THREATS
Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

"Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union''

Report No: DR/2.4/01

Best practices of health sector and EU hospitals for risk management and reduction against terrorist attacks and inter-organisational plans

Version: Final

Date: 3/02/2016

Authors: Ahmadreza Djalali, Pierluigi Ingrassia

Table of Contents

Executive Summary

In recent years, terrorist attacks have made the headlines on a regular basis; following the attacks in Paris (November 2015) the terrorism threat seems to be growing inside the European Union (EU). In 2008 the European Council issued a directive to a EU Member States (MS) to undertake measures for critical infrastructure protection (CIP). However, the results of Deliverable 2.1 (D2.1) showed the existence of gaps in EU health system preparedness with respect to terrorist attacks.

This report aims to identify best practices in resilience and preparedness of hospitals in response to direct terrorist attacks against the hospital facility. The research methodology includes a search of open source information using well-known public search engines and the analysis of data captured during the research phase of D2.1.

The literature review provided limited data relating to hospital resilience and preparedness to terrorist attacks but a group of articles have reported experiences of hospitals, both in and out of the EU, responding to mass casualty events where casualties have been injured during an attack elsewhere and the hospital has implemented emergency plans to deal with the immediate surge of victims. Other search results included various guidelines and recommendations for protecting infrastructures against terrorist attacks; one of the guidelines is health centre specific. Among the 49 EU hospitals that responded to the D2.1 questionnaire only three hospitals reported activity relating to resilience and preparedness in response to a direct terrorist attack.

Despite more than 100 terrorist attacks against hospitals since 1981 (Ganor and Wernli, 2013), and a perception that the terrorist threat seems to be increasing

within the EU, there is little evidence to indicate that hospitals have made sufficient efforts to improve resilience and preparedness for possible attacks. The publication of best practice in this field remains elusive, and only a few hospitals in the EU can be considered as examples of good practice. The current situation calls for an urgent revision of EU level strategy and action if EU hospitals are to improve resilience and implement an effective response to a direct attack against the hospital.

1. Introduction

Research conducted in D1.3 identified a decrease in terrorist attacks in the EU between 2009 and 2011, with a further reduction reported in 2013 (TE-SAT 2012:6). However, the attack at the Charlie Hebdo magazine in Paris and the coordinated attacks throughout Paris in November 2015, to cite two prominent examples, have ensured terrorism remains in the news headlines. The terrorist landscape and the developing threat have been addressed in D1.2 (section 4.1). The literature supports the theory that terrorism has developed from high profile hostage situations throughout the 1970s and 80s to become a situation populated by acts of extreme violence and lethality, where the distinction between legitimate targets and places of safety have been blurred to the extent that some would argue that nothing is off-limits (see D1.2 section 4.1). D1.3 addressed the potential threats that could affect hospitals, the literature revealed the potential for the hospital to be a soft target for a direct terrorist attack or the possibility of being the target for a secondary attack, known as the so called second strike attack. The notion that hospitals are places of safety and sanctuary is dispelled by the work of Ganor and Wernli (2013) who discuss the approximately 100 terrorist attacks that have been perpetrated against hospitals worldwide, between 1981 and 2013, causing 775 deaths and 1,217 injured casualties. Among those attacks 11 European hospitals were attacked, mainly by armed assaults and bombings. This condition requires additional capacity building and planning in hospital resilience, risk reduction and preparedness with regard to possible terrorist attacks. However, the current condition of EU hospital preparedness, in respect of disasters and human-made crisis such as a terrorist attack, has been reported as insufficient, which was supported by the research conducted for D2.1. Evaluation of 49 hospitals in 16 EU states suggested that a considerable portion of EU hospitals are not well prepared and resilient to manage the impact of a direct attack against the hospital, with no implementation of financial resources, not being considered as a priority, and lack of knowledge being the main barriers to have resilient and well prepared health systems in EU, in respect of terrorist attacks against health infrastructures.

To establish effective preparedness and resilience to manage the potential effects during a crisis, health systems need to have a precise analysis of previous experiences from other similar entities. Although there are many limitations on current research about disaster medical planning, the best practice data can be used to improve resilience and emergency planning by health systems.

A good practice may be defined as a methodology, project or process which has already proved successful and also has the potential to be transferred to a different geographic area. The measure of success should be that the practice has already provided results in achieving a specific objective, preferably the results should be measurable (see for example Interreg IVC).

Key criteria of best practices are suggested as below:

- Currency: The practice is of current or recent application and is seen to make a difference.
- Innovation: The practice offers a fresh solution to a current issue.
- Benefit: The practice should be beneficial and those benefits should be tangible and measurable.
- Transferability: The practice should be transferable to other geographical regions and settings.

- Reference of theory and practice: The practice should be based on current theory and in keeping with recent findings (Guide on best practice).

