Primer on

Security Risk Management

— A WHITE PAPER —

June 2020

Prepared by: Kevin E. Peterson, CPP
Innovative Protection Solutions, LLC
Post Office Box 5066
Herndon, Virginia 20172-1964
703-318-7181 info@innovativeprotection.com

PART 1

Risk Assessment

Introduction

Whether in the public or private sector, and whether dealing with traditional or cyber security (or both), assets protection[1] practice is increasingly based on the principle of *risk management*. The term "risk management" has been in common use in other fields such as insurance, finance, investments, business, research & development and engineering for many years; however, it has more recently been applied in security management and assets protection. The concept is a perfect fit for the field of *assets protection* since our primary objective is to *manage* risks by:

- balancing the cost of protection measures with their benefit
- seeking synergy in protective measures, and
- aligning the protection approach with the organization's strategic goals

The title of this paper is ***Security*** Risk Management to distinguish the subject matter from risk management perspectives from other fields such as those listed above. More recently, the term *Enterprise Security Risk Management* (ESRM) has entered the lexicon and its practice is steadily evolving into the standard for the security and assets protection arena. Although the domain of ESRM goes beyond what is addressed in this paper[2], our primer forms a solid foundation for its application, both in the conceptual and practical realm.

Taking a Strategic Risk Management Approach

Too often organizational leaders look to the "quick fix" to satisfy their security needs. They buy a popular security system or are convinced by a sales representative that a particular product or service is the all-encompassing answer to their protection needs. They are convinced that their critical assets are then completely safe without ever even asking what those assets are or what types of threats they face.

This is a particular problem for small and medium-sized businesses, but could certainly apply to any size enterprise. As early as the 1990s the need for a strategic approach – and a new paradigm - was recognized even if it wasn't necessarily called "security risk management" at that point. According to security consultant and investigator Robert Gardner, CPP speaking about small businesses:

> One critical area…where outside professional advice is [too] seldom sought…is security and loss prevention. Too often, [security] measures, if they exist at all, are implemented as a hurried reaction to a bad experience. These are frequently emotional rather than logical decisions. Little or no research is done. Little effort is made to distinguish between real and perceived problems. No consideration is given to alternatives. The end result is a collection of independently operating procedures that, in some cases, may actually make matters worse. The benefits of a thoughtfully designed and coordinated system are lost. The patchwork approach to problem solving works no better in loss prevention than it does in the rest of the business world.
>
> (Gardner, 1995)

[1] The term "assets protection" is often associated with the area of financial investments, however in the context of this document it refers to the comprehensive and proactive function which serves to protect any organization's people, property, information and intangible assets against all hazards, as outlined in the ASIS publication "Protection of Assets," Security Management Volume (see Sources Cited).

[2] See Enterprise Security Risk Management Guideline, ASIS-ESRM-2019

The solution to the adverse situation that Gardner described is to develop a comprehensive *assets protection* strategy based on a strategic risk management approach. Taking a "strategic approach" means basing the enterprise's *assets protection* practice on sound *planning, management and evaluation*, and taking into consideration both the organization's mission and the environment in which it operates. A "strategy" should articulate – to you and to your executive decision makers – ***what*** you're protecting, ***why*** you're protecting it and ***how*** you're protecting it (Peterson, 2006).

Another early description of the concept was provided by the National Infrastructure Protection Center (NIPC)[3], which defined *risk management* as "a systematic and analytical process by which an organization identifies, reduces and controls its potential risks and losses." They further stated that *risk management*:

- Identifies weaknesses in an organization or system
- Offers a rational and defendable method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valuable assets
- Improves the success rate of an organization's security efforts by emphasizing the communication of risks and recommendations to the final decision-making authority
- Helps security professionals and key decision-makers answer the question "How much security is enough?"

(National Infrastructure Protection Center, 2002)

It's useful for security professionals to review sources such as this in order to help us recognize that despite constantly advancing technologies and a rapidly evolving global business environment, the underlying concepts of risk management are essentially timeless.

As evidence of contemporary relevance, though, the 2019 ASIS International Guideline on Enterprise Security Risk Management states that "ESRM is a *strategic approach* to security management that aligns an organization's security practices to its overall strategy using globally accepted risk management principles. (emphasis added) (ASIS, 2019) So we see that the goal has always been to assess and manage security risks appropriately and efficiently while striving to help an organization achieve its strategic goals.

The reason that this is a particular challenge for small businesses is that entrepreneurs, innovators launching start-ups and small business owners typically view security risk management as something for large corporations with enormous assets protection resources and internal talent. In reality, it is especially important for smaller entities since their business may be less resilient to potential losses, and therefore even more reliant on a sound security risk management approach.

Ultimately, the outcome should always be a strategic approach to planning and implementing a well-orchestrated medley of mitigation measures (often called "risk treatment" or "controls")

[3] With the establishment of the Department of Homeland Security (DHS) in 2002, the responsibilities of the NIPC were redistributed between the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate and the FBI's Cyber Division.

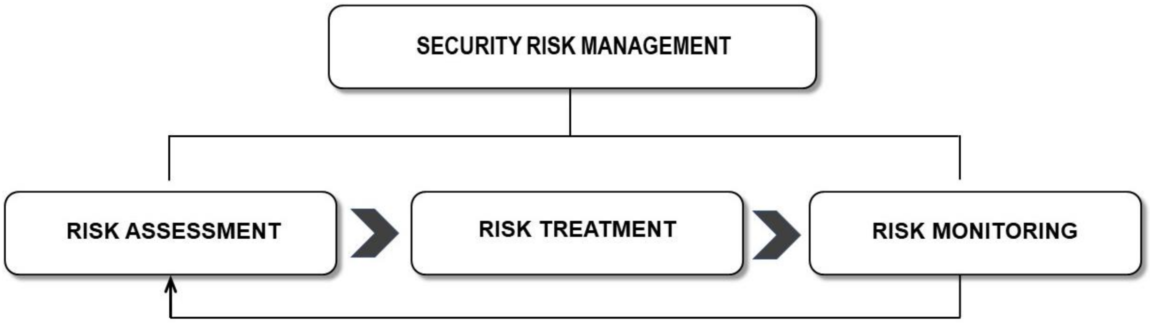
tailored to the specific organization and its current risk management objectives, no matter its size or nature.

