

Improving Results with a Security Risk Assessment

By James McGuffey, CPP

This paper is a basic overview of the security risk assessment process. It reflects a process that the author utilizes when requested to assist in the resolution of security incidents or security requests. An example of a security request is the selection of CCTV equipment or an alarm system; a security incident might involve an assault or theft. The author has turned down work because a customer felt rushed to install a security system without first conducting a security risk assessment.

Funds are sometimes spent on unnecessary security equipment or a project that might have been completed with less cost had more research occurred, while in other cases spending a little more money on a comprehensive integrated security system would eliminate man-hours and reduce labor cost significantly. An experienced security manager or consultant understands the importance of performing a security risk assessment prior to changing a security system or process.

A security program's objectives are to deter, delay, detect, deny, respond to and or recover from reasonably foreseeable events. Understanding security problems that a company is experiencing will help meet these objectives. This is done by assessing threats that could impact assets, the probability of these threats becoming loss events and the impact on assets should the loss event occur.

Once it is determined that a loss will have a negative impact on organizational assets, countermeasures should be discussed, evaluated for cost effectiveness, tested and implemented. Management will determine the level of risk acceptance for their organization. One example of risk acceptance is the fine-counting currency by banks or other businesses responsible for verifying currency. One business might elect not to fine count \$50.00 bills, citing the cost saved by weighing each strap of currency as offsetting any loss that might occur. Another business might decide that this level of risk is not acceptable and elect to fine count all \$50.00 bills and only weigh straps of \$20.00 bills or lower denominations. Another company may decide that all bills to include \$1.00 must be fine counted without exception.

Unless management accurately assesses the level of risk that their organization can accept, their long-term profits and reputation will suffer. Unfortunately too many companies have become breeding grounds for internal theft by opting to accept employee theft as part of doing business. The author has reviewed numerous statistics

and incidents related to employee theft which continue to be a top threat for organizations. Most studies report that between 40% to 60% of employees steal from their employers in one form or another and approximately 1/3 of all business go out of business as a result of theft.

Unfortunately in today's world, many companies have either lost their ability or interest to balance risk with profit. They have gambled on shortcuts to reduce expense, hoping to increase profits while placing their employees, their shareholders and the public at substantial risk of injury and or financial ruin.

THE PROCESS:

Step One: Conduct a Security Survey. A security survey is conducted by an experienced security practitioner along with someone who is familiar with your operation and property. A security survey is the basic tool used in a security risk assessment. It consists of an on-site examination to determine existing security measures, identify deficiencies, establish the protection needed and recommend measures to enhance overall security.

Step Two: Appoint a safety and security focus group. Management appoints a safety and security focus group representing all departments. These participants should be persons who are familiar with day-to-day operations and their facility and property. The security consultant will serve as the facilitator for this group and train them in the Vulnerability/Risk Assessment.

Step Three: Identify assets in need of protection. Assets are people, property, information and reputation of the organization, with people being the most important.

Step Four: Identify risks/threats that could impact assets identified. Risk refers to the possibility of experiencing harm or loss from a security incident, a threat or an event. A threat is a person, place, thing or event which poses danger to an asset.

A **loss event profile** identifies individual threats that could become events. This profile involves understanding the conditions, circumstances, objects, activities and relationships that can produce the loss events.

Following are a few questions to ask when identifying risks or threats that could happen. What person or position could commit the act? Would more than one person be required? How easy would it be to commit the act? Could identification documents be forged easily if needed for access? Could the identity of the perpetrators be learned if activity succeeded? Would the act generate a record or audit trail which would help in the investigation? Would a single occurrence be recognized?

Following are a few but not all possible risks or threats to consider are: employee theft, external theft, workplace violence, assault by stranger in parking lot, fire, robbery, burglary, identity theft, bomb threat, injury, vandalism, natural disasters, industrial espionage, extortion, kidnapping, slander, payroll fraud, accounts receivables and payables fraud, purchasing fraud, receivables fraud, and cyber crime.

Step Five: Determine risk probability and ranking. Loss event/threat/risk probability evaluates the number of ways in which an event can occur. The more ways that a particular an event can occur the greater the probability that it will occur. Factors that impact the likelihood of a threat occurring are: historical experience, social and physical environment, and criminal state of mind. Historical information is often the most helpful since frequency of occurrence suggests probability of future occurrence.