Additionally it is important to acknowledge that best practice will not be properly actioned and embraced by an institution unless there is sufficient goodwill from senior management (see D1.4 sections 5.1, 5.2., 5.3 and D1.5 sections 1.2 ,2.4). Security systems only operate well if there are sufficient and adequately trained staff to monitor and action them (see D1.4 section 1.2). There needs to be management support to ensure that staff are communicated with, trained and assessed on their specific roles and responsibilities in the case of an emergency. This is especially important as an incident is likely to require cooperation with external agencies, police, fire services, and armed forces, and clarity of communication and command chain is critical in emergency situations (see D1.4 section 5.4).

The main objective of the current task and deliverable 2.4 is to recognize and evaluate the best practices of health sector and EU hospitals for risk management and reduction against terrorist attacks and inter-organisational plans.

2. Methods

This study is a review including articles, documents and cases of the survey 2.1 (deliverable 2.1 of THREATS project). The study was conducted between May 2015 and September 2015.

Three sources of data were used to search, evaluate and recognize the best practices of hospitals in respect of terrorist attack against them. The inclusion criteria for the document were that: 1) formally reported or published by the researchers or authorities; 2) are in English language.

Although the context of current project (THREATS) is EU and direct terrorist attacks against hospitals, the documents from non-EU countries and also out of hospital terrorist attacks were also evaluated in this study.

The first source was Google and relevant sources such as Google scholar. The second source was Pubmed, and the third source was the data which came from survey 1 of same work-package of current study (Deliverable 2.1) in which 49 hospitals from 16 EU states were evaluated in respect of resilience and preparedness in case of terrorist crises.

To search in Google and Pubmed, different key words were used including: hospital, health facility, preparedness, resilience, terrorist, crisis, best practice, good practice, etc. These engines were chosen because they publish scientific literatures and articles in the field of health and medicine, including crisis management.

No time period was considered to limit the search outputs.

Data analysis was performed on the basis of the indicators that were defined as the checklist of survey 1 (deliverable 2.1).

The approaches described provided triangulation on the question and relevant findings of this study. Although other methods such as site visiting, development of exercises, and making a simulation were optional approaches, the financial and authority limitations turned these approaches aside from the current study.

3. Results

Three sources of data were searched to recognize possible best practice of hospital plans on resilience and preparedness in respect of direct terrorist attacks against it.

- The first source of data was Pubmed. There was no article in Pubmed that reports a hospital preparedness and resilience plan with regard to direct terrorist attack against the hospital. Also, despite 100 attacks against hospitals (Ganor & Wernli 2013), none of the articles reported either hospital functional collapse or hospital response operation as a result of real direct terrorist attack against the hospitals. However, there were group of articles that reported hospital response to out of hospital terrorist attacks. As examples, 14 of these articles, published between 1995 and 2015, were chosen and evaluated, six of which described hospital terrorist attacks in Europe and the remaining eight were from other geographical areas (see appendix 1 for a list).

  There was a wide range of casualties number admitted at the reported hospitals, from a few to more than 400. However, the in-hospital mortality rate was reported as very low in these articles.

  Almost all articles confirm that the hospitals had crisis management plans of some sort and did activate them to manage the surge of casualties coming from the terrorist attack scene. However, poor communication has been reported as the major problem in these articles. Also, during the Tokyo subway attack with Sarin gas, huge problems came from the lack of preparedness for chemical emergencies and the absence of decontamination facilities. There is insufficient data to evaluate if the hospitals carried out good practice during these events and had adequately considered standardized elements of resilience, preparedness and response to terrorist attacks.

❖ The second source of data was the first survey of this work package (D2.1) and the responses of the hospitals evaluated. Detailed analysis of the elements reported by the 49 evaluated hospitals showed that the preparedness and resilience plan of only three hospitals might be presented as acceptable practice. In fact, one hospital from Sweden and two hospitals from the United Kingdom have established most elements of hospital resilience and preparedness in respect of a direct terrorist attack against their hospital. A summary of key elements of these best practices are explained as below:

- In both countries (UK & Sweden), hospitals are considered as health critical infrastructures.
- The hospitals have developed the resilience and preparedness plan on the basis of a national indicator in respect of the preparedness of health system critical Infrastructure, including hospitals, for possible terrorist attacks. The plan is a written document available for relevant authorities.
- Both UK hospitals declared having an experience of response to a terrorist attacks (out of hospital event) but Swedish hospital did not have same experience.
- On the basis of previous experiences, the hospitals consider the possibility of being a secondary target of the terrorist attack even where it happens outside of the hospital.
- One of the hospitals has experienced one known data breach in the past five years, but none of the hospitals have experienced a network breach.
- Whilst not a terrorist event, one of hospitals had experience of a Hazardous Materials emergency.