The Risk Management Process

Security Risk Management (SRM) can be thought of at two levels: macro and micro. At the macro level, the thinking is more philosophical and generic. Essentially, you identify and measure the problem, do what you can to fix the problem, and then make sure the fix worked and continues to work over time. This general philosophy follows the "Plan-Do-Check-Act" or PDCA model[4] which is commonly used as a basis for International Standards of all sorts.

At the micro, or more granular level, it is a specific process (set of steps) that can be applied to a specific organization, subunit, location, project, activity, operation or even a particular asset.

Figure 1 - Elements of Security Risk Management at the Macro Level



© 2018 Innovative Protection Solutions LLC. All Rights Reserved.

Figure1 shows the Risk Management process at the macro level. The first element is ***Risk Assessment***. This is critical because it essentially defines what is being protected, what it is being protected against, what weaknesses or relevant conditions exist, and protection priorities. It then begins to develop the framework for a protective strategy (***Risk Treatment***[5]) which is tailored to the entity being protected – whether that is an organization, facility, person, project, intangible asset or something else. Once a protection strategy is in place and operating as a routine, it must be monitored on an ongoing basis (**Risk Monitoring**) to ensure the system is functioning properly and that any relevant changes are noticed and addressed in an appropriate manner.

Viewing SRM at the macro level is valuable since it is, in essence a *mindset* - a way of thinking about how to protect an organization's ability to perform its mission and thrive.

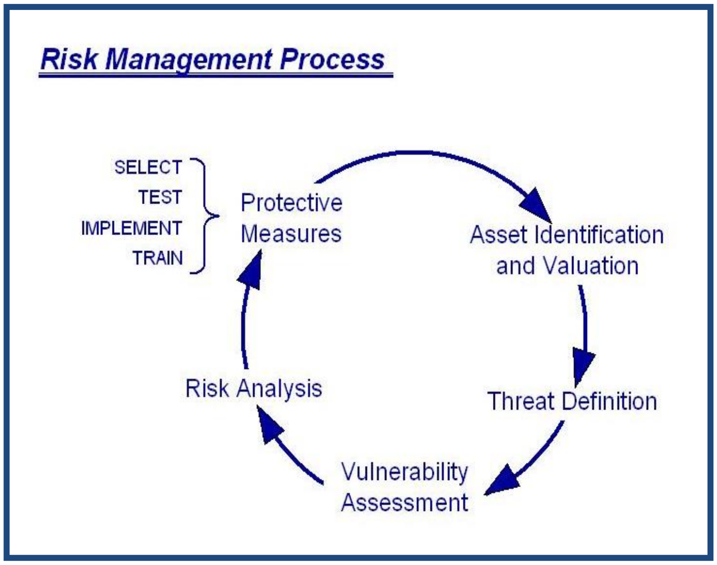
[4] For more information on the PDCA Model, visit the American Society for Quality at https://asq.org/quality-resources/pdca-cycle

[5] "Risk Treatment" is the term commonly used in current international and national standards. It is also known as "Risk Mitigation," "Risk Controls," or "Countermeasures."

On a more granular level, there are five steps in the security risk management process (see Figure 2). The steps align with the elements at the macro level. Notice that the first four steps depicted in Figure 2 (assets identification/valuation through risk analysis) represent “assessment,” the fifth step (protective measures) represents “treatment” and the cyclical nature of the process represents “monitoring.” This process actually implements Security Risk Management and can be applied in any business or organizational setting or level.

The five steps of the *Risk Management Process* ultimately lead to a comprehensive *assets protection* strategy which functions – often behind the scenes – on an ongoing basis. It all begins with identifying realistic assets protection objectives and then conducting a comprehensive risk assessment (described below) which forms the basis for a protection strategy. This can be done at the enterprise-wide level and/or at the specific process or project level. Depending upon the nature of the business it may be appropriate to do it at multiple levels.

Figure 2 - The Security Risk Management Process (Micro Level)



© 2002 Innovative Protection Solutions LLC

Step 1 – Assets Identification and Valuation. The first step in the risk assessment is identification and valuation of assets. As Gardner asserts, “the first step in establishing [any] effective [assets protection] program involves identifying the businesses’ assets” (Gardner, 1995). Although this is a step that is frequently overlooked, no effective security program can be implemented without a thorough understanding (on the part of both the asset owner and the security professional) of what it is that is being protected – or *should* be protected. All three types of assets – tangible, intangible and mixed - should be considered and incorporated into the risk assessment process. Too often, asset owners and security professsionals focus exclusively on tangible assets or on those which appear on the accountant’s balance sheet. This is a major mistake, as increasingly, a predominant portion of an organization’s value lies in intangible and mixed assets (ASIS, 2020).

Each component of the *risk management process* must be evaluated (gauged or rated); and this can be done either qualitatively or quantitatively. The value of *assets* are often expressed in dollar amounts, but assigning such a number is not always possible, particularly in the case of intangible and mixed assets. Even when dollar values are assigned, a credible number which can reasonably be defended can be elusive, and often times simply cannot be determined.

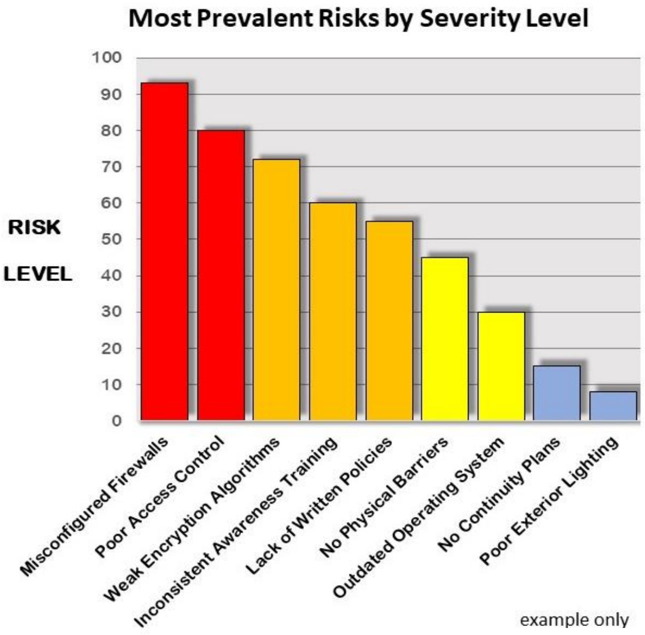
This provides a natural lead in to the debate over *qualitative* versus *quantitative* assessment and analysis approaches. Each approach has inherent pros and cons. The bottom line, however is that the most appropriate approach will be determined by the desires of the executive decision maker and the preferred style of the assessor (security professional).