Qualitative and quantitative approaches are used to gather information with the qualitative approach being the most widely used. The **qualitative approach** evaluates data obtained from police and community interviews, contract and employee interviews, analysis of existing procedural and physical security and process and operational studies. This data is used to assess threats and vulnerabilities and implement countermeasures consisting controls that discover a vulnerability or threat, reduce the likelihood of an incident and or reduce the impact of an incident. The qualitative approach is often used when statistical information is not readily available.

The **quantitative approach** utilizes annualized loss expectancy (ALE) which is a calculation of single loss expectancy (SLE) multiplied by annual rate of occurrence (ARO). The quantitative approach attempts to identify those threats and risks likely to occur and rank them in the order of seriousness to the organization and the likelihood that they will occur. Then based on that ranking, appropriate counter measures can be assigned. Ira Somerson, states in *The Art and Science of Risk Assessment* that probability can rarely be precise, and in some cases, promote complacency. The author prefers to use a mixture of both quantitative and qualitative approaches.

Step Six: Determine impact of loss event on the organization. Loss event criticality refers to the impact of a loss on people, property, reputation and information. The Loss event criticality rating assigns letter and numerical ratings to each anticipated event or threat. Criticality ratings used by security practitioners may vary. If unable to assign a probability factor you might note that event Y is more apt to occur than event X.

Step Seven: Determine countermeasures to reduce or prevent adverse impact. When all risks have been identified and prioritized, countermeasures are identified to eliminate or reduce the threat and improve vulnerabilities. Vulnerability refers to a weakness within the system or lack of safeguards. Countermeasures consist of loss

prevention, loss control and loss indemnification that transfer, mitigate, reduce or eliminate the risk or threat. Countermeasures include: police, procedures, personnel, barriers, equipment, and records such as incident reports, access reports and transaction logs.

Security experts agree that the human factor poses the greatest single source of risk for any asset. A good security program begins with hiring the right people. A security risk assessment will help to determine vulnerabilities in your hiring process.

Step Eight: Perform a cost and benefit analysis: Countermeasures and security programs should not cost more than the benefits received and should relate to the level of risk exposure. Prior to spending capital to implement countermeasures, management must measure the return on the expenditures (ROE) which is done by determining the avoided losses (AL), recoveries made (R), and the cost of the security program or expenditure (CSP). $AL+R$ divided by $CSP = ROE$.

On February 17, 2010, a pilot flew his small plane into an IRS facility in Austin, Texas. News stations rounded up well credentialed security experts to solicit comments. One expert stated that we must find a way to have TSA or other guards posted at the 5,000 plus small private air strips across the U.S. It reminded the author of similar countermeasures utilized following our 9/11 attack when well intentioned security experts reacted with a counter measure that called for guards at every location throughout the world without weighing the benefits or costs or liability. Posting these guards without specific post orders or specialized training only served to create a false sense of security and expose people and property to even more danger.

While the author believes in acting quickly to avoid future events, we must always remember a cardinal rule in security that requires cost justification in the selection of countermeasures to ensure that benefits outweigh cost.

Step Nine: Risk management is an on-going process requiring implementation, monitoring, revising and improvement of countermeasures as needed. Many companies maintain comprehensive security systems and processes but fail to continuously track, monitor and revise these programs and processes as needed. The author has investigated thefts, injuries, and other security incidents where a facility possessed state of the art CCTV and alarm systems only to find that the system was not working properly or was not being monitored.

A 2010 burglary case involving more than \$100 million art theft occurred at a Paris Museum where the security alarm was not functioning. The theft occurred early in the morning when an individual wearing black clothes and a mask managed to get inside

the building by slipping through a broken window. The thief, who was recorded by the museum's surveillance system, managed to get in and out of the building without being detected because the alarm system had been broken for nearly two months.

Which businesses require a risk assessment?

All businesses can benefit from a security risk assessment regardless of size or nature of work performed. Let's look at a laundry room located inside an apartment complex located in a tough inner city area. There are inherent risks to this sort of operation such as assaults and vandalism but one risk that may be overlooked is the theft of copper since this metal is now a highly sought after item.

Copper theft at a laundry room may result in flooding to the apartments after the copper piping connected to the washers is cut. Damage from flooding will likely cost more than the actual loss of the copper, not to mention the interruption of service to the tenants. Each business is unique and the risks impacting one.

