

Joe Traynor
Collections Officer
West Dunbartonshire Council
Education and Cultural Services
Levenford House
Helenslee Road
Dumbarton
G82 4AH
Scotland
25th July 2007

31 JUL 2007

Our Ref: UK2306

Dear Mr Traynor

RE: Security Inspection – Clydebank Museum, Clydebank

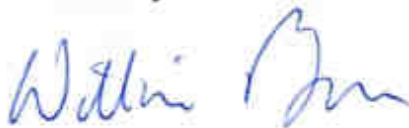
I have to thank you on behalf of John O'Brien for Janette McPhail's friendly reception on his visit to Clydebank Museum on Friday 22 June 2007. Together they reviewed the Museum building with its overall security in mind and whether your Museum could meet the general conditions for Government Indemnity. I understand that Mr O'Brien has discussed his visit with you on the telephone and I have much pleasure in enclosing his report for your information and action as necessary.

I have to advise you that although your museum has had a crime free existence for years, certain weaknesses have been identified in your protection levels and this could invite unwelcome attention. You will be aware conditions of loan under the Government Indemnity Scheme are that the gallery must be hardened to a level rendering illegal entry nigh impossible and that there must be 'continuous' invigilation, requiring staff to be on the premises during the exhibition.

Mr O'Brien has discussed with you the recommendations contained in his report. I understand that the museum is closing in July for refurbishment/re-organisation and this may be an opportune time to implement the recommendations contained in his report, which will allow me to approve loans from nationals under the Government Indemnity Scheme.

Please advise me whether these recommendations can be put in place. If you have any further queries on this matter, please do not hesitate to contact me.

Yours sincerely



William Brown
National Security Adviser

O'BRIEN SECURITY CONSULTANCY

CLYDEBANK MUSEUM
Clydebank Town Hall
Dumbarton Road
Clydebank
G81 1UE
Scotland

File Ref No: UK 2306

PART ONE: INTRODUCTION

1 Background

- 1.1 Clydebank Museum was visited on Friday 22 June 2007 at the request of the National Museums of Scotland in connection with the proposed loan of clothes for a Victorian Exhibition scheduled for August 2007 to January 2008.
- 1.2 During the visit Janette McPhail, Acting Museum Supervisor, briefed and provided the tour of the museum, which is located on the ground floor of the Clydebank Town Hall

2 Threat of Criminal Activity

- 2.1 The experience gained over many years of the type and methods used in criminal activity against museums and galleries has been used to determine the measures needed to protect this venue.
- 2.2 With such institutions the attention of the criminal is drawn by publicity to the material on display and every opportunity is afforded him to make his reconnaissance. During open hours this can lead to a smash and grab type of attack, but more often advantage is taken of inadequate protection arrangements to lever open display cases or remove from open displays.
- 2.3 During closed hours it is now not uncommon for the criminal having recognised the existence of an intruder detection system and with the prior knowledge gained of the precise whereabouts of the items he seeks and physical security weaknesses, to make a rapid attack and then escape with the proceeds well before police attend in response to the alarm system. Increasingly these attacks are taking place through upper floors and roofs following the improvements made over the years to the physical protection of museums at the lower levels.

3 Level of Threat

- 3.1 The determination of the potential level of threat is very much influenced by the attractiveness and value of the collection, although the nature of the venue's surroundings and any history of crime or incidents can play a part.

- 3.2 At the same time it should be noted there is every indication that where appropriate security measures are taken the risk to collections is considerably reduced.
- 3.3 Apart from fire – a significant hazard – the existing hazards are assessed to be vandalism, plus daytime attempts to steal from the galleries and by nighttime, a professional burglary. The museum gave every appearance of being a well organized and managed establishment.

4 Risk Assessment

- 4.1 In assessing risk account has been taken (as relevant) of:
- Any external perimeter including fences, walls, gates and any other means of access
 - The shell of the building and its apertures
 - Zoned areas (including temporary exhibition galleries and stores), internal doors and any need for access control
 - Any presence of security staff for 24-hours
 - Any staff in residence
 - The requirements for an intruder detection system
 - The need for an automatic fire detection system
 - How CCTV can be applied effectively
 - How security lighting might be used
 - The method of display
 - Invigilation levels
 - Arrangements for key management and operating procedures
 - The impact of commercial functions or any mixed use of the venue