> *Qualitative Analysis* – is any approach which does not use numbers or numeric values to describe the risk components. Generally, comparative terms (descriptors) such as “critical,” “high,” “medium,” “low” and “negligible” may be used to gauge the asset value, other risk components and the level of risk itself.
>
> *Quantitative Analysis* – is any approach which uses numeric measures to describe the value of assets or the level (severity or probability) of threats, vulnerabilities, impact or loss events. It can vary from simple rating scales (e.g., 1 to 5) or rankings to sophisticated statistical methods and mathematical formulas[6].

Sometimes it is most appropriate or convenient to use a “blended” approach which combines elements of both qualitative and quantitative approaches. Another technique is to begin with a qualitative analysis and then progress to a quantitative process for more detail.

Many executive decision makers prefer information to be summarized in charts and graphs which can display a great deal of data in a concise manner. (One example is shown in Figure 3) This is the strongest argument for using a quantitative approach. The other major advantage is the ability to manipulate the data automatically using computer programs and algorithms.

Figure 3



© 2020 Innovative Protection Solutions, LLC

Qualitative methods, on the other hand, are generally simpler and quicker to use, and often provide results that are just as meaningful as numeric calculations. In either case, the most important steps are to:

- clearly define each “level,” “rank” or “descriptor” used in the assessment/analysis[7], and
- ensure that the quality of the input is the best possible (i.e., be sure to avoid “garbage in → garbage out”)

[6] There is a wide variety in how professionals define “quantitative analysis.” Our purpose here is to keep the process as simple as possible in order to serve the security professional and asset owner with a minimum of complexity and confusion.

[7] This is important so that both the assessor (security professional) and the client/executive decision maker have a common understanding of what is meant, for example, by a “high” threat.

One of the difficulties in determining the value of an organization's assets is the lack of agreement on exactly what "assets" are. The assessor (security professional) and the asset owner must agree at the outset on what will and will not be considered an "asset" for the purposes of the assessment (and overall SRM process). Many asset owners and senior executives themselves, do not have a clear understanding of their assets – other perhaps than those that appear on the balance sheet.

Among the factors to consider in determining asset value for *tangible assets* are immediate response and recovery costs, investigation costs and replacement costs, but also indirect costs (which are often overlooked in the overall assessment). Indirect costs may include such things as:

✓ temporary leased facilities
✓ equipment rental/purchase
✓ alternative suppliers/vendors
✓ alternative shippers/logistics support
✓ temporary warehousing facilities
✓ special employee benefits
✓ counseling/employee assistance
✓ loss of market share (temporary or permanent)
✓ decreased employee productivity
✓ increased insurance premiums
✓ temporary workforce/staffing
✓ recruiting/staffing costs for permanent workforce
✓ increased security costs (temporary or permanent)
✓ increased need for communications capabilities
✓ data recovery/IT system restart-reconfiguration
✓ administrative support needs
✓ increased travel
✓ marketing/public relations efforts
✓ emergency/continuity plan revamps

In addition, intangible and mixed assets must be considered even though they are generally very difficult to valuate. Executive decision makers need to be educated with respect to intangible and mixed assets. Although it is often difficult or impossible to place a specific dollar value on them, they are certainly subject to loss events and can have a significant impact on the organization's vitality and mission performance.

Threat. Enterprises - regardless of size, location or mission - face a wide variety of threats. These fall into the three categories: *intentional, natural and inadvertent*. A comprehensive – and hence more meaningful – threat assessment will consider all three categories of threats. Since September 11, 2001, it is common to focus heavily (sometimes almost exclusively) on the terrorist threat when conducting corporate or organizational risk analyses. However, terrorism is only one aspect of one category (intentional) of threats which should be considered. This tendency is not unique. In the mid 1980's, for example, there was a strong emphasis on the theft of advanced military technology. At other times, the security community has focused heavily on white collar crime, cyber attacks, natural disasters or other calamities. For the foreseeable future there will rightfully be an intense emphasis on the pandemic threat.

What is needed however, is a balanced approach to threat assessment. Of course, some types of threats will be more prevalent at certain times and in certain places. Long term assets protection strategies, however, must be based on a realistic, full scope and balanced threat assessment. According to security expert and author Ira Winkler, “accurate assessment of the level of threat against your organization is critical to the success of your…security plan.” “Threat is an essential factor in your risk reduction formula, and you must consider it carefully. If you don’t, you’ll simply be flying blind when it comes to prioritizing countermeasures…” (Winkler, 1997, p37)

In terms of evaluating levels of threat (again either qualitatively or quantitatively), we generally rely on the following approaches for each of the three categories:

> ***Intentional Threats*** – Evaluation of intentional threats is based on identification and study of potential adversaries. Assessors should think ”outside the box” when listing potential adversaries. For example, the most obvious adversary in a particular case may be international terrorist organizations, organized crime or aggressive business competitors. Another important potential adversary, however, may be activist groups (such as environmental rights activists, other special interest groups or even the violent protesters who participated in riots in several US cities during 2020) – and this threat could be easily overlooked. The identification and assessment of adversaries is a growing challenge today based on the post-Cold War environment, the global nature of our economy, worldwide demographic shifts and the emergence of a far more asymmetric (less conventional and more difficult to define) or ambiguous nature of modern day threats.
>
> In most cases, adversaries can be judged according to their *capabilities* to cause a loss event (or perpetrate a successful attack) and their *intentions* to do so. Among the sources of information on adversary capabilities and intentions are: past history, organization rhetoric, public pronouncements, other open sources, internal communications (newsletters, Web Sites, etc.), law enforcement reports, automated databases and threat assessment professionals.
>
> ***Natural Threats*** – Rather than adversary capabilities and intentions, natural threats are typically evaluated using historical trends and statistics. Long-term data is generally collected on weather and other natural hazards for specific geographic areas, terrains and environments. In some cases, natural hazard effects data has been assembled for particular industry sectors or facility types. Although this data provides extremely useful planning information, assessors must recognize that the unexpected can, and usually does occur. Therefore, comprehensive contingency planning and at least some degree of all-hazard preparedness is strongly recommended by most professionals. Government sources such as the National Weather Service, National Oceanographic and Atmospheric Administration, the US Geologic Survey and state equivalents can provide a wealth of information useful for planning purposes.
>
> ***Inadvertent Threats*** – Perhaps the most overlooked or neglected threats are inadvertent threats. They include accidents, errors and omissions. Security expert and author Ira Winkler put it best when he opined that the biggest threat to US corporations is human error. As he stated, “People make mistakes, and those mistakes are the most likely things to hurt you.” (Winkler, 2005, p 54)

