**The Risk Assessment Process for Cultural Properties**

By: Brian Gouin

Risk is defined by Webster as the possibility that something bad or unpleasant will happen. We assess risk all the time in our daily lives: Is driving this fast worth it? Do I cross the street here? Do I invest in that stock? Assessing risk is also big business; insurance companies are built on understanding and reducing risk. Large corporations have Risk Managers and Risk Management Departments dedicated to decreasing the possibility that an adverse event will occur. Similarly, the main functions of a Security Director and Security Department are to assess and manage risk.

The Risk Assessment Process as it relates to security is the analysis of assets, threats, and vulnerabilities. Risk is based on the relationship of those three factors and can be expressed either qualitatively or quantitatively. A risk assessment is the process of identifying and prioritizing risks for the purpose of mitigating those risks. Risk can rarely be eliminated, but reasonable steps can be taken to mitigate risk. This risk assessment process is the same regardless of the type, size, or location of an organization or facility. However, there are elements of the analysis of assets, threats, and vulnerabilities that are unique to Cultural Properties.

Step 1: Assets

The first step in the risk assessment process is to identify all the assets in a facility and assign a level of criticality to each asset. Without asset identification, security measures would be arbitrarily selected and deployed. Assets need to be known to be protected. Assets fall into three categories: people, property, and information. People include employees, visitors, patrons, contractors, and etcetera. Property comprises both tangible items such as the building and everything within it and intangible things such as reputation and competitive advantage. Information covers such things as databases, financial records, and proprietary records.

Performing the required interviews and site survey to identify all the assets within a facility begins in the same way for a Cultural Property as any other facility. The difference emerges with the assignment of criticality for those assets, particularly property assets. Critical assets are those which are more important for an organization to execute its primary missions and functions than others. It should be noted that as with all other facilities, people are the most critical asset in a Cultural Property. The criticality of individual property and information assets should also be carefully established.

As an example, the formula for Coca Cola is an extremely critical asset. If it were to be stolen and published, the company's competitive advantage would be compromised and it would financially suffer, perhaps catastrophically. Comparatively, even a full warehouse of soda being stolen or destroyed may have some financial consequence but does not stop the company from

operating. The product can be replaced easily and insurance coverage exists to cover product replacement costs so the criticality is relatively low.

Because a main element of a Cultural Property is to preserve the records, artifacts, art, and language of our nation for future generations to enjoy and understand, objects within these facilities are much more critical than general inventory within other types of facilities. This property can never be replaced. Should one of these assets be lost, damaged, or destroyed, not only is that item gone forever but there are also major consequences to other assets such as the reputation and competitive advantage of the institution. Therefore, a Cultural Property will generally assign a higher criticality level to interior property assets than most facilities, and is some cases like historical sites the buildings themselves.

Step 2: Threats

The second step in the risk assessment process is to identify all the threats to the identified assets and perform a threat assessment. There are two main categories of threats: human and natural. Human threats can come internally from within an organization, externally, or a combination of both. The threat can be intentional or unintentional. Natural threats are mostly natural disasters. Unfortunately, there is a wide spectrum of threats to Cultural Properties simply because of their profile. Some threats such as natural threats are the same as for any other institution, although fire is one of the most serious threats overall to Cultural Properties because of its potential for complete destruction.

Some of the human threats are also common to most organizations. These include disgruntled employees or former employees, small time criminals, people with domestic disputes, and those under the influence of drugs or alcohol. However, Cultural Properties have additional global threats reserved for high value targets. Theft from employees, visitors, or armed intruders is a major threat because of the high value of the assets and for political or social reasons. Terrorism is also a threat for similar political or social reasons, a real or perceived connection to government, or simply because a large number of people assemble at the institution. Cultural Property security analysts must consider this wider variety of threats when analyzing risk.

Once all the threats have been identified, the assets that can be targeted by the defined threats also need to be identified. Not all assets are targets for every threat and some assets are targets from multiple threats. The likelihood that as asset will be targeted is based on the severity of the threat. It takes a specific expertise to analyze all the threat data and make the determination as to the severity of a threat to compromise an asset. Some of this is common sense, but further review requires examining historical information and crime statistics. There are companies that have been formed exclusively to analyze crime data as well as evaluate inherent threats in order to make these assessments.

A threat assessment evaluates the effect of any compromise of an asset from a threat for the purpose of ranking the severity of all the threats to all the assets. It is the analysis of the

relationship between the likelihood that an asset will be targeted by the threat versus the criticality of that asset. This relationship can be presented either qualitatively or quantitatively.

Below is an example of a qualitative analysis presentation. The assets in this case are library books in a storage facility and the threat is internal theft. The X axis is asset criticality and the Y axis is threat likelihood. A very basic rating scale of low, medium low, medium, medium high, and high is used. The fields are color coded for comparison purposes. In this example, the threat likelihood is medium low and the asset criticality is medium. The proper box is marked and the threat to the asset is analyzed graphically. Such an analysis should be performed for every threat to every asset and compared. It is important to remember that every asset does not necessarily mean every individual painting or every book in the building but may mean all paintings or books in a room or on a floor depending on the layout.

Qualitative Analysis

Threat Likelihood – Internal Theft

| | L | ML | M | MH | H |
|---|---|---|---|---|---|
| H | | | | | |
| MH | | | | | |
| M | | | | | |
| ML | | | X | | |
| L | | | | | |

Asset Criticality – Library Books

Below is an example of a quantitative analysis presentation. The rating scale of low, medium low, medium, medium high, and high is instead represented numerically as 1 through 5. The numbers are added together and compared to the total number of potential points in order to determine a simple percent. Again, such as analysis should be performed for every threat to every asset and compared.

Quantitative Analysis

1. Threat likelihood from internal theft = 2
2. Asset criticality of library books in storage facility = 3
3. Threat Assessment of Internal Theft of Library Books in a Storage Facility: 3 + 2 = 5 on a scale from 2 to 10 = 44%

It should be noted that both of these presentations are rudimentary and are shown to illustrate the concepts. In some cases both cultural property institutions and security consultants specializing in risk assessments use more complicated charts and formulas to display these relationships.

Step 3: Vulnerabilities

The third step in the risk assessment process is to identify all the current security measures, identify the vulnerabilities to the assets, and perform a vulnerability assessment. In simple terms, the goal of a vulnerability assessment it is to identify weaknesses in the current security program. Inventorying the existing security measures is commonly called a security survey and is accomplished through interviews, review of security procedures and other documentation, a site visit, and review. To be accurate and complete, the security survey should be inclusive of policies & procedures including training and emergency preparedness, physical security including accessibility and electronic measures, and personnel including actions and post orders.

The vulnerability assessment is a similar process to the threat assessment in step two. Once all the current security measures have been identified, a rating is assigned to the vulnerability of each identified asset. Once more, specific expertise is required to determine the effectiveness of the current security measures in order to establish a vulnerability rating for each asset. Cultural Property experience is even more of a necessity when making these determinations, perhaps even experience within the specific type of Cultural Property. Determining vulnerabilities in such places as reading rooms and collection sites are more difficult than the average facility because particular knowledge is required about the rules and operation of such areas and the normal behaviors of patrons and staff.

A vulnerability assessment compares the existing security measures against the identified assets to determine the effectiveness of the current security measures in protecting the assets. It is the analysis of the relationship between the vulnerability and criticality of each asset. The same asset criticality is used for both the threat and vulnerability assessments. As with the threat assessment this relationship can be presented either qualitatively or quantitatively. Below is an example of each using the same assets of library books in a storage facility and threat as internal theft. In these examples, the vulnerability rating is medium high or a 4 and the asset criticality is medium or a 3.

Qualitative Analysis

Vulnerability Rating – Library Books

| | L | ML | M | MH | H |
|---|---|---|---|---|---|
| H | | | | | |
| MH | | | X | | |
| M | | | | | |
| ML | | | | | |
| L | | | | | |

Asset Criticality – Library Books

Quantitative Analysis

1. Vulnerability rating of library books in storage facility = 4
2. Asset criticality of library books in storage facility = 3
3. Vulnerability Assessment of Effectiveness of Current Security Measures: 4 + 3 = 7 on a scale from 2 to 10 = 67%

Step 4: Risk Assessment

With the first three steps of the risk assessment process complete, the data needs to be analyzed together to evaluate risk. Risk is the relationship between assets, threats, and vulnerabilities.

**R = A + T + V**

A Risk Assessment is the process of identifying and prioritizing risks with the goal of reasonably mitigating those risks. The risk to one asset may not be the same as the risk to another asset. Each asset (or group of assets) needs to be evaluated individually. There may also be more than one threat to each asset that needs to be evaluated individually based on varying vulnerabilities. To make this evaluation, an analysis is performed of the relationship between the threat assessment and vulnerability assessment. The asset criticality was already taken into account in both the threat and vulnerability assessments so it is not included in this final step.

As with the threat and vulnerability assessments, this relationship can be expressed qualitatively or quantitatively. Below is an example using the ratings from our previous examples. For the qualitative risk assessment, there are various methods that can be used to determine what the ratings should be based on what was expressed graphically. Depending on how complicated the model, anything from assigning numbers to each box and doing the math to drawing sensible conclusions can be used. For the quantitative assessment, the threat assessment and vulnerability assessment numbers are added and compared to the total number of potential points.

Qualitative Risk Assessment – Internal Theft of Library Books in Storage Facility

Threat Assessment – Internal Theft

| | L | ML | M | MH | H |
|---|---|---|---|---|---|
| H | | | | | |
| MH | | | | | |
| M | | | | | |
| ML | | | | X | |
| L | | | | | |

Vulnerability Assessment – Effectiveness of Current Security Measures

Quantitative Risk Assessment – Internal Theft of Library Books in Storage Facility

1. Threat Assessment from Internal Theft = 5 on a scale from 2 to 10 = 44%
2. Vulnerability Assessment of Effectiveness of Current Security Measures = 7 on a scale from 2 to 10 = 67%
3. Risk Assessment of Internal Theft of Library Books in a Storage Facility = 12 on a scale from 4 to 20 = 53%

Once this analysis is completed for every threat to every asset (or group of assets), the results can be ranked either qualitatively or quantitatively to prioritize the severity of the risks. Why do this at all? As with many industries, Cultural Properties have limited budgets and only so much money to work with. It is sometimes difficult to quantify the Return on Investment (ROI) for the Security Department budget because it is seen as an expense only. A well thought out Risk Assessment can help define that ROI and logically determine where available funds should be spent.

Recommendations should be developed for improvements to existing security measures based on the vulnerability assessment and each should include a cost estimate. These recommendations must also be inclusive of all parts of the security program: physical security, policies & procedures, and personnel. Then, a cost benefit analysis should be conducted to compare the cost of the risk mitigation recommendations to the risk rating in order to determine the benefit. Only then is the Risk Assessment complete. From this analysis, decision makers can decide the desired type and degree of risk mitigation strategies to be employed.

Cultural Properties hold such an important place in our society. Protecting them and their contents is equally as important. Security professionals must determine what security measures are best to mitigate the risk for their particular institution. By performing a professional and complete Risk Assessment, the institution can ensure that precious budget dollars are allocated to the most effective security protection for the irreplaceable assets entrusted to its care.

*Brian Gouin is a Senior Security Consultant at Nationwide Security Corporation in Branford CT. Brian has worked in the security industry for over 30 years as both an integrator and independent security consultant. He is the author of two security related books and has contributed articles and chapters to many other security and business publications. He is a member of ASIS, the IFCPP, the NFPA, and is a former Director of the IAPSC. Brian can be reached at briang@nationwidesecuritycorp.com.*