A security risk assessment will not prevent all threats from occurring but it will help to avoid or mitigate many of the threats that you would otherwise not be prepared to handle.

Value added from a security risk assessment.

1) Risk assessments help to raise security and safety awareness and are more apt to succeed when employees are involved in the assessment process. 2) Risk assessments help to identify risks that could result in injury to employees or customers resulting in 3rd party law suits. Judgments can exceed the amount of coverage provided by insurance and punitive damages may not be covered. 3) Risk assessments can have an immediate impact in reducing expenses and increasing profits. 4) Risk assessments look at the cost effectiveness and efficiency of existing controls. Funds spent on equipment or systems that are not properly utilized or managed are not contributing to the bottom-line. 5) A risk assessment is recommended prior to designing or making major changes in a security program. A security manager might be wasting funds as well as placing the organization at legal risk. 6) The Sarbanes-Oxley Act of 2002 directs management of publicly held companies to prevent and detect fraud within their organizations related to financial reporting. Risk assessments will not only help meet some of the SOX requirements, it will also help increase morale, productivity and profits.

Who should conduct a risk assessment?

The author recommends that only security practitioners, who are experienced and credentialed, work with management to conduct security risk assessments.

Evaluating the foreseeability of a threat is crucial in the assessment process.

Historical records are important in determining future events. Records maintained by the organization relating to losses and loss events are helpful when assessing future incidents since frequency of occurrence suggests probability of reoccurrence.

Police and other community interviews, employee and contractor interviews, existing physical security and procedures, other facilities and like businesses, standard of care and best practices for similar businesses, police response, access roads, etc. are also considered.

Balancing risk with profit is a must for long-term sustainable results.

A day does not pass without the news media reporting a serious safety or security incident resulting from lack of security or safety processes in place. In April 2010 a large coal mining company well known for their focus on profits incurred an explosion that resulted in the death of 25 workers. The media reported that this company had been cited for 600 violations in the past year at the location where the explosion incurred.

Too many companies continue to deliberately place profits ahead of employee and public safety by refusing to balance profit with risk. Only when productivity is made equal to safety and security will an organization be able to protect assets which include people, property, information and reputation. Existing business models of “profit at all cost” must change!

REFERENCE SOURCE: “The Art and Science of Security Risk Assessment” Ira S. Somerson, CPP 2009 ASIS International.

Disclaimer: *This paper is based on what the author believes are generally accepted security principles as of the date of its writing, and on data gathered from what are believed to be reliable sources, this article is written for general information purposes only and is not intended to be, and should not be used as, a primary source for making security decisions.*

ABOUT THE AUTHOR: James McGuffey, CPP has 38 years of security and safety management experience with responsibility for the protection of approximately 70 high risk facilities in various parts of the U.S during his career. He is now a security consultant and has been retained as an expert witness by defense and plaintiff firms for security and safety incidents. Jim is an expert on premise security and teaches businesses how to conduct security risk assessments to protect people, property, reputation and information.

Jim earned numerous national awards for consistently improving safety, security and profit while working for global leaders in the security/transportation industry where he held the positions Area General Manager, District Manager and Regional Vice President with full P&L responsibility for various profit centers.

Jim earned a B.A. in Criminal Justice from Aurora University and an M.A. in Management from Webster University. Jim served 3 years in the military and 8 years in law enforcement and is an adjunct professor teaching criminal justice courses at a college near his home.

Jim has been an active member of A.S.I.S. since 1981 and is also a member of International Association of Professional Security Consultants (IAPSC). Jim earned the Certified Protection Professional certification which is valid through December 31, 2012. Throughout the world, the Certified Protection Professional (CPP®) designation is acknowledged as the security profession's highest recognition of practitioners. It is evidence that an individual is "Board Certified in Security Management." The CPP® is awarded based upon experience, education, and of an examination that provides an objective measure of an individual's broad-based knowledge and competency in security management. Ongoing professional development is required in order to maintain the credential. The CPP® is administered by ASIS International, the preeminent international organization for security professionals, with more than 35,000 members worldwide.

Please contact Jim at 215-460-7370 or jimmcguffey@verizon.com for any questions regarding the Security Risk Assessment Process or to learn more about our services provided. www.acesecurityconsultants.com

Revised July 11, 2010