Another key consideration – which is a subset of the *inadvertent threat* - is that of peripheral threats – for example a threat which is targeted at a neighboring facility, but which may have a major impact on your operation. The effects of peripheral threats can include: utility interruptions, required evacuations, closure of access routes to your facility, unwanted attention or traffic at your facility, full or partial operations shut-downs, productivity or supply chain disruptions, and environmental effects (e.g., smoke, debris, water or chemical runoff, etc.).

Inadvertent threats are the most difficult to predict and prepare for. Although, to some degree, knowing the nature of the mission, workforce, operations or other environmental factors can contribute to the ability to anticipate inadvertent threats, there is usually little or no historical data to use for planning purposes. It might be helpful to study accidents and errors that have occurred in the same or similar industries or types of facilities. The best defenses are preparation, education & awareness, and the realization that inadvertent and peripheral threats exist.

Vulnerability. The most common view of "vulnerability" is a security *weakness* or *problem*. Although this can be the case, we must also recognize that some vulnerabilities are simply existing conditions or business practices which support mission accomplishment. For example, engaging in sales by e-commerce can be viewed as a vulnerability, but it may also be an essential way of conducting business for a particular company. One concise definition of 'vulnerability' is "a weakness, condition or organizational practice that may facilitate or allow a threat to be implemented or increase the magnitude of a loss event." (Peterson, 2006)

One important difference between a *threat* and a *vulnerability*, is that a vulnerability is a characteristic of the organization, asset, project or facility. As such, it is generally something over which the organization or asset owner can exercise at least some degree of control. Threats, on the other hand, are usually outside the control of the organization.

Vulnerabilities can be evaluated in different ways, but one common approach is to measure them in terms of *observability* and *exploitability*.

- ***Observability*** is the ability of an adversary to see and identify a vulnerability. For example, a hole in a chain-link perimeter fence will likely be highly observable by a potential adversary, whereas an inoperable surveillance camera would not.
- ***Exploitability*** is the ability of the adversary to take advantage of the vulnerability once they become aware of it.

In assessing natural threats, we can still use the concepts of observability and exploitability, although from a slightly different perspective. The *observability* factor would essentially be reversed, and refer to our ability to observe – or become aware of, track, etc. – the oncoming threat (e.g., storm). This involves mechanisms for early warning and notification of the impending threat. On the other hand, exploitability would be expressed in terms of the particular threat's ability to cause damage specific to our facility, mission or organization.

Using this observability/exploitability approach, security and risk management professionals can assess and develop plans to mitigate vulnerabilities both in the long-term (strategic) and immediate (tactical) time frames.

For inadvertent threats, the observability/exploitability approach is again slightly different. In this case, we measure our vulnerabilities via two questions:

- are we aware of the vulnerabilities? and
- are the particular vulnerabilities subject to relevant inadvertent threats?

Again, both the inadvertent threats and associated vulnerabilities are generally the most difficult in any organization to identify and measure. This should not, however, be used as an excuse for neglecting this aspect of the overall risk posture.

Risk Analysis. In this step, the assessor puts all of the information on assets, threats and vulnerabilities together, and then considers the potential impact or consequences of a loss event. In all risk analyses, but particularly in quantitative ones, it is advisable to determine the evaluation levels (for threat, vulnerability and impact) by committee. In other words, assessments should be performed by a multidiscipline team of subject matter experts[8] in order to reach credible and justifiable numbers as input to the analysis. Justifying the numbers is the area where assessors are most often challenged by clients, executives and decision makers in terms of reporting their *Risk Analysis* results.

There are many effective and time-tested approaches to calculating risk results once the numbers (evaluation levels) have been identified. One relatively straightforward approach uses the formula shown below to calculate the overall risk:

$$\textbf{Risk} = (\textbf{Threat} \times \textbf{Vulnerability} \times \textbf{Impact})^{1/3}$$

Using this formula, which multiplies the risk factors rather than adding them, recognizes that if any single factor is zero, the resulting risk is zero (at that time and place). In this approach, the evaluation factors (threat, vulnerability and impact) are rated on a 0 to 100 scale. Such a scale is easy for people to understand because they are accustomed to thinking in terms of percentages. Using the cubed root places the overall risk figure back on the 0 to 100 scale again, one which is easy for people to understand and to visualize using charts and graphs.

In a quantitative or blended assessment, a numeric scale for the evaluation factors is established (see Figure 4) and specific definitions for each range (critical, high, medium and low in this example) determined. The range definitions should be relevant to the type of facility,

Figure 4

Example of numeric range assignments for descriptive Risk levels

Key to Risk Factor Evaluation

Critical	**76 – 100**	🟥
High	**51 – 75**	🟧
Medium	**25 – 50**	🟨
Low	**<25**	🟦

[8] Team members and the required expertise must be tailored to the individual assessment. Examples of team member expertise may include: Physical Security, IT Security, Information Protection, Personnel Security, Technical Security, Operations, Audit and Safety.

industry sector and/or environmental factors which will influence the client's perspective of threat, vulnerability, loss event impact and overall risk.

Risk analysis results should be presented to the client or decision maker in a manner which assists them in understanding the data and making excellent decisions. This includes placing the identified risks in a priority order or into priority categories to help show, from the assessor's perspective, which risks should be addressed first.

A final note about risk analysis, as discussed in a 2000 *Security Management* article entitled "Truth & Consequences," we need to consider low probability/high consequence risks as well as those that are most likely to occur in our workplace (Garcia, 2000). Many corporate executives and decision makers only want to hear about the risks that represent the highest probability of occurrence – that's where they want to expend their resources. We must also, however, give serious consideration to potential losses that, although they are not highly likely to occur, will result in very significant consequences (mission impact) if they do occur. Examples of such risks might include terrorist attacks and catastrophic workplace violence or active shooter incidents. Again, the objective of a comprehensive assets protection strategy is a rational balance between focus on high probability-of-occurrence risks and low probability/high consequence risks. (see "Likelihood versus Consequence Scatter Charting" on page 13.)

