PROTECTING ART COLLECTIONS: A STRATEGIC APPROACH

Inspector Richard Roberts
Australian Protective Service, ACT

Paper presented at the Art Crime
Protecting Art, Protecting Artists and Protecting Consumers Conference
convened by the Australian Institute of Criminology
and held in Sydney, 2-3 December 1999

Introduction

As we've heard over the past two days, the threats to art collections are quite real and substantial. So I'm pleased to have been invited to speak here today about how at least some of those threats can be defended against. I'm fortunate to have been privy to the security strategies of a large, diverse range of both public and private sector organisations, including those of Australia's major art museums. So it feels good to be able to offer the benefit of that experience to an obviously receptive audience.

The aim of my presentation today is two-fold. Firstly, to provide a broad appreciation of a strategic approach to security risk management - one that not only effectively addresses security risks, but also makes security compatible with broader corporate goals and concerns. To do this I'll talk briefly about the importance of an effective security risk management plan and its key features. It's also worth noting that the framework I'll discuss is equally effective in managing fraud risks, and is essentially the same as the approach outlined in the draft Commonwealth Fraud Control Policy.

Secondly, I'll share some examples from my experience about how, despite the best of intentions, organisations unwittingly leave themselves exposed to serious risks. I won't however identify the organisations or even industries to which these examples relate, to maintain their confidentiality. So, if you're a client of the APS here today, relax! However, I can assure you all that the examples, and the lessons to be learnt from them, are as relevant to art museums as they are to other organisations.

The Security Risk Management Plan

A Security Risk Management Plan is a series of activities that, together, provide a logical, considered and comprehensive approach to the management of security risks, in a way that is consistent with broader organisational activities, and that adds value to the organisation by helping achieve its broader goals.

Such a plan comprises five key elements. Firstly, a security risk review, which identifies the risks faced, assets that need protection (based on the consequences of harm to them), vulnerabilities in existing security arrangements, and options to address those gaps, again in a manner consistent with broader objectives, concerns and constraints. To provide a sound basis for the following steps in the plan, and to gain high level commitment for it, it's essential that the review is, and is perceived by stakeholders to be, competently conducted and objective, and that it provides a clear, compelling rationale for its findings and recommendations.

The subsequent steps in the plan then consist of security policy, security procedures, security awareness and training activities, and a regular review, testing and audit mechanism. Together, these five elements ensure that risks are reliably identified, along with any changes in them, and that security arrangements therefore remain adequate.

Security policy and procedures

Once the risk review findings and recommendations are accepted, then security policy should be developed. This policy is clear, documented statements of intent on how security risks are to be managed, and the aims and commitment of the organisation in doing so. Then security procedures should be developed, consisting of clearly defined activities to be conducted to meet security policy objectives. There are many issues to be considered when developing and implementing policy and procedures, and I'll touch on just a few of them shortly.

Security training and awareness activities

Regular training and awareness activities are essential to the maintenance of an effective security risk management plan. There's little value in conducting a risk review and knowing what your problems are, and having procedures in place to deal with them, if staff are unaware of the risks faced, or lack the skills to meet their obligations. All too often, security induction briefings and training activities are far too brief or ad hoc to properly reinforce the importance of security, the organisation's commitment to it, and to provide meaningful knowledge and skills to staff. In several recent cases, I have seen security induction allocated just ten minutes in a week-long induction program. Not surprisingly, the security knowledge and skills of staff, and their commitment to security, were insufficient to effectively manage the risks faced.

Regular review, testing and auditing

A security risk management plan is a living document; one that must be regularly reviewed, and tested, to ensure it remains effective and remains consistent with the broader goals and concerns of the organisation. Testing of security arrangements should be an integral part of the plan, to ensure its effectiveness before a real threat does so, and perhaps finds it lacking. Even simple measures such as practical exercises, along the lines of fire drills, desk-top 'what if' exercises, newsletter articles and screen-saver messages, are invaluable in testing procedures, refreshing skills, building confidence and keeping commitment and awareness levels high.

