Enterprise Risk Assessments

Holistic approach provides companywide perspective

By Jerry D. Loghry and Chad B. Veach

Abstract: *This article discusses the components of a risk assessment within an enterprise risk management setting. It outlines the steps necessary to perform a risk assessment and tools necessary to analyze the results. The authors also present a case study illustrating this process in practice in a manufacturing setting.*

ALL COMPANIES OR ORGANIZATIONS face a certain level of risk each day, whether the result of natural events, accidents, intentional acts or business decisions. These risks may subject the entity to loss or gain, which is why managing them is important. Managing risk involves identifying, assessing, controlling, eliminating and minimizing the impact of unforeseen events on resources or profits. Regardless of the nature of the risks, facility owners and organizational leaders have a responsibility to reduce or manage these risks to the greatest extent possible.

Enterprise risk management is a coordinated approach that a business can and should take to assess and respond to all risks (CAS, 2003). Traditional business models and management techniques use what could be called a silo approach, keeping the management of risk separate and parallel within individual business functions, departments or subject-matter expertise. This style of management has limited effectiveness caused by the lack of consideration of how risks are affected by the interaction of each area, and territorial conflicts between business units and subject-matter experts. Use of this method has more to do with the organizational structure of the business than the risks faced by the organization. The silo approach can be a result of a missing hierarchy, leading to one person or entity responsible for risk management.

True enterprise risk management requires a holistic approach that evaluates risk from a companywide perspective. The process should be overseen by one person or entity such as a chief risk officer (CRO) or corporate risk management department. Smaller businesses may not have the resources for a dedicated risk manager or CRO, but the risks are typically not as high either. Regardless of size, a company must have someone who has the responsibility and duties associated with managing risk on a macro scale.

Risk Assessments

What risks does an organization face? No one can answer that question without a thorough and complete risk assessment. A risk assessment is a qualitative measure of the potential for losses resulting from the occurrence of uncertain events in a specific period of time. In layman's terms, it is evaluating possible events that may occur, their causes and the impact they may have on a company (Lam, 2003).

Who can perform risk assessments? Any safety, health or security professional should be able to conduct a reasonable risk assessment with a little research and practice. The basis of a risk assessment is applying logical thought to the exposures and hazards that these trained professionals already work with on a daily basis.

The outcome of a risk assessment will be a report that outlines exposures, vulnerabilities, threats, hazards, probability of loss, potential impact to assets and mitigation recommendations. Looking at all aspects of an organization's operations—from information processing to asset distribution to asset criticality—with assurance that all threats have been documented and accounted for is a formidable task. Following are components of a risk assessment: exposure determination; vulnerability assessment; threat assessment; hazard assessment; risk analysis; mitigation/countermeasure determination; performance testing; and strategy review and modification (EMC, 2006).

Jerry D. Loghry, M.S., CSP, CPP, *is the loss prevention information manager at EMC Insurance Cos. He has more than 20 years' experience in the loss control field. He holds an M.S. and a B.S. from Iowa State University, and has served on several national and international committees. Currently, Loghry is serving on NFPA 730 and 731 Premises Security Technical Committee. Loghry is a professional member of ASSE's Hawkeye Chapter and a member of the Society's Risk Management/ Insurance Practice Specialty. He is also a member of ASIS International where he has served in several capacities both locally and internationally.*

Chad B. Veach, CSP, ARM, *is a senior engineer with EMC Insurance Cos. and has provided policyholder assistance with fire protection, security and workplace safety for 11 years. Veach earned a B.S. in Civil Engineering from Iowa State University. He is a member of ASSE's Hawkeye Chapter, as well as a professional member of the Society of Fire Protection Engineers and a member of ASIS International. Veach is also currently chair of the Occupational Safety & Health Advisory Council for the State of Iowa.*

To determine risk, each threat's probability and potential severity to the organization must be evaluated.