- The crisis management plan is regularly (once a year) revised and updated on the basis of some guidelines and also includes the feedback from established exercises.
- These hospitals are provided with information/guidance on how to reduce the vulnerability to terrorist attacks or the consequences of them, outside or inside the hospital from either within their own sector or from governmental guidance and advice .
- All three hospitals are provided with security intelligence regarding terrorist threats, and have a security manager within the hospital who is responsible for receiving and disseminating this intelligence. The manager is responsible for managing the threat and risk of terrorism. Besides, the hospitals have implemented various protective measures to reduce the threat or consequences of a terrorist attack, either outside or inside the hospital, or the medical centre.
- Consistent to previous findings, there is no specific funding available to be used for resilience and preparedness programmes in respect of terrorist attacks against these hospitals. However, one of the UK hospitals uses external funding resources for this issue.
- The hospitals use various inspections/checks to assess the vulnerability and consequences of a terrorist attack outside or inside the hospital.
- These hospitals undertake regular exercises, training and awareness programmes for the hospital staff in respect of threats, vulnerability and consequence of terrorist attacks on the facility.
- The results of these programmes are reviewed and evaluated to identify strengths and areas for improvement of the hospital crisis management plan including resilience and preparedness elements. All these three hospitals declare that there

is a mechanism for monitoring the continuous correction of gaps that were identified in the exercises. Some examples of previous changes have been the upgrade of security equipment, additional security measures, and changes of policies and procedures.

- The hospitals consider explosion, shooting, using CBRN agents, and cyber attacks as possible terrorist threats against the medical centre.
- To contact and conduct cooperation with other response entities and stakeholder agencies is a fundamental part of the crisis management plan of these hospitals.
- To protect the safety of staff, patients and inhabitants in case of a terrorist attack to hospital, the hospitals consider a range of actions, such as: identifying an area of safe refuge, having a procedure for sheltering in-place, having lockdown and evacuation procedures.
- The hospitals are to some degree self-sufficient in terms of back-up energy, water and food supply.
- All three hospitals have ongoing emergency management training and education programmes. Furthermore, they use tabletop exercise, full-scale rehearsals, face-to-face training, lectures, presentations, and also online training modules to train personnel and improve the response against emergencies.
- The hospitals have experience of participation in simulation / exercise in response to terrorist attacks, either as internal simulation or external training including national exercising.
- The key personnel of all three hospitals have been identified and trained in how to implement a formal Incident Command system. In addition, the hospitals provide training for relevant key staff on how to recognize and respond to suspicious

activity, including unidentified packages and persons exhibiting suspicious behaviour.

- To improve the safety of the medical centre, these hospitals perform a list of activities and precautions, such as:
  - access to sensitive areas of the hospital are restricted to authorized personnel only
  - alarm system to detect unauthorized entry or attempted entry to critical components
  - specific training of security personnel, including the proprietary security force, contractual security personnel and duty law enforcement officers
  - gate control system to control the access of vehicles
  - closed circuit television cameras with record and archive capability
  - screening of visitors who seek to enter the hospital after regular visiting hours, monitoring centre
  - screening of visitors in normal visiting hours
- The hospitals regularly use a security assessment framework to assess physical facilities of the facilities.
- In order to sustain communications with the local emergency management agency, these hospitals have established special modes of communication. Furthermore, they have installed a backup radio system within dedicated emergency control rooms. These specific tools of communication are periodically tested.
- In respect of Cyber and information security, the hospitals adopt multiple precautions including:
  - Each employee has an individual account with a unique username and password

  - Restricted unauthorized access to the network
  - Monitored network activities for unauthorized use
  - Patient confidential information management
  - Internet firewall software and virus protection are installed on every computer
  - Physical locks on devices and their communication ports to prevent tampering
  - Routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services
  - Secure connection to the Internet
  - Development and evaluation of strategies to maintain critical functionality during adverse conditions
- In respect of hospital personnel, various precautions are taken under consideration, as below:
  - when hiring personnel, background, employment eligibility and professional references are appropriately verified according to standardized guidelines
  - the hospital provides identification badges to all employees and volunteers
  - when terminating employment, employees are required to turn in photo IDs, keys, access codes, and other security-related items
- At these hospitals, the personnel have a checklist to use for threats or suspicious calls or to report suspicious activity, on the basis of approved procedures.
- These hospitals stockpile Personal Protective Equipment and also have established decontamination facilities to be used during possible CBRN emergencies.
- Consistent with the previous surveys undertaken within the current study, financial shortcoming, poor knowledge of personnel, and giving low priority to the preparedness of hospital in respect of terrorist attacks are declared as problems

and issues by these hospitals. However, the hospital security is considered as very high priority to the headquarters, chief executive officers and managers and key directors of these hospitals.

