Risk Assessment Approaches for the Reopening of Cultural and Heritage Venues

by Andy Davis, CPP
30 March 2021

Slowly, global cultural and heritage sites are starting to reopen to the public. As part of that reopening process, it is important for those responsible for securing artifacts, visitors, and venues to ensure that their security risk management approach remains viable. The cultural and heritage sectors have been severely impacted by forced closures and loss of revenue; not all are centrally funded, and some, unfortunately, have been forced to close for good.
In the Q&A below, Andy Davis, CPP, chair of the ASIS Cultural Properties Community and owner of Trident Manor Limited, discusses security risk management approaches that professionals in the global cultural and heritage sectors may consider as their facilities reopen.

Many museums and cultural sites were forced to close in 2020 for significant periods of time, in compliance with COVID-19 restrictions. As they reopen, is it simply a case of ensuring that their earlier approaches to risk management are still fit for purpose?

To some extent, yes, but unfortunately that would only provide half of the solution. While many of the internal and external threats to these sites and facilities remain the same, the social environment in which the world is operating has changed irreversibly—at least in the short to medium term. The context in which the previous assessments were—or should have been—undertaken is different. Therefore, the threats that are faced and the risks they pose by default have also changed.

Could you provide some examples of how those threats and risks have changed?

The most obvious example is the COVID-19 threat that has had a global impact. It has impacted our approaches to personal safety, operational activities, and freedom of movement. Any reopening strategy must assess the risks that COVID-19 brings and identify strategies to minimize them. This means looking beyond the obvious health risks. Is there a decreased risk by having fewer people in the venue? Is there an increased risk of confrontation if someone refuses to wear a mask?

Other examples include protests in some countries caused by colonial exploits—like Black Lives Matter protests—primarily in European nations and the United States; conflicts in Ethiopia; political upheaval in Myanmar; the port explosion in Beirut; and many more localized incidents and events. These would not have been part of earlier assessments or evaluations, so it is important to remember the constant threats such as crime, violence, and terrorism that exist but also how to reassess them alongside new or emerging ones to ensure your protective approach is robust.

How do you recommend beginning the risk assessment process in 2021?

Interestingly, you should not start anywhere physically near the venue being assessed. This is because it is important to understand the organization, its culture, approach to risk, and resources available before starting on the assessment. This establishes the context for the assessment, as recommended in the **ASIS Standards on Risk Assessments** and **ISO 31000**.

Another action that I always take prior to visiting any site is to conduct research. This includes researching local crime statistics, the social fabric of the area, evidence of urban decay or regeneration, and media items that paint a picture of what is happening at and around the venue. By doing this, I start to form a multidimensional understanding of some of the potential threats and opportunities that exist.

Normally, I would also start a risk rating table to capture the threats as I perceive them and initiate an indicative risk scoring process considering the likelihood—and consequences and impact—of the threat occurring. One tip I recommend is to identify and record specific threats. Just having the threat of crime (a general threat) on the table makes it difficult to accurately assess without looking at more specific threats (i.e. robbery, fraud, pickpockets). It is more work, but it creates an accurate understanding of the risks posed.

There are advantages and disadvantages if this process is undertaken in-house where there is already knowledge and familiarity with the site, but there is also a greater likelihood of acceptance of the findings. Equally, an external reviewer is able to undertake an independent review but may not have an in-depth organizational understanding—which could have ramifications for the assessment's findings.

This seems like a lot of work to undertake before getting onsite.

It is, but it is no different to building a house without foundations—the structure may appear solid but weaknesses may be hidden or unconsidered. By using a thorough and rigorous approach before arrival, there are more opportunities to adopt a lateral thought process and reduce the likelihood of missing vulnerabilities.

Is there a set way to undertake assessments once onsite?

Others may disagree, but I think the important thing is to adopt a methodical approach. I start from the outside and work my way inwards. This enables me to adopt an **adversarial mind-set** where I am looking for vulnerabilities to exploit or identify effective protective layers, examples include windows being left open, poor access control practices, and likely police response times. I teach students attending programs at the Trident Manor Training Academy that the easiest way to adopt an adversarial mind-set is to "think like a criminal" or "think like a terrorist." It is amazing some of the attack methodologies students have considered. This approach means that when vulnerabilities are identified, I can then switch mind-sets to that of a protector and consider ways of negating the vulnerabilities—as far as practicable. I would adopt this approach throughout the whole building, front of house, back of house, basement areas, and—if accessible—the roof.

As part of this methodical approach, seek to ensure that security in depth is achieved through interlocking security measures. This is coined the POT-E approach, which identifies all security

measures that fall within physical, operational, technical, or educational measures. Therefore it should be possible to address security weaknesses by applying one or more of these measures. The more layers of protection that are applied, the better security is afforded, and vulnerabilities are reduced.

One thing I recommend assessors do when visiting sites is to visually document their findings and observations. Not only is a picture worth a thousand words in any report, but it prevents written notes from being misinterpreted and allows for a speedier assessment—which from a client's perspective saves money.

What do you mean by POT-E measures?

Physical measures would include fences, doors, windows, skylights, display cases, etc. A window is a physical barrier preventing someone from outside getting into the premise. Its effectiveness as a security feature will depend on its positioning, accessibility, frame fabric, type of glazing, and locking mechanism. If standard (non-security) glass is used, then it would be vulnerable to a direct force attack. You would want to seek ways of enhancing the protection or accept the risk associated with the window.

Technical measures have a primary function of notifying someone of an event that is occurring (alarms, search arches) or of supporting and assisting operational activities (video surveillance, cloaking devices). Some people wrongfully believe that technical systems are a preventative tool. They are not because they normally only notify and enable a response to an incident—effectiveness of that response is another matter.

If you look at technical applications in the context of the window above, you might consider installing a sensor to notify security if the window is broken or someone gains entry through it. To further improve technical effectiveness, you might install a camera system to watch and monitor the window and surrounding space.

Operational measures are those policies, practices, and procedures that are implemented as a part of protective measures. For example, these measures could include ensuring the window is locked at night and the alarm system is set to notify someone if it is breached.

Finally, education is an often-forgotten security measure—in many cases it is not even recognized as such by practitioners. Education, whether training, providing guidance, or increasing awareness, is the glue that holds all the other security measures together. If staff are not educated about the threats that exist at a venue, how can they be expected to proactively reduce the risk exposure? If staff are not trained on actions and activities they are expected to take, how can we blame them if mistakes are made in procedures?

Using the example of the window again, staff need to understand the threats that could impact it. For instance, tell staff if burglaries of business premises are high near the venue and that the window might be used as a point of entry into the premises for thefts to occur. Remind staff that it is important to lock the window to make entry more difficult, and upon vacating the premises the alarm must be set to ensure a police or security response. Staff should also be instructed on how to set the alarm and unset it in the morning.

The window explanation shows how education impacts physical, technical, and operational practices. An organization should never assume that someone will act in a certain way. If it fails to share and inform staff about what is expected of them, it is increasing its operational and organizational risk.

Having reviewed all threats, risks, and vulnerabilities, what is the next stage of the assessment?

I would return to the risk rating table and review the original assessments, followed by identifying suitable risk reduction strategies and then reevaluating the threats and risks they posed. This final risk rating can then be measured against a prioritization list for risk reduction implementations and highlighted, where necessary, within a report.

I also encourage writing a detailed report, documenting findings in a structured and logical manner that recipients can follow. I normally start the report with an executive summary, followed by a findings section with recommendations, a conclusion, and an appendix. Within the findings, I recommend documenting physical, followed by technical, operational, and educational weaknesses—starting externally, then from the lowest floor up to the highest floor or roof. Within the appendix, include evaluation descriptors (so readers understand how things have been measured), a completed risk rating table, a composite list of all recommendations, and additional imagery—if necessary.

Sometimes it is important to present findings to senior managers, especially when financial decisions exist around capital or operational expenditure.

Is this the end of the process? Or are there additional steps you recommend?
It is the end of a stage, but not the end of the process. The risks that have been identified need to be addressed, transferred, or accepted. The risk assessment process should be contentious and under regular review either periodically or after a significant event. It is only by undertaking this continuous review that risks are proactively identified and reduced that prevent loss and damage to property while reducing the likelihood of harm to visitors or staff.

What are some of the primary risks cultural properties and heritage sites face when they reopen?
In the short term, operational risks caused by the COVID-19 virus will be the most impactive risk they face. COVID-19 has not gone away, but new practices have been implemented to ensure venues can open safely. As with anything new, however, mistakes are more likely because of the change, and this may lead to insufficient staff being on duty to correctly oversee processes or shortcuts to be taken in safe operational practices.

An added risk is the fact that some people still believe COVID-19 is a hoax, so they refuse to wear masks or follow instructions designed to keep others safe. This has the potential to create conflict, complaints, and reputational damage.

Policies and procedures should be established so there is absolute clarity about organizational expectations and individual responsibilities. The most important thing is to educate staff and provide training, support, and encouragement.