program and the effectiveness of the officers in relating to each of the other assessment elements described above. Specific elements to be reviewed include:

- Post orders
- Training
- Cost vs. benefit
- Culture fit/professionalism
- Effectiveness in reducing loss
- Compliance to the providers agreement

Site Interviews – The surveyor should interview key personnel at the site to help determine the level of

security awareness and operational compliance. Additionally, he or she should examine employee and visitor traffic flow patterns, access needs, any unique site or facility culture, while also examining vulnerable or critical areas as they relate to operations at the facility. Results from the interview should determine concerns from perceived threats. Information should also be gained regarding existing practices, ideas for improved security, and confirm or gather additional information on any history of past incident issues.

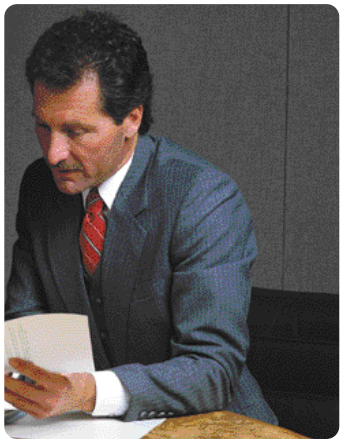
The most important part of performing an assessment, or having one done for you, is to ensure that both parties understand expectations.

Using Risk Assessment Software – Case Study

Cox Enterprises is the holding company for four major business units including Cox Communication, the cable company; Cox Broadcasting, incorporating television and radio stations across the country; Cox Media, which owns newspapers through the United States; and Manheim Auto Auctions.

In February 1999, Bob Brand of Cox Enterprises, Inc., contracted with Pinkerton Consulting and Investigations to conduct risk assessments utilizing the software tool RiskWatch. The objective of the assessments was to identify overall risk associated with the enterprise and to make very specific recommendations to provide field managers with the tools necessary to manage their security concerns. With such a diverse range of companies and cultures between each of four Cox Enterprise divisions, providing a standardized method of measuring risk was essential.

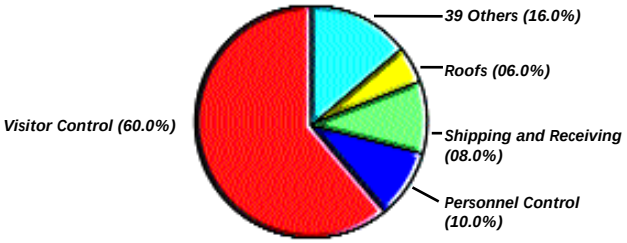
Using Software to Quantify the Assessment. Modifying the user-friendly software to assess site-specific threats and vulnerabilities enabled Pinkerton to produce a report that delivered very specific recommendations and justifications for proposed actions to be taken.



Automating and Aggregating the Security Questionnaire. The ability to quickly survey a wide range of employees ensures that every possible vulnerability will be discovered and identified. To simplify the process, employees answer questions that were tailored for and specific to their jobs.

A RiskWatch vulnerability assessment graph can illustrate the major areas of weakness in a sample security profile:

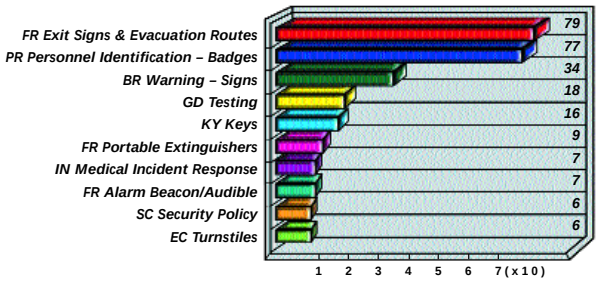
RiskWatch Vulnerability Assessment Graph



Collecting Threat Information. Threat data can be obtained from a variety of sources, including use of normalized crime statistics through a country-specific threat data provider, and the use of internal company incident reports, which can be compiled over time to provide a good look at the security history of an organization. The software can aggregate and categorize threat data that makes each site unique when recommending safeguards to mitigate threat.

Identification of Appropriate Controls. As well as providing a snapshot of the organization's current security procedures, it is important that the assessment result in actual recommendations for improvement. Software automates the process of quickly calculating ROI (return on investment) data and actually recommending appropriate controls based on how much they would cost the organization, balanced against how much they could save against threat occurrence. An example of an ROI graph is shown below:

(Return On Investment) ROI Graph



Calculated in order of the 10 highest ROIs.

With justifiable ROI data in hand, field managers for the various Cox divisions were able to develop accurate security budget plans for the next several years. Not only will the budget requests be justified, based on the findings of the assessment, but senior management has a level of confidence in knowing that the measurements for the findings have standard uniformity across each division.