Protective Measures. After a thorough risk analysis, the next step is to recommend a suite of protective measures which effectively address the relevant risks while considering available resources and minimizes any adverse impact on the enterprise's mission and operations. In other words…"now that we know the problem, how do we fix it?"

This suite of protective measures represents the heart and soul of our assets protection *strategy*.

As indicated in the *Security Risk Management Process* diagram on page 5, this step involves a number of sub tasks. They generally include:

- **Select** – Although this may seem straightforward, it often is not. Security professionals should offer a "menu" of possible options to effectively address the identified risks. According to a National Infrastructure Protection Center (NIPC) publication on *risk management*: "whereas a single countermeasure may seem intuitive to an analyst or security manager, alternative countermeasures should be identified and evaluated to select those which offer an optimal trade-off between risk reduction and cost" (National Infrastructure Protection Center, 2002). Options or option "packages" may be arranged by cost level, urgency, convenience level, aesthetics or some other factor. Despite the fact that the security professional is offering a variety of options, he/she should present a "recommended option" based on their expertise and understanding of the client's needs.
- **Test** – In many circumstances, recommended hardware, software or procedures will have to be tested against several questions. These may include: Does the solution operate as expected in this specific environment? Does the integration of different components of the overall system with one another seem to be successful? Is the

solution operating as expected with other systems in the facility? Is the solution having the desired effect in terms of risk reduction? Are people (security staff, employees, facility users) adapting well to the new solution? Can we accurately project the short-term and long-term costs of operating the system? In some cases, these questions cannot be answered until the solution is up and running. For this reason, it may be advisable - where possible - to implement the solution (or parts of the solution) on a trial basis or in a limited physical area (e.g., part of the building) to allow for such testing, and to "work out the bugs."

- **Implement** – This task may be simple or complicated depending upon the solution which has been selected. Among the factors which should be considered when implementing a solution are: notification of employees (and visitors if applicable), cost of installation, possible disruption to facilities or access to them, possible downtime or partial facility closures, the need for signage to support the new solution, facility access for an installation team/contractor, necessary changes to policies and/or procedures, and the time needed for staff and employees to acclimate to the solution.
- **Train** – Depending on the nature of the selected solution, security staff and/or employees themselves may need to be trained on new hardware or procedures. This training must be factored in to the cost of the solution in terms of time and money – and should be incorporated into the overall implementation plan.

A more thorough discussion of this step is provided in Part 2 of this primer, "Risk Mitigation," which begins on page 17.

Risk Analysis...Automated or Manual?

A variety of automated tools (software programs) are available on the market to assist in performing risk assessments and risk analyses. There are pros and cons to using such tools, but the operative term is "assist." Software programs should not be relied upon as the sole vehicle in conducting an assessment or analysis. Among the arguments against automated tools for this purpose are:

- the possibility that individuals with no knowledge of assets protection concepts or practice will mistakenly believe that they can purchase a piece of software, plug it into their computer and conduct a meaningful risk assessment on their own
- the high cost of some commercial software programs
- the undue complexity of some commercial software programs (the use of unnecessarily complicated programs for relatively straightforward assessments)
- the fact that computer programs cannot or do not factor in unquantifiable characteristics (which may have a significant influence on risk) such as the "personality" or culture of an organization

Automated risk analysis tools are, in general, not good at dealing with intangible factors and information which is difficult to quantify. One example of such information is the "nature" (or character) of a particular risk – a very important consideration in risk analysis in most cases. In writing on the topic of long range planning, the renowned management expert Peter Drucker stated that "it is not only the <u>magnitude</u> of risk that we need to be able to appraise…it is above all the character of the risk (Drucker, 1970)[*emphasis added*]. This principal applies equally to the security-related risks we are addressing here.

There are, however some advantages to using software tools as an aid in some cases. Such tools are very effective at storing, processing and manipulating large amounts of data and numeric values. In a risk analysis, they can compare related data and project the benefit of various protection options. They are also valuable in situations where a large number of similar assessments are being conducted or where multiple assessments which are extremely complex will be performed. For example, the US Federal Protective Service uses software tools to perform physical security assessments at hundreds of Federal Government facilities around the United States. The assessments are all very similar and require a strongly systematic and repeatable process. In addition, the assessments are retained and can be compared with previous surveys. In this case, a software tool is definitely appropriate.

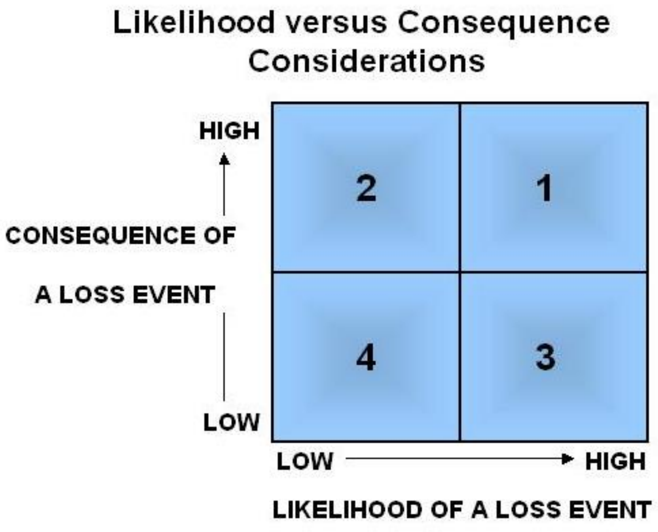
Another effective use of risk analysis software tools is for comparing the relative benefits for a number of different protection options or combination of options.

In the end, however, whether using sophisticated software tools or manual processes, the meaningfulness of the risk analysis results will depend – to a very high degree - upon the quality of the input. Automated programs that require the user to “guess” at dollar values and other numeric inputs will result in a risk calculation that is nothing more than the input…a guess. Security professionals, clients and executive decision makers alike, must recognize this fact and accept it.

Likelihood versus Consequence Scatter Charting

Another method of considering organizational risks is the use of a “Likelihood versus Consequence Matrix,” sometimes referred to as a “scatter chart.” Conceptually, any organization must consider the question of *likelihood versus consequence* (impact) for their relevant risks or potential loss events. This is simply an inherent part of a credible Security Risk Management or Assets Protection program. The diagram below illustrates this issue by way of four quadrants.

Figure 5


Likelihood versus Consequence Considerations
HIGH
CONSEQUENCE OF
A LOSS EVENT
LOW
2
1
4
3
LOW
HIGH
LIKELIHOOD OF A LOSS EVENT

Logically, a risk (potential loss event) located in Quadrant ‘1’ would require the most urgent attention and resource allocation. These risks have a high likelihood of occurring and, if they do, will have significant consequences or impact on the organization. The consequences may be in the form of increased operating costs, damage to reputation/public trust, decreased safety or efficiency, loss of personnel resources, loss of or damage to facilities/equipment, or loss of critical information.

The priority of addressing risks will generally decrease with each successive quadrant. Many organizations, however, neglect the fact that quadrant ‘2’ warrants significant attention. Risks which lie in this quadrant have a low to moderate likelihood of occurrence, but a high consequence or impact if they do occur. Examples of risks which typically fall into quadrant ‘2’ are dramatic workplace violence incidents and terrorist attacks.

Risks which fall into quadrants ‘3’ and ‘4’ should not be automatically discounted. Various events (reorganization, expansion, adding new missions, change in neighbors, change in threat level, etc.) can easily move some risks from one quadrant to another. For this reason, security and management officials must periodically review the risk posture as well as operational and administrative changes which may influenced the “likelihood versus consequence” equation.

Additional “consequence” considerations include legal liability and damage to the organizational culture and workplace atmosphere. The overall protection strategy and component measures should be subject to a periodic cost-benefit analysis based on projected consequences of a loss event including legal liability and other impacts on critical assets.

The Likelihood versus Consequence scatter charting technique may be used in combination with a traditional risk analysis method. This often provides a more comprehensive and accurate picture of the risk environment (and contributing factors) than the use of one method alone. It can also inspire a more creative way of thinking about risk and how to address it.

Leveraging Outside Expertise

It is often highly advisable to involve a carefully selected vendor or outside consultant in the development of the risk assessment process and protection strategy. As Gardner writes: “in order to implement an effective security program, managers must…be aware of the true threats to their business. Very few managers have the training and experience necessary to conduct a meaningful risk analysis for their business.” He continues, “unfortunately, it is all too common that any security related advice and guidance a business manager may receive comes from a sales person rather than an independent security expert.” “This approach to security management invariably results in inadequate protection and a false sense of security.” (Gardner, 1995) …not to mention the waste of valuable resources.

The benefits of outside expertise include the fact that an “outsider” brings a fresh view and is not tainted by previous opinions, prejudices/preferences and organizational politics. Reputable consultants and vendors also bring expertise and up-to-date knowledge on best practices, techniques, products and industry standards which may or may not exist within the organization. As in any outsourcing endeavor, the consultant/vendor should be chosen carefully in consideration of their specialty, experience, professionalism and the degree to which they are truly independent. Ensure there is a clear and mutual agreement among all parties on the purpose and scope of the project as well as any relevant constraints and the expected product.

Finally, we must recognize that security risk management is a cyclical process – one which must regularly re-evaluate changes in assets, threats, vulnerabilities, loss event impact and risk treatment implements. These factors are in constant flux and must be monitored deliberately and carefully to ensure that the protection strategy and its components remain both effective and efficient – and continue to support the strategic goals of the enterprise. Hence, risk monitoring is essential. This may include the use of metrics to aid in the monitoring process.

Although there will often be other factors such as budgets, culture, organizational structure and political considerations, the organization's *assets protection* strategy should always be primarily risk-based. More detailed information on risk assessment and quantitative methods such as Annual Loss Expectancy and Loss Event Profiling can be found in a variety of textbooks and other reference documents.

PART 2

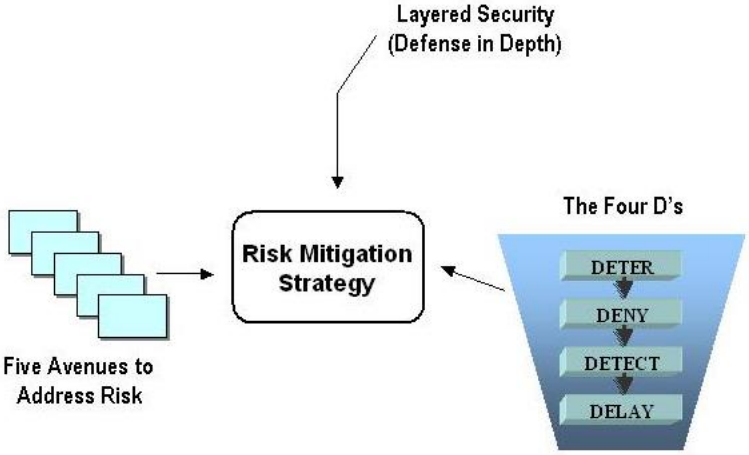
Risk Mitigation

Following a thorough risk analysis, the next step is to recommend a suite of solutions or "mitigation measures" to address the risks that have been identified, and hopefully, prioritized. By "suite," we mean a series of measures that work together and comprise elements of a deliberate plan – or a "mitigation strategy."

The Foundation: A Mitigation Strategy

As mentioned in the introduction to this primer, security risk management must be based on a comprehensive **strategy**. Carefully developing this strategy is essential whether establishing a new security/assets protection program or "renovating[9]" an existing one.

Taking a truly *strategic* approach helps avoid major mistakes such as knee-jerk reactions to incidents/events, introducing inefficiencies, over-relying on vendors or salespeople for solutions, and serious resource misallocations. Any risk mitigation strategy should consider three underlying or foundational concepts: the five avenues to address risk, the four 'Ds," and layered security (defense in depth). The best and most effective protection programs are based on strategies that integrate the philosophies embodied in all three of these foundational concepts.

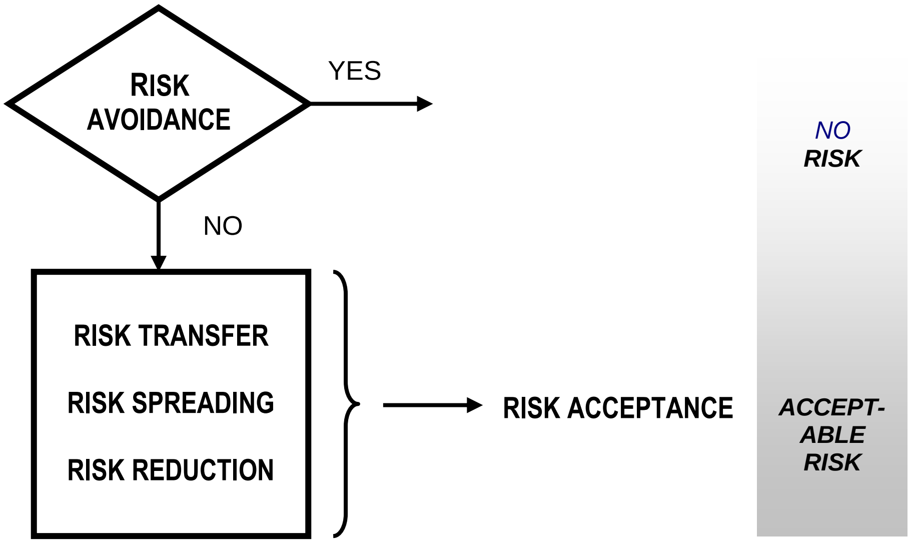


The Five Avenues to Address Risk

This underlying concept is directly related to the comprehensive risk management approach. It contends that there are five distinct avenues we can follow to address identified risks to assets. Generally, a comprehensive *Assets Protection* strategy incorporates a well-thought-out combination of all or most of these avenues. The five avenues are: risk avoidance, risk transfer, risk spreading, risk reduction, and risk acceptance.

[9] As used here, the term "renovating" refers to updating, expanding, correcting, re-focusing or otherwise changing a security or assets protection program which is currently in place. This is often done as a result of changes in an organization (acquisition, merger, growth, etc.), a significant security incident or loss event, evaluation of whether a program is meeting its objectives, a new security manager or other situations.

The following diagram illustrates the application of “the five avenues to address risk.” It begins with an initial consideration of risk avoidance, then proceeds to three additional avenues of addressing risk (transfer, spreading and reduction). Ideally, these three avenues are employed in concert with one another as part of a comprehensive strategy. Finally, the diagram shows that any residual risk must be acknowledged and accepted.



© 2006 Innovative Protection Solutions LLC

RISK AVOIDANCE – This is the most direct avenue for dealing with risk. It simply involves removing any opportunity for the risk to cause a loss event. Many security professionals consider *risk avoidance* impractical – and therefore, essentially irrelevant - since the measures required to completely avoid risk will essentially negate the enterprise’s ability to perform its mission or accomplish its objectives. For example, if a business operates an electronic commerce (e-commerce) site, the use of that site introduces some inherent risk in terms of the IT environment. To completely “avoid” that inherent risk, the company would have to shut down the site – and therefore, could not conduct any online business or make any sales.

RISK SPREADING – This very effective practice avoids putting “all your eggs in the same basket.” The best example of this is geographically distributing an organization’s assets. If a company maintains an inventory of high value merchandise, for example, and they stored all of the merchandise in a single warehouse, they would potentially loose 100% of their merchandise if that warehouse experienced a major loss event (e.g., theft, flood, fire, etc.). If, however, their merchandise were distributed among three geographically separated warehouse facilities, the loss event would result in a potential loss of only about one third of their total inventory. This simplified example provides an excellent illustration of the concept of *risk spreading*. Another good example of risk spreading is the practice of off-site back-ups for computer data. By storing a copy of this highly valuable “asset” in another location, a relatively quick recovery from the loss of the original data can be effected. Risk spreading can increase the cost of an operation, but the generally modest costs are usually offset by the decrease in risk to critical assets.

RISK TRANSFER – The typical example of risk transfer is the purchase of insurance. Although not commonly viewed as a part of the traditional "security" function, insurance is generally a key element of an organization's (or individual's) risk management strategy. Another form of risk transfer is the act of making oneself a less attractive target than other potential targets (such as neighboring facilities). Although it may not be considered "polite" this is a way of "transferring" a portion of your risk to your neighbor. In some cases, a portion of risk can be transferred to suppliers, vendors or others through contract clauses or other types of formal agreements.

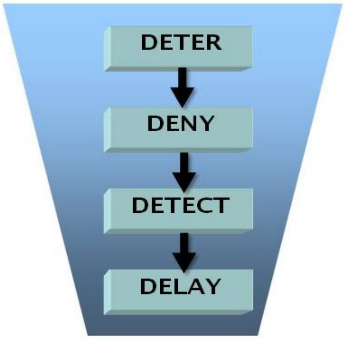
RISK REDUCTION – Essentially, *risk reduction* involves any security measures or other actions that would reduce the risk to assets. The most common and direct means of reducing risk, in this sense, are actions which decrease the vulnerability in the risk equation (whereas *risk spreading* and *risk transfer* primarily decrease the impact of a loss event). Among common *risk reduction* mechanisms are security measures, policy enforcement, and employee education and awareness, as well as financial and legal positioning.

RISK ACCEPTANCE – After all *risk spreading*, *risk transfer* and *risk reduction* measures have been implemented, some risk will remain since it is virtually impossible to eliminate all risk (except as discussed under *risk avoidance*). This risk is termed "residual risk." One example of *risk acceptance* is the setting of shrinkage tolerance levels in the retail industry. In addition, some organizations have established a formal process for risk acceptance. For example, the US Department of Defense requires a "Designated Approval Authority" to sign a document indicating that they accept the residual risk in IT systems under their jurisdiction after they have reviewed the threat and protective measures in place. In fact, this is a recommendation as part of the IT System Accreditation Process across all US Government agencies[10].

Carefully considering the *five avenues to address risk* is an excellent exercise and can be very effective at helping SRM professionals and management – whether in the physical, logical or converged world - to think outside the box in terms of multiple approaches to protecting assets.

[10] "Accreditation is a process whereby a Designated Approval Authority (DAA) or other authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk." (National Institute of Standards and Technology, 2002, p D-1)

“The Four D’s”



This is a classic principle in the crime prevention community and applies equally well to almost any aspect of *assets protection* or Security Risk Management. It nicely complements its “cousin” concepts: *the five avenues to address risk* and *layered security* (defense in depth). The “Four D’s” are *deter*, *deny*, *detect* and *delay*. Under this concept, the first objective in protecting assets is to ***deter*** any type of attack or attempt by a potential adversary to cause harm.

The second objective is to ***deny*** the potential adversary access to the target (your asset). This is typically achieved through traditional access controls and other physical, personnel or technical security measures.

The next objective – should deterrence and denial fail in whole or part – is to ***detect*** the attack or situation. This can be done in a variety of ways, traditionally using surveillance and intrusion detection systems, human observation or even a management system which will immediately identify or flag shortages or inconsistencies (e.g., an inventory tracking system which reports out-of-tolerance conditions).

Finally, once an attack or attempt is in progress, we want to ***delay*** the perpetrators enough to either convince them to give up/terminate the attempt or to allow an appropriate security/law enforcement response to the scene.

Like the other foundational concepts, the Four D’s can be applied in a traditional security environment or in the logical security sense with respect to IT systems. Such tools as access controls, authentication, encryption, intrusion detection systems, anomaly reporting, firewalls, port management, and content filtering work together to support the concept of the Four D’s in the world of cyber security.

Layered Security (Defense in Depth)

A closely related concept is that of *layered security*, which is also known as *defense in depth.* Again, this principle applies across the board to physical, logical and converged environments. Defense in depth recognizes that a single protection measure is not adequate, and that a series of well-planned and complementary levels (or layers) of varying types of security measures comprise an effective *assets protection* scheme.

Another way to think about it (presented from a cybersecurity perspective) is that layered security is “…the idea is…that any single defense may be flawed…so a series of different defenses should each be used to cover the gaps in the others' protective capabilities. Firewalls, intrusion detection systems, malware scanners, integrity auditing procedures, and local storage encryption tools can each serve to protect your information technology resources in ways the others cannot.” (Perrin, 2008)

From a physical security perspective, layered security normally encompasses such elements as barriers, perimeters, locking systems, access control, electronic surveillance, safes, vaults, sensors and security officers. Tools which work to support efforts to deter, detect, delay and deny a threat actor attempting to access an asset.

In a more comprehensive sense, however, the concept can include personnel security, technical security, policies and procedures, security education, facility layout, traffic patterns and even – in the case of shopping centers for example - neighborhood watch programs.

In short, *assets protection* should involve a comprehensive strategy, not a combination of piecemeal elements (officers, CCTV, access control systems, etc.). Developing such strategies, particularly in today's complex global environment, requires both broad expertise and a very thorough thought process based on underlying concepts such as those described above.

Mitigation Measures

A comprehensive strategy incorporates all aspects of protective measures that are appropriate to the environment based on its mission, nature, physical attributes and risk assessment results. As mentioned, these should be viewed as part of *suite* of solutions. Among the families of measures to be considered are:

Physical Security (barriers, locks, access control, etc.)
Electronic Security Systems
Security Officers
Policy and Procedure/Business Practices
Security Awareness and Training
Facility and Campus Layout, Design and Architecture
CPTED (Crime Prevention Through Environmental Design)
Contracts and Clauses
Legal and Financial Posturing
Insurance
Information and Intangible Assets Protection
Cybersecurity
Personnel Security
Technical Surveillance Countermeasures
Business Continuity and Crisis Preparedness
Travel Security
Compliance Program (legal, regulatory and policy)
Liaison and Relationships
Healthy Management Environment

Generally, not all of these are under the purview of the Security Director or CSO. Thus SRM is clearly a multi-faceted function which requires varying degrees of coordination and collaboration. As the ASIS Chief Security Officer Guideline indicates, the ideal CSO is a strong negotiator, facilitator and consensus builder. Some of the other traits mentioned include “strategic orientation,” “conceptual thinker,” “a global perspective,” and “the ability to interact at all levels of the organization.”

Finally, there is no place for complacency in SRM. It involves a constant process of monitoring, evaluating and making/advising business decisions on necessary changes to the risk mitigation strategy and its components. This requires a formal mechanism to continually monitor assets, threats, vulnerabilities and protection measures, as well as organizational and environmental factors.

Changes may include increasing, decreasing or adjusting protection levels; and this can be accomplished by modifying technology, people’s duties, policy/procedures, staffing levels, program emphasis or other aspects of the overall program. Sometimes the risk management monitoring process will show how to save money by doing things smarter, better or more efficiently; or by not doing things that no longer make sense.

Sources Cited

ASIS (2020), Information and Intangible Assets Guideline, Draft, ASIS International, Alexandria, VA USA

ASIS (2019), Enterprise Security Risk Management Guideline, ASIS-ESRM-2019, ASIS International, Alexandria, VA USA

ASIS (2012), Protection of Assets, Security Management Volume, Chapter 4, Introduction to Assets Protection, pp 54-65, ASIS International, Alexandria, VA USA

ASIS International, Information Asset Protection Guideline, ASIS GDL IAP 05 2007

ASIS International (2004), Chief Security Officer Guideline, ASIS GDL CSO 06 2004

ASQ (2020), What is the plan-do-check-act (PDCA) cycle?   American Society for Quality, Milwaukee, WI USA, https://asq.org/quality-resources/pdca-cycle, accessed June 2020

Drucker, Peter F. (1970), Technology, Management & Society, p. 144, Harper and Row Publishers, New York, NY   USA

Garcia, Mary Lynn, CPP (2000), “Truth & Consequences,” *Security Management*, June 2000, pp. 44-48, ASIS International, Alexandria, VA USA

Gardner, Robert A., CPP, (1995), “Small Business: Reducing the Risk,” www.crimewise.com, accessed November 2010

National Infrastructure Protection Center (2002), “Risk Management: An Essential Guide to Protecting Critical Assets,” November 2002, Washington, DC USA

Peterson, Kevin E., CPP (2006), Principal Consultant, Innovative Protection Solutions LLC, unpublished material, Herndon, VA USA

Perrin, C. (2008), “Understanding layered security and defense in depth,” TechRepublic, Dec 18, 2008, www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth, accessed 2 Jan 2021

Winkler, Ira (2005), Spies Among Us,” Wiley Publishing, Indianapolis, IN USA

Winkler, Ira (1997), Corporate Espionage, Prima Publishing, Rocklin, CA USA