Exposure Determination

It is impossible to conduct a risk assessment without understanding what assets are exposed to the threats. Without exception, each organization will have the following exposures to loss: people; property; liability; income; information (proprietary); reputation (EMC, 2006).

Vulnerability Assessment

The first step is to recognize that every organization or business has vulnerabilities that can affect its operations. A vulnerability assessment is a self-examination designed to identify where operations are vulnerable. Left unattended, even small problems can grow into crises. Typical high-level vulnerabilities many organizations have in common include loss of:

- access to premises;
- building;
- equipment;
- personnel;
- utilities;
- communication;
- major vendor(s);
- information;
- market share (EMC, 2006).

Threat Assessment

Threats are events that may cause harm or loss to an organization's assets or profits. To determine risk, each threat's probability and potential severity to the organization must be evaluated. Following are examples of threats to which an organization may be exposed.

Accidental/Intentional Acts

- arson;
- embezzlement;
- explosion;
- fire;
- power outage;
- riot;
- sabotage;
- terrorism;
- theft;
- forgery;
- fraud;
- vandalism;
- labor strikes;
- trespass;
- espionage;
- chemical release;
- product contamination;
- electrical overload;
- human error.

Environmental/Natural Acts

- earthquake;
- flood;
- fire;
- wind;
- lightning;
- hurricane (ASIS, 2003).

Hazard Assessment

Each identified threat has one or more hazards that allow the threat to affect the organization's assets. The hazards determine how each threat affects the risk. If these hazards are removed, manipulated or modified, an organization can eliminate or mitigate the impact of a threat.

A common example used to demonstrate the hazard assessment principle is the threat of fire in a facility. One hazard that would allow a fire to start might be the proximity of open flames to combustible materials. If the hazard of the open flames was eliminated or reduced, the threat of fire would be reduced and, thus, the risk to the organization reduced.

Consideration must be given to how the probability of loss and potential severity of loss are affected by the hazards and threats identified. For the threat of fire, the risk will depend greatly on building construction type, fire protection systems, safety and security policies in place and other factors.

Probability of Loss

Elementary statistics show that probability is measured as the number of times in which a particular event can result from a certain activity, divided by the number of all outcomes occurring from that activity. This statement illustrates the most direct way to calculate probability mathematically; unfortunately, it seldom works in practical risk assessments. Most of the time there is insufficient data, often in unusable formats, to permit accurate forecasting. Most organizations only keep information in connection with actual insured losses. Typically, losses that are not covered by insurance, near-hit incidents and other data are not maintained in enough detail or not kept for a sufficient length of time to be useful.

Instead, employ the following basic concept: The more ways an event can occur in given circumstances, the greater the probability that it will occur. Accurate historical loss experience can also be an excellent source of information concerning probability. The frequency of previous event occurrences can indicate a strong probability of future recurrences.

Since it is usually impossible to mathematically calculate the probability of threats striking an organization, a probability rating will be assigned to each threat based on all available loss and/or historical data. The primary purpose of these ratings is to allow prioritizing the application of countermeasures and distribution of resources. Often five categories of probability are determined. With the amount of information available about most organizations and their threats, in addition to the experience of a risk management professional, it should be possible to assign one of the following five ratings (EMC, 1993):

- **Highly likely:** Given no changes, the event will occur during a chosen period.
- **Likely:** The likelihood of occurrence is much greater than nonoccurrence.
- **Neutral:** There is just as much likelihood that the threat will occur as it will not occur.
- **Unlikely:** The likelihood of nonoccurrence is much greater than occurrence.
- **Highly unlikely:** The event is very unlikely to occur. This does not imply impossibility, merely high improbability.

It must be realized that one or more hazards associated with each threat will influence the probability that the threat event will occur. For example, a facility located near a flood zone will be exposed to a higher probability of occurrence of flood than a facility on higher land. It also must be understood that an exposure interval is very important to establish and apply equally in the estimation of probability in order to compare threats on an equal time basis.