- The third approach was to search Google and Google scholar to find best practices of hospitals in respect of resilience and preparedness to face terrorist attacks. There was no published report on good practice of either health system or hospitals in respect of resilience and preparedness for direct terrorist attacks. This confirms and is consistent with the observation in D1.5 (section 5) and D2.1 (section 4) that the health sector is less aware of the risk of a terrorist first strike than seems desirable. However, there were some documents that presented a list of recommendations and procedures in the subject of risk assessment of terrorist attacks against infrastructures. Among those documents, a document published in the UK by the National Counter Terrorism Security Office (NaCTSO) specifically takes health system under consideration as "Counter Terrorism Protective Security Advice for Health" (2009, reviewed 2014). This guideline considers some of very important elements of a health system in respect of resilience and preparedness in case of terrorist attacks.

A summary of this good practice from this document follows, and extracts from the original can be found in Appendix 2. Based on advice to the facilities in the UK, it is suggested that key tasks include:

I. Risk management

Step One: Identify the threats.

Step Two: Decide what a health centre needs to protect and identify its vulnerabilities under the categories:

- People (staff, patients, contractors and the general public)
- Physical assets (buildings, contents, equipment, plans and sensitive materials e.g. pathogens)
- Information (limiting access to electronic and paper data)

Step Three: Identify measures to reduce risk.

These may be very similar to the measures identified in order to harden a hospital against crime in general.

Step Four: Rehearse and revise emergency and contingency plans and review your security measures.

Major incident plans have to be tested to ensure that emergency and security plans remain accurate, workable and up to date.

II. Security planning

An adequate security plan is essential and should include the following:

- Protective security measures
- Instructions to security staff
- Instructions on how to respond to a threat
- Instructions on how to respond to the discovery of a suspicious item or event
- A search plan
- Evacuation and lockdown plans
- Business continuity plans
- A communications and media strategy.

III. Physical security

This flows from the risk assessment, and physical security in a hospital needs to walk the line between the need for safety and the mission of a hospital as an open access facility that provides healthcare:

- Security awareness
- Access control
- Security patrols
- Traffic and parking controls
- Doors and windows
- Perimeter
- Integrated security systems

IV. Good housekeeping

Good housekeeping reduces the opportunity for placing suspicious items and reduces opportunities for and effects of false alarms and hoaxes:

- Consideration of placement and type of litter bins
- Use of clear bags for commercial waste disposal
- Clear exits and public areas
- Reduce opportunities to hide devices
- Lock unoccupied offices, rooms and store cupboards
- Keep external areas as clean and tidy as possible
- If appropriate, prune vegetation and trees, especially near entrances.

V. Access control

Good access controls are needed to ensure that the buildings and any part of them are only accessed by authorised people. Security staff deployed externally should adopt a 'see and be seen' approach. .

VI. CCTV guidance

The importance of CCTV as a component of a security system is widely supported, but CCTV does need to be monitored and maintained.

VII. Small deliveries by courier and mail handling

Consideration of whether a screening process is needed.

VIII. Search planning

Security patrols should be part of everyday work. Searches of the healthcare site should be conducted as part of daily good housekeeping routine. They should also be conducted in response to a specific threat and when there is a heightened response level.

IX. Evacuation planning

As with search planning, evacuation should be part of the security plan. In relation to terrorism the evacuation of health facility might be needed because of:

- A threat received directly to the health body
- A threat received elsewhere or an incident elsewhere passed on to the health body by the police
- Discovery of a suspicious item or vehicle in or outside of the building.

X. Personnel security

Some external threats, whether from criminals, terrorists, or competitors seeking a business advantage, may rely upon the cooperation of an 'insider'.

Personnel security is a system of policies and procedures which seek to manage the risk of staff or contractors exploiting their legitimate access to a health bodies' assets or premises for unauthorised purposes.

XI. Information security

The loss of confidentiality, integrity and most importantly availability of information in paper or digital format can be a critical problem for health bodies.

Cyber Attacks on systems could:

- Allow the attacker to steal or alter or remove sensitive information
- Allow the attacker to gain access to the computer system and do whatever the system owner can do.
- Make the systems impossible to use through 'denial of service' attacks.

XII. Vehicle borne improvised explosive devices (VBIEDs)

Vehicle Borne Improvised Explosive Devices (VBIEDs) are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage.

Security precautions, proportional to the risk and taking into account the practicalities of the site, must be in place to ensure hospital vehicles are always kept securely.

XIII. Chemical, Biological and Radiological (CBR) attacks

The likelihood of a CBR attack remains low but hospitals should consider:

- Review the physical security of any air handling systems.
- Improve air filters or air handling systems, as necessary.
- Restricting access to water tanks and other key utilities.
- Reviewing the security of food and drink supply chains.
- Seeking advices of an organisation that uses CBR detection technologies as part of their contingency planning measures.
- Whether the areas of safe refuge are suitable for CBR sheltering.
- How to communicate necessary safety advice to staff and how to offer reassurance.

XIV. Suicide attacks

The use of suicide bombers is a very effective method of delivering an explosive device to a specific location. The most likely targets are mass casualty crowded places, symbolic locations and key installations. Protective measures against suicide bombers should be covered by the physical and personnel security measures.

XV. Firearm and weapon attacks

Terrorist use of firearms and weapon is infrequent, but it is still important to consider this method of attack and a proportionate response to cope with such an incident.

XVI. Communication and training

A communication strategy should be taken under consideration for raising awareness among staff and others who need to know about your security plan and its operation.

XVII. Hostile reconnaissance

Hostile reconnaissance is used to provide information to operational planners on potential targets during the preparatory and operational phases of terrorist operations, such as:

- Obtain a profile of the target location.
- Determine the best method of attack.
- Determine the optimum time to conduct the attack.

An intelligence gathering operation is needed to record, research, investigate and analyse:

- Suspicious sightings
- Suspicious activity

at or near:

- Crowded places

or prominent or vulnerable:

- Buildings

- Structures
- Transport infrastructure.

XVIII. High profile events

These may make a hospital briefly a more attractive target.

XIX. Threat levels

Terrorism threat levels should be considered in planning the appropriate security response.

4. Conclusion

Despite more than 100 terrorist attacks against hospitals since 1981, and increasing terrorist threats during last years, there is no evidence of a published report regarding whether hospitals have carried out sufficient efforts on resilience and preparedness for possible attacks. Therefore, it seems that there is a significant gap in the health system, in respect of hospital resilience and preparedness for direct terrorist attacks against the health services. Previous studies of THREATS have already reported that financial shortcomings, perception of risk, lack of knowledge and competing priorities for resources are the main barriers to the desired state.

Data analysis of 49 hospitals in Europe revealed that only a few hospitals in EU states can be considered as examples of good practice, in respect of preparedness for direct terrorist attacks. Even these hospitals have not established all elements needed to be resilient in case of a terrorist attacks. This situation requires a revision in EU level strategy and action regarding hospital resilience and preparedness against terrorist attacks.

Although multiple guidelines on prevention and preparedness of public facilities for terrorist attacks are available worldwide, there is only one guideline that was found that has focused on health system and comprehensively provides a list of interventions to be considered by medical centres and health bodies with regard to resiliency and preparedness for terrorist attacks.

Overall, this study identified that EU hospitals are not sufficiently prepared to manage terrorist attacks directed at medical facilities; there is little evidence of standardised planning and guideline to prevent a possible threat against hospitals. The current situation can be improved by the development and adoption of a comprehensive and standardised toolkit specifically designed and targeted to assist and guide EU hospitals in the steps to mitigate terrorist threats and to manage the impact and consequences of a possible terrorist attack. This guidance should build upon the extant good practice and generic advice for the protection of facilities, personnel and data but be tailored to the specific needs and demands of the health care sector and hospitals.

This will require a multi-agency and multi-sectoral approach as our hospitals and health care facilities represent not only a major critical asset to our communities but the long term well-being of society.

5. References

Barbera JA, Yeatts DJ, Macintyre AG. Challenge of hospital emergency preparedness: analysis and recommendations. Disaster Med Public Health Prep. 2009;3(2):S74-S82.

Becker SM, Middleton SA. Improving hospital preparedness for radiological terrorism: perspectives from emergency department physicians and nurses. Disaster Med Public Health Prep. 2008 Oct;2(3):174-184.

Bennett RL. Chemical or biological terrorist attacks: an analysis of the preparedness of hospitals for managing victims affected by chemical or biological weapons of mass destruction. Int J Environ Res Public Health. 2006 Mar;3(1):67-75.

Cone, D. C., & Cummings, B. A. (2006). Hospital disaster staffing: If you call, will they come? American Journal of Disaster Medicine, 1(1), 28-36.

Counter Terrorism Protective Security Advice for Health. National Counter Terrorism Security Office. 2009. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374771/Health__Reviewed.pdf

Dimaggio C, Markenson D, Loo G. Redlener I. The willingness of u.s. Emergency medical technicians to Respond to terrorist incidents. Biosecurity and bioterrorism: biodefense strategy, practice, and science. Volume 3, number 4, 2005

Djalali A, Della Corte F, Foletti M et al. Art of Disaster Preparedness in European Union: a Survey on the Health Systems. PLOS Currents Disasters. 2014 Dec 17. Edition 1

Eckstein M, Cowen AR: Scene safety in the face of automatic weapons fire: a new dilemma for EMS? Prehosp Emerg Care 1998, 2:117–122.

European law enforcement agency. European Union Terrorism Situation and Trend Report 2014. www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015. Accessed October 20th, 2015.

Ganor, B. and Wernli, M. (2013) International Institute for Counter-Terrorism (2013) *Terrorist Attacks against Hospitals Case Studies.* [s.l.]: ICT. Available from: www.ict.org.il/Article/77/Terrorist%20Attacks%20against%20Hospitals%20Case%20Studies

Goodhue, Burke, et al. Willingness to Respond in a Disaster: A Pediatric Nurse Practitioner National Survey. Journal of Pediatric Health Care (2011) Volume 26, Issue 4, pag. 7-20

Guide on best practice. Info entrepreneurs. Available from http://www.infoentrepreneurs.org/en/guides/best-practice/.

Kearns RD, Myers B, Cairns CB, et al. Hospital bioterrorism planning and burn surge. Biosecur Bioterror. 2014 Jan-Feb;12(1):20-28.

Lanzilotti, S. S., Galanis, D., Leoni, N., & Craig, B. (2002). Hawaii medical professionals assessment. Hawaii Medical Journal, 61(8), 162-173.

Martens, K., Hantsch, C., & Stake, C. (2003). Emergency preparedness survey: Personnel availability and support needs. Annals of Emergency Medicine, 42(Suppl 1), 389.

Masterson L, Steffen C, Brin M, Kordick MF, Christos S. Willingness to respond: of emergency department personnel and their predicted participation in mass casualty terrorist events. J Emerg Med. 2009 Jan;36(1):43-9.

Okumura T, Hisaoka T, Yamada A, et al. The Tokyo subway sarin attack--lessons learned. Toxicol Appl Pharmacol. 2005 Sep 1;207(2 Suppl):471-476.

O’Sullivan, T. L., Dow, D., Turner, M. C., Lemyre, L., Corneil, W., Krewski, D., Amaratunga, C. A. (2008). Disaster and emergency management: Canadian nurses_ perceptions of preparedness on hospital front lines. Prehospital Disaster Medicine, 23(3), s11-s18.

6. Appendices

Appendix 1

A list of attacks considered on pp10-11

- Terrorist attacks in Paris, France in November 2015
- Bombing in Boston, USA, in 2013
- Bombing and shooting in Oslo, Norway in 2011
- Shiraz bombing, Iran, in 2008
- Bombing in Tel-Aviv, Israel, in 2006
- Bombings at London subway, United Kingdom, in 2005
- Madrid train bombing, Spain, in 2004
- Taba bombing attack, Egypt, in 2004
- Bombing in Istanbul, Turkey, in 2003
- Terrorist attack in Myyrmäki, Vantaa, Finland, in 2002
- Bali bombing, Indonesia, in 2002.
- World Trade Center, New York, USA, 2001
- Tokyo subway Sarin attack, Japan, in 1995

Appendix 2

An extract from Counter Terrorism Protective Security Advice for Health. National Counter Terrorism Security Office. 2009 (reviewed 2014).

> “This guidance has been developed to assist the health sector in addressing a range of security issues relating to possibility of a terrorist attack to a crowded place within their site. The advice provided in this booklet is built on knowledge, learning and best practice developed between the National Counter Terrorism Security Office, health sector security professionals including the NHS Counter Fraud and Security Management Service (NHS England), and representatives from the devolved health care administrations across the UK.
>
> …
>
> As part of their security regime, all health care sites should conduct regular reviews of their facilities to ensure proportionate security measures are in place. Each review should consider any new threats and developments to the health sites and the surrounding area. Any security measure to prevent a terrorist attack will also feed into general crime prevention measures and business continuity which will ensure that health care sites can cope with an incident while also continuing with their core activities. Having a robust security culture and being better prepared will reassure patients, staff and visitors and the wider community that your health care sites are taking such issues seriously.
>
> …

Risk management

With regard to protective security, the best way to manage the risks to a health body is to start by understanding and identifying the threats to it, and its vulnerability to those threats. A threat refers to a possibly malicious event, instigated by an individual or group, which has the potential to cause loss of or damage to an asset (people and property) for example, insider threats, IT and terrorists attacks. Dealing with the potential threat of a terrorist attack…is important to give it due consideration in emergency and security plans.

This will help to decide:

- What type of security and contingency plans you need to develop
- What security improvements you need to consider taking account of cost and their impact on existing security measures. It is important to review what security measures, policies and procedures are already in place as well as compliance with these before investing in additional security measures.
- Simple good practice coupled with vigilance and well exercised contingency arrangements may be all that is needed. Therefore this may not necessarily mean additional work as existing crime prevention measures will also provide a deterrent against terrorism.
- If, however, you assess that you are vulnerable you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable.

Step One: Identify the threats.

Understanding the terrorists' intentions and capabilities what they might do and how they might do it is crucial to assessing threat…

Step Two: Decide what a health centre needs to protect and identify its vulnerabilities.

The priorities for protection should fall under the following categories:

- People (staff, patients, contractors and the general public)
- Physical assets (buildings, contents, equipment, plans and sensitive materials e.g. pathogens)
- Information (limiting access to electronic and paper data) …

Step Three: Identify measures to reduce risk.

…TERRORISM IS A CRIME and many of the security precautions typically used to deter criminals are also effective against terrorists. For example methods to reduce the risk of burglary or theft for example, will also provide a deterrent against terrorism. Whatever security measures are introduced, an integrated approach to security is essential. This involves thinking about physical security, information security and personnel security (i.e. good recruitment and employment practices). There is little point investing in costly security measures if they can be easily undermined by a disaffected member of staff or by a lax recruitment process. …

Step Four: Rehearse and revise emergency and contingency plans and review your security measures.

…

Major incident plans have to be tested. The testing involves Category 1 responders, organisations at the core of a healthcare emergency response (e.g. primary care trusts, NHS acute trusts, foundation trusts and Local Health Boards) and Category 2 organisations who are cooperating bodies and less likely to be involved in the heart of planning work. Any rehearsals and exercise should wherever possible, be conducted in conjunction with all partners, emergency services and local authorities. Regular tabletop exercises simulating an emergency situation and 'live' exercises should be completed to ensure that emergency and security plans remain accurate, workable and up-to-date. …

Security planning

Responsibility for the implementation of protective security measures following a vulnerability and risk assessment will fall on the Security Manager who should have sufficient authority to direct the action taken in response to a security threat. …

Creating a Security Plan

The Security Manager should aim to produce a plan that has been fully exercised, and which is regularly audited to ensure that it is fit for purpose. When creating a security plan, consider the following:

- Details of all the protective security measures to be implemented, covering physical, information and personnel security
- Instructions/briefings to security staff including the types of suspicious behaviour to look for and methods of reporting
- Instructions on how to respond to a threat (e.g. telephone bomb threat)

- Instructions on how to respond to the discovery of a suspicious item or event
- A search plan
- Evacuation and lockdown plans, including both partial and full evacuation/lockdown measures
- Business continuity plans, should include all mutual aid arrangements in the event of a major incident that results in an evacuation/lockdown
- A communications and media strategy developed by your Communications /Media department which includes handling enquiries from concerned family and friends

…

Physical security

Physical security is important in protecting against a range of threats and addressing vulnerability.

Security measures should be put in place to remove or reduce your vulnerabilities to as low as reasonably practicable bearing in mind the need to consider safety as a priority at all times. Security measures must not compromise the safety of your staff and patients.

Your risk assessment will determine which measures you should adopt, they will range from good housekeeping (keeping communal areas clean and tidy) through to CCTV, perimeter fencing, intruder alarms, computer security and lighting…

Some of important actions that should consider are:

- Security awareness…
- Access control…
- Security patrols…

- Traffic and parking controls…
- Doors and windows…
- Perimeter…
- Integrated security systems… …

Good housekeeping

Good housekeeping improves the ambience of your site/location and reduces the opportunity for placing suspicious items or bags and helps to deal with false alarms and hoaxes.

You can reduce the number of places where devices may be left by considering the following points:

- Avoid the use of litter bins around critical/vulnerable areas i.e. do not place litter bins next to or near glazing, support structures, most sensitive or critical areas (but if you do ensure that there is additional and prompt cleaning in these areas).
- Alternatively review the management of all your litter bins and consider the size of their openings, their blast mitigation capabilities and location, i.e. do not place litter bins next to or near glazing or support structures.
- The use of clear bags for commercial waste disposal is a further alternative as it provides an easier opportunity for staff to conduct an initial examination for suspicious items. Good practice in relation to waste will be included in the respective health bodies' waste management policy.
- Keep public and communal areas exits, entrances, queues, lavatories clean and tidy, as well as service corridors and areas.

- Keep the fixtures and fittings in such areas to a minimum ensuring that there is little opportunity to hide devices.
- Lock unoccupied offices, rooms and store cupboards.
- Ensure that everything has a place and that things are returned to that place.
- Place tamper proof plastic seals on maintenance hatches.
- Keep external areas as clean and tidy as possible.
- If allowed, pruning vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages. ...

Access control

Good access controls are a vital component to ensure that any building and any part of it are only accessed by authorised people. They are a vital means of ensuring that areas of health bodies are restricted to authorised people, whether this is through a physical access control (i.e. achieved by a guard) or by mechanical or technological means.

Security staff deployed externally should adopt a 'see and be seen' approach. This approach should be monitored by CCTV operators if available and communication between visitors and staff established.

Any lack of vigilance around pedestrian and vehicle entrances affords anonymity to a potential terrorist.

Risk assessment

Refer to 'managing the risks' on page 29 and decide the level of security you require before planning your access control system. Take into account any special features you may require.

Ease of access

Examine the layout of your site. Ensure that your entry and exit procedures allow legitimate users to pass without undue effort and delay.

Ideally, adopt a photo ID card access control system which varies in appearance for the different levels of access across the site. Security staff should be instructed what to examine when checking passes and this should be quality assured through testing.

Training

Ensure your staff are fully aware of the role and operation of your access control system. Your installer should provide adequate system training.

System maintenance

Your installer should supply all relevant system documentation, e.g. log books and service schedules. Are you aware of the actions required on system breakdown? Do you have a satisfactory system maintenance agreement in place? Is there a contingency plan you can implement at a moments notice?

Interaction

Your access control system should support other security measures. Consider system compatibility between access control, alarms, CCTV and text alert systems

Access control is only one important element of your overall security system.

CCTV guidance

The importance of CCTV as a component of a security system is widely supported especially as CCTV can help clarify whether a security alert is real and is often vital in any post incident investigation …

Ask yourself the following questions about your CCTV system:

- Is your CCTV system regularly serviced?
- Is your CCTV system currently achieving what you require it to do? Do you need it to confirm alarms, detect intruders through doors or corridors and produce images of evidential quality?
- Are the CCTV cameras in use for the protective security of your event integrated with those used to monitor crowd or visitor movement?
- Would the introduction of an Automatic Number Plate Reader (ANPR) system complement your security operation?...

Consider also the following points:

- Ensure the date and time stamps of the system are accurate.
- Regularly check the quality of recordings.
- Digital CCTV images should be stored in accordance with the evidential needs of the Police. Refer to CAST (HOSBD) publication 09/05.
- Ensure that appropriate lighting complements the system during daytime and darkness hours...
- Keep your recorded images for at least 31 days.
- Use good quality media and check it regularly by ensuring that backups are operating correctly
- Ensure the images recorded are clear that people and vehicles are clearly identifiable.
- Check that the images captured are of the right area.
- Implement standard operating procedures, codes of practice and audit trails.
- Give consideration to the number of camera images a single CCTV operator can effectively monitor at any one time.

- Do you have sufficient qualified staff to continue to monitor your CCTV system during an incident, evacuation or search? ...

Small deliveries by courier and mail handling

Each health centre should consider the need for a screening process at their mail handling site, whether at a temporary or permanent structure and consider the following

…

- Indicators to Suspicious Deliveries/Mail, such as:
  - It is unexpected or of unusual origin or from an unfamiliar sender.
  - There is no return address or the address cannot be verified.
  - It is poorly or inaccurately addressed e.g. incorrect title, spelt wrongly, title but no name, or addressed to an individual no longer with the company.
  - ....
- Planning mail handling procedures…such as:
  - Seek advice from your local police Counter Terrorism Security Advisor (CTSA) on the threat and on defensive measures in conjunction with the health bodies' LSMS/Security Manager.
  - Consider processing all incoming mail and deliveries at one point only. This should ideally be offsite or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the site.
  - Ensure that all sources of incoming mail (e.g. Royal Mail, couriers, and hand delivery) are included in your screening process.

- ....

Search planning

Security patrols should be part of everyday work, and the LSMS/ Security Manager should be responsible for overseeing them.

Searches of the healthcare site should be conducted as part of your daily good housekeeping routine. They should also be conducted in response to a specific threat and when there is a heightened response level.

As previously mentioned under Security Planning, it is recognised that for the majority, responsibility for the implementation of any search planning, following a vulnerability and risk assessment, will fall upon the LSMS/Security Manager.

The following advice is generic for most health bodies, but recognises that health bodies are built and operate differently. If considered necessary, advice and guidance on searching should be available through your local CTSA.

Search Plans

- Search plans should be prepared in advance and staff should be trained in them.
- Search planning should be incorporated in the overall security plan and should be part of routine good housekeeping.
- The conduct of searches will depend on local circumstances and local knowledge, but the overall objective is to make sure that the entire area, including grounds, are searched in a systematic and thorough manner so that no part is left unchecked.
- The member(s) of staff nominated to carry out the search do not need to have expertise in explosives or other types of device. But they must be familiar with

the place they are searching. They are looking for any items that should not be there, that cannot be accounted for and items that are out of place.

- Ideally, searchers should search in pairs; to ensure searching is systematic and thorough.

…

Evacuation planning

…

As with search planning, evacuation should be part of your security plan. In relation to terrorism you might need to evacuate your health body because of:

- A threat received directly to the health body.
- A threat received elsewhere and passed on to you by the police.
- Discovery of a suspicious item (perhaps a postal package, an unclaimed holdall or rucksack).
- Discovery of a suspicious item or vehicle outside a building.
- An incident to which the police have alerted you.

Whatever the circumstances, you should tell the police as soon as possible what action you are taking.

The biggest dilemma facing anyone responsible for an evacuation plan is how to judge where the safest place might be