5 Conclusion

- 5.1 Given the past crime-free history, as long as Clydebank Museum restricts its collections as now, the threat to the museum itself, is rated LOW/MEDIUM – but it would rise with the introduction of any substantially attractive and portable exhibitions.
- 5.2 Risks can be reduced considerably by
- Examining the use of the doors into the galleries off the main corridor. One is required for entry and another for emergency exit from the Trade & Industry Gallery. The others should be kept locked and the door for use in an emergency fitted with an electronic lock capable of releasing on fire
 - Reconfiguring the building's intruder detection system so that when the museum is closed and the Town Hall open, the museum (Zone) can be kept in a secure alarmed state
 - Installation of a personal attack button (pab) at the reception desk and/or portable pab to be carried
- 5.3 This venue is currently not suitable for GIS loans. However the alternative measures suggested involving the strengthening of the galleries, surrounded by an effective intruder detection system (IDS), coupled with invigilation during any exhibition would enable most low value loans to be approved. The exception would be exceptionally high value, portable loans, when the situation would require to be reviewed.

PART TWO: RECOMMENDATIONS

6 Countering the Threat

- 6.1 Recommendations are made in response to the identified risks and in the context of the advice given in the MLA publication *Security in Museums, Archives and Libraries* and other guidelines to be found on the MLA website at www.collectionslink.org.uk. In making these recommendations every effort has been made to provide cost effective physical measures consistent as far as possible to the surrounds, with relevant technology in support. Where inhibited by the type of measures that can be taken compensation has been sought elsewhere in the security equation.

7 Physical Security

- 7.1 The provision of good physical security is the cornerstone of MLA's security policy. It can often prevent a crime taking place, but if not can still delay the criminal pending a police response to the intruder detection system.
- 7.2 There is no one source for standards for physical security products, but the following are useful:
- BS 3621 for locks
 - BS EN 1303 (Grade 4 or 5) for lock cylinders
 - BS 5544 for anti bandit glazing
 - LPC 1175 for building products
 - BS 5454 that includes security standards for archive

8 Display Cases

- 8.1 Display cases are the last line of defence for exhibits, but they are often also needed to provide a controlled microenvironment. Varying degrees of protection can be provided, from that designed to reduce the risk of accidental damage through to protection for small, attractive or fragile objects that need to be housed in strong, attack-resisting cases. If a case is sufficiently robust to resist attack it can compensate to a degree for limitations in another element of security provision e.g. the availability of attendants.
- 8.2 When considering the security qualities of a display case the four main elements to consider are: the lock, hinges, the framing, and the glazing. The locks need to be of a good standard and resistant to picking and direct physical attack, which is more easily achieved if they are hidden from view. The hinges need to be of a similar standard, being well secured to the case, whilst construction of the frame should be such that an attack will not affect the overall integrity of the case. Glazing needs to be laminated and set well into the frame. More detailed advice is available on the MLA website.

9 Intruder Detection System

- 9.1 An intruder detection system (IDS) that meets BS EN 50131 together with the Industry's Codes of Practice for Security Systems and is connected to an alarm receiving centre over a monitored line (e.g. BT RedCare) is required to initiate a police response. Where telephone lines are vulnerable to attack and high risk is involved a dual signalling system is needed (e.g. BT RedCare GSM).
- 9.2 In view of the high number of false calls to the police the Association of Chief Police Officers (ACPO) in England and Wales and ACPOS in Scotland have policies governing the response by police to these types of alarms. Detailed guidelines on this vitally important aspect are to be found on the MLA website.
- 9.3 It is MLA's policy not only to use an IDS in support of physical measures, but also to seek to have the earliest notification of attack. This is achieved by having detection on the perimeter of the building, which will entail, for example, the use of vibration and break glass detection on windows where environmental conditions permit. If this cannot be achieved then the system should be so arranged to detect at the earliest moment any intrusion into the protected space. Magnetic contacts are standard for external doors, but in the case of emergency exits it is usual to have them on 24 hours to detect unauthorised exit during open hours.
- 9.4 IDS should include at least one personal attack button (pab), which will normally be at the reception desk. Provision can also be made for portable radio pabs to be interfaced with the hardwired system.
- 9.5 There have been cases of detectors in museums and art galleries being masked during the day with a view to returning at night and affecting an undetected entry. Where this has happened substantial losses have been involved, as the criminal has been able to work undetected for a long period of time. From time to time detectors are also masked unintentionally by screens and other items. It is essential that when the premises are being closed for the night that detectors be checked for masking. This can usually be done by a walk test, which also raises staff awareness and actively monitors the efficiency of the system.