Impact of Loss

Once the threats and their probabilities are determined, assess the potential impact from a successful attack. The potential impact of loss is the degree to which the operational mission of the organization is impaired, combined with the duration of the impairment. Only personnel closely associated with an organization can determine the impact a threat may have on that organization. This critical element of a risk assessment should not be determined by outside consultants or vendors. The results of a successful threat occurrence are commonly assigned to one of the following four categories (EMC, 1993):

- **Devastating:** A loss that could result in total shutdown of operations, facility damage beyond habitable usage or loss of most or all key employees.
- **Severe:** No operations for a period of 2 weeks and some operations off-line for an extended period of time; 50% employee access and loss of some vital or sensitive information.
- **Noticeable:** Facility temporarily closed for 1 day or less, limited number of assets damaged, majority of operations unaffected, mission of the organization continues.
- **Minor:** Organization experiences no significant impact on operations, downtime less than 4 hours.

The nature, size and operations of the organization will determine the severity of the impact. Some organizations can handle greater periods of downtime or losses of assets than others. Each assessment must take into account these differences. The terms used above are not intended as absolutes.

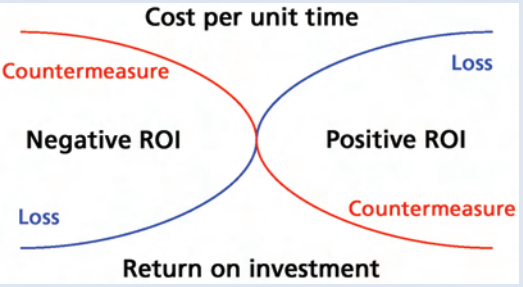
Risk Analysis

The interaction of the potential impact of loss and the probability of threat occurrence rating can be used to evaluate the potential risk to an organization by each of its threats. By using a simple matrix and its associated symbols each threat can receive priority ranking for consideration of mitigation efforts and countermeasures.

Mitigation/Countermeasure Development

Based on the findings of the risk analysis, identify mitigation efforts, countermeasures or existing program upgrades that will eliminate or reduce the hazards contributing to the effectiveness of the threats. Countermeasures and mitigation efforts can take a variety of forms, including implementation of a comprehensive safety and security awareness program, to installation of a workplace ergonomics program, to rekeying a building. Typically, more than one countermeasure can be applied to a given threat. The individual conducting the risk assessment will need to understand the organization's culture and operations to recommend appropriate, effective countermeasures.

Figure 1
Cost-Benefit Relationship



The most important component of any mitigation effort is senior management support and participation in the process. Only the senior management of an organization can determine which threats are tolerable and which must be addressed immediately based on the organization's mission, goals, strategic plan and budget. Senior management's support and personal participation is critical to the effectiveness of any risk management program and is vital to demonstrate the company's commitment to the safety of its employees and security of its assets.

Each recommended countermeasure or mitigation effort should be examined for four elements: validity, reliability, cost and implementation timing. Each is critical in determining the appropriateness of recommended countermeasures (GAO, 1999).

Validity: Does the countermeasure do what it is supposed to do? Is it an appropriate application for the threat? Example: If attempting to detect someone climbing a perimeter fence, then a fence vibration detection system would have greater validity than the installation of a digital video surveillance system.

Reliability: Will the countermeasure, over time, consistently provide the mitigation it was designed to provide? Example: Does the hand geometry access control system keep an unauthorized individual from accessing the building 100% of the time? Note that no electronic system, mitigation effort or security program is 100% reliable.

Cost: What is the initial cost of installing or implementing the countermeasure? What are the ongoing maintenance costs? What are the operational costs? All three must be considered to provide the most cost-efficient countermeasures.

Implementation timing: What is the elapsed time required to put the countermeasure into effect? If one countermeasure has a significantly longer implementation time than other available countermeasures, this fact should be underscored.

Never lose sight of the fact that sometimes it is simpler and more cost effective to accept the risk than to bear the cost of a countermeasure. As the cost

After countermeasures and mitigation efforts have been implemented, it is important to operationally test them.

of a countermeasure approaches the value of the asset, the countermeasure's cost-benefit diminishes and it becomes easier to justify the risk than support implementing the countermeasure. Figure 1 (p. 33) illustrates this principle.

Performance Testing

After any or all countermeasures and other mitigation efforts have been implemented, it is important to operationally test them. Does the countermeasure, now placed into the real world, work to reduce the intended threat? Each component, system, process and program must be tested to ensure that the results live up to the expectations at the time of purchase. This testing should be conducted in normal daily operational mode and during simulated emergency situations. If any component, system, process or program does not fulfill the specifications, the supplier (if appropriate) must be required to replace the elements that do not meet the specification. For items that were not formally specified, a determination must be made whether to modify the element to meet the expectations, live with the element and its current capabilities, or remove the countermeasure entirely.

Strategy Review & Modification

An organization's management must continually reevaluate the effectiveness of its risk management program to ensure that existing risk assessment reflects current operations, threats, probability, impact and necessary countermeasures. Because of the ever-changing environment all organizations face, this review should be continuous in nature so that changes to assets, vulnerabilities, threats or hazards do not render the assessment obsolete. The risk assessment should be reviewed at least annually.

After each strategic review, management must determine whether any modifications to the risk assessment are warranted. Many modifications are very costly and may have unintended consequences if not thoroughly evaluated. If a core component of an organization has changed, new threats have developed or technological advances make a system obsolete, modifications should be made. If it is determined that significant changes have occurred or that several new threats have developed, it is recommended that a completely new risk assessment be conducted.

Case Study

Following is a case study of a risk assessment conducted for a manufacturer, installer and service provider of permanent and mobile lighting systems with global influence.

Risk Assessment Case Study

The authors were approached to provide security-related consulting. The company requested this consultation due to a perceived need for enhanced security at its corporate offices. Company representatives instinctively wanted security officers at all entrance points and surveillance cameras installed throughout the facility, although there was no basis for these countermeasures. The authors persuaded the company to participate in a risk assessment to identify and address the company's true risk management needs.

The risk assessment process began by identifying the assessment team members. The final team consisted of the corporate safety manager, corporate counsel, the authors and the insurance company's engineering services representative.

The process began with a review of risk assessment steps and terminology. These assessment steps included identifying the company's exposures, vulnerabilities, threats, hazards and existing countermeasures. The team agreed upon five standard exposures and eight vulnerability categories that covered all of the company's risk. The team then brainstormed all possible threats that could logically affect the company. This list was consolidated into a final list of 37 probable threats.

The team then identified existing hazards within the company and its operations that would facilitate the successful occurrence of each identified threat. This identification used a site survey, review of historical losses, document review, interviews and other means. This information was compiled into a working document that the team could reference during the next steps.

Next, the team estimated the probability of the identified threats and their associated hazards to successfully assail the company assets. The probability was estimated using historical loss data from the insurance company, historical weather data from the National Weather Service, local and regional crime statistics, community surveys, and analytical review of the hazards, existing countermeasures and threats.

The company representatives on the assessment team were challenged to define the possible losses inflicted by each identified threat. The authors developed a document that allowed company team members to more effectively process and rank each threat. Once the probability and impact categories were determined, the team completed a risk assessment matrix to graphically present the combined findings. The results of the teams' efforts are shown in Figure 2.

At this point the team members limited the threat list to the top 10 for presentation and recommendation purposes to the senior management. The authors determined which current countermeasures could be modified and what new countermeasures could be implemented to reduce or eliminate these 10 greatest threats. Each identified countermeasure modification and addition was examined for financial feasibility and documented with a return on safety and security investment calculation. The company asked that the ROI calculations be presented in estimated payback period (years). The calculations included countermeasure costs (determined by countermeasure initial and ongoing costs) divided by cost avoidance (determined by countermeasure effectiveness and threat probability).

The information developed during the risk assessment was documented in a report to the com-

Figure 2

Risk Analysis Matrix

Impact \ Probability	Highly likely	Likely	Neutral	Unlikely	Highly unlikely
Devastating	Fire	Nothing	Arson, tornado	Explosion	Nothing
Severe	Workplace accidents	Labor strikes, homicide	Chemical release	Flood	Terrorism, collapse
Noticeable	Traffic accidents, power outage, cyber crime/hackers, theft, mechanical failure, human error, computer virus, wind, assault	Road construction, power surge, sabotage, vandalism, lightning, embezzlement	Water outage	Nothing	Riot, train derailment, earthquake, acts of war, kidnapping
Minor	Trespass	Hail	Fraud, forgery	Espionage	Nothing

High risk
Moderate risk
Low risk

pany's senior management and presented by the company team members. A secondary report was developed by the authors to provide senior management with recommended countermeasures.

Conclusion

Risk assessments cannot be a one-time activity for any organization. Each organization is an ever-changing entity, where changes over time will affect the risk it faces. Changes that affect any exposure, vulnerability, threat or hazard must be addressed in a risk assessment review or complete risk assessment process. No risk assessment, whether developed by private industry or the government, is 100% accurate. However, conducting any qualitative measure of the potential for losses to an organization is better risk management than not conducting one. Risk assessments allow better examination of an organization's risks because many preconceived notions of necessary safety and security measures may be influenced by media hot buttons, personal biases and organizational pressures. Risk assessments provide an organized methodology that can be used to justify opinions and funding requests.

Each organization must approach the risk assessment process and results of the process differently. No two organizations are the same and, therefore, their risk assessments may vary considerably. Users of risk assessments should understand that although science is a major component in the analysis of risk to an organization a risk assessment is truly an art and will be refined by experience and repetition. ■

References

ASIS International. (2003). *General security risk assessment guideline.* Alexandria, VA: ASIS International Guidelines Commission.

ASIS International. (2004). Security vulnerability. *Protection of assets manual.* Alexandria, VA: Author.

Broder, J.F. (2006). *Risk analysis and the security survey* (3rd ed.). Burlington, MA: Butterworth-Heinemann.

Casualty Actuarial Society (CAS). (2003). *Overview of enterprise risk management.* Retrieved Dec. 29, 2008, from http://www.ucop.edu/riskmgt/erm/documents/overview.pdf.

Committee of Sponsoring Organizations of the Tredway Commission (COSO). (2004). *Enterprise risk management—Integrated framework* [Executive summary]. Retrieved Dec. 29, 2008, from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

Employers Mutual Causalty Co. (EMC). (1993). *Security risk management.* Des Moines, IA: Author.

EMC. (2006). Security. *Loss prevention information manual.* Des Moines, IA: Author.

Health and Safety Executive. (2006). *Five steps to risk assessment.* London: Author. Retrieved Dec. 29, 2008, from http://hse.gov.uk/pubns/indg163.pdf.

Lam, J. (2003). *Enterprise risk management—Incentives to controls.* Hoboken, NJ: John Wiley and Sons.

Landoll, D.J. (2006). *The security risk assessment handbook: A complete guide to performing security risk assessments.* Boca Raton, FL: Auerbach Publications.

McNamee, D. (1998). *Business risk assessment.* Altamonte Springs, FL: Institute of Internal Auditors.

Peltier, T. (2001). *Information security risk analysis.* Boca Raton FL: Auerbach/CRC Press.

Roper, C.A. (1999). *Risk management for security professionals.* Boston: Butterworth-Heinemann.

U.S. Department of Justice, U.S. Marshals Service. (1995). *Vulnerability assessments of federal facilities.* Washington, DC: Author.

U.S. General Accounting Office (GAO). (1999). *Information security risk assessment—Practices of leading organizations* (Supplement to GAO's May 1998 executive guide on information security management). Washington, DC: Author.