SOME COMMON FINDINGS

Little or no systematic risk review

I find that organisations generally have a reasonable appreciation of the risks they face, but that many have never conducted any structured, in-depth analysis of those risks. Consequently, the importance and vulnerability of some key assets is often not fully appreciated or at least clearly and formally enunciated. Sensitive information and corporate reputation are prime examples in this regard. The formal articulation of security risk is particularly important when you consider that funding for security is sometimes a contentious issue, and usually contingent upon convincing executive management of the need to commit resources to it, and perhaps even modify the way business is conducted.

Underestimation of risk

Perhaps the biggest mistake often made is the assumption that a lack of security incidents to date means there is no threat, or that security measures must be adequate simply because a risk hasn't occurred.

One of the greatest threats to security is the belief that there is no threat. When I say this I'm reminded of an explosives facility I once visited it was happily located between a prison and a match factory! However, after the last two days, I'm sure everyone here has no doubt about the threats the art world faces.

Another concern I often see is the likelihood of a risk being overly emphasised, rather than the consequences. While likelihood is a valid consideration, giving proper, serious consideration to the consequences as well can be a sobering experience, and one that leads to prudence in the acceptance of the likelihood of a risk eventuating.

Vulnerabilities not recognised

The prevalence of unrecognised risk exposure and vulnerability to serious security risks within many organisations is often quite alarming. Here are some examples, from substantial organisations with major assets.

One organisation shared contract guards as the result of local government outsourcing. When I reviewed the guards' written procedures, it was evident that the guarding company did not allow its guards to physically touch wrongdoers, including those committing acts such as malicious damage, theft and robbery. The guards were only to verbally direct the culprits to stop and call the police. This was certainly not satisfactory to the client when they heard about it for the first time from me, after the guards had been in place for several months.

In another case, an elderly guard was locked alone inside a building after hours to monitor alarms and respond to threats. He had this job because he had heart problems and wasn't well enough to perform other guard duties. His inability to provide an effective response to threats had not been recognised, and neither had the risk to him personally given his ill health.

Inadequate resources

Quite often, corporate commitment to security in not borne out in financial commitment to security risk management, or support for security measures that are funded. For example, broad, impressive commitments to security are made in corporate plans and policies, but insufficient resources are then allocated to make them realities.

One way this frequently occurs is the inadequate human resourcing of security management. For example, security managers often have more that just security responsibilities, and security is often obliged to take lesser priority due to more urgent, but less important matters such air conditioning and cleaning problems.

As a result, many security functions, particularly those that add real long-term value and effectiveness to security risk management plans, such as risk monitoring, systems testing, policy and procedures development, training and awareness, are often never gotten around to. Although multi-tasking is a fact of life in today's corporate world, should it be at the expense of good security?

Policy and procedures poorly documented

Typical examples in this respect include unclear or inadequate assignment of responsibility for security tasks. Another concern is the lack of incident-specific procedures - ones providing detailed guidance on dealing with specific events such as bomb threat, protest, malicious damage, theft and robbery for example. Often, procedures are too broad and generic. They don't provide sufficient direction to ensure a decisive, coordinated and effective approach is taken. Also, they may lead to people getting involved in situations they should stay out of, and putting themselves and others at serious risk.

The last concern I'll mention is outdated policy and procedures. In a review I just completed procedures directed that in the event of a bomb threat either the APS or local police should be called. Sound advice when it was written. However, a few years ago the APS discontinued this service in the local area after it was agreed the local police should be the sole provider. To compound matters, the police phone number in the procedures was so old it is now disconnected.

I also found that the person nominated in the procedures to assess and manage bomb threat incidents was surprised to hear it was them, and said they had no expertise in the function.

Summary and conclusion

The substantial financial, artistic and cultural value of many works of art, and their often unique, irreplaceable nature, justify substantial measures to protect them. But in today's tough business world, that protection must compete with other demands on finite resources. So, for adequate security to be provided, and for it to be considered an integral, positive part of good management, it must be based on risk management principles and take into account broader concerns and objectives.

The approach I've outlined today enables this to happen, and contributes to the relevance, perceived value and acceptance of security strategies. The examples of unrecognised vulnerabilities provided will, I hope, reinforce for you how serious risk exposure can go unnoticed and pose a serious threat to organisations. And I hope that my talk today has also reinforced with you the value of an effective security risk management program.

QUERIES - Follow-up queries in relation to this presentation are welcome, and should be directed to Inspector Richard Roberts on 02 6270 2686.