10 CCTV

- 10.1 CCTV is powerful crime prevention medium. Where there are valuable collections, especially if there are limitations on the number of invigilating staff available, it would be wrong not to invest in this proven method of crime prevention. At the same time it must not be seen a panacea to the threat of crime, but if the benefits are identified in the light of the advice in the guidelines to be found on the MLA website are properly applied the likelihood of crime taking will be reduced. A very modest black and white system covers only a few parts of the museum. The monitor is positioned by the reception desk and has no recording facilities
- 10.2 Though not a GIS requirement, a colour digital system is recommended, covering areas where the most valuable, portable or exposed objects are displayed. In addition a camera should be positioned in reception capturing head and shoulder images of visitors as they arrive.

11 Lighting

- 11.1 The use of security lighting can be a very cost effective deterrent. On balance activation by passive infra red (PIR) is preferred as it makes it more difficult for the intruder to adjust to the change in conditions, can draw others' attention and is more energy efficient. It can be particularly valuable in areas that are contained by walls or fences, as activations will be limited more to unlawful intruders than animals or passers-by. Care should be taken to put the lighting and detectors as far as possible out of reach.

12 Key Security

- 12.1 Only keys sufficient to enter should be taken from the premises. Internal keys need to be in a key safe or cabinet, which is out of general view and in a secure area. Keys are to be only issued to authorised persons and never to contractors or outside agencies.

13 Restricted Areas

- 13.1 Casual access by members of the public to the private areas during open hours can be prevented by the provision of digitally operated mechanical locks or more sophisticated electronic keypads, with or without entry cards.

14 Temporary Exhibition Area/Gallery and Government Indemnity

- 14.1 The intention to use the premises for loans from national institutions or under the Government Indemnity Scheme (GIS) dictate that certain security measures need to be taken - see MLA website for specific guidelines..
- 14.2 Taking account of the need for changing exhibitions, having determined the nature of the loans to be borrowed and the requirements under GIS, ideally the gallery should be hardened to a level rendering easy illegal entry nigh-impossible and capable also of being kept in a separate secure alarmed state while other parts of the building are in use.
- 14.3 Invigilation throughout the museum was discussed. It is required that any gallery containing a GIS loan be *continuously* invigilated. The receptionist on duty in the ground floor gallery deals with visitor enquiries; phones; administrative and shop duties, making it easier for the opportunist thief to commit crime when they are distracted on these other tasks. It is recommended that during these exhibitions another person is employed on invigilation duties backing up the receptionist, who is the only front of house person on duty. It is also recommended to investigate the use of Friends/Volunteers of the Museum as invigilators, as is the case elsewhere. Short written security orders to invigilators would be needed, specifying their duties, how they are to be relieved and on what objects to concentrate. Whether Clydebank Museum chooses to invigilate other areas is an internal matter: areas with exposed objects, unglazed pictures merit protection. CCTV will go some way towards solving the invigilation issue, but it should be remembered that CCTV is not a total substitute for an invigilator on the spot.

15 Stores

- 15.1 Stores often contain concentrations of material and can therefore present a higher risk dictating greater protection arrangements than might be appropriate elsewhere in the building. Arrangements therefore need to be made for them to be kept in a separate secure alarmed state while other parts of the building are in use

16 Fire Detection System

- 16.1 It can be argued that sometimes the threat from fire is greater than any other threat as even the smallest fire can generate large volumes of damaging smoke.
- 16.2 Clydebank Museum's system is adequate for purpose.

17 Environment and Access

- 17.1 For information in relation to general environmental management and any matters relating to access refer to the Museums & Galleries Commission Publications Backlist to be found on the MLA website. For any additional advice contact the local Area Museum Council.

18 Disaster Planning

- 18.1 The Museum, Record Office and Historic Properties Emergency Manual published jointly by the East Midlands Museum Service and the North West Museums Service provide a framework for the formulation of a disaster plan. Further advice is to be also in the MLA publication *Security in Museums Archives and Libraries*. For additional advice contact the local Area Museum Council.

19 Further Information

- 19.1 In addition to those mentioned above there are quite a few guides and specifications on other aspects to be found on the MLA website at www.collectionslink.org.uk.

20 Disclaimer

- 20.1 This report has been prepared to the best of the consultant's ability after reasonable enquiry, but may be relied upon on the understanding that the report contains matters of opinion and is based on the information provided by the client and depends upon the circumstances to which it relates having been fully disclosed to the consultant.


John O'Brien
Consultant Security Adviser to MLA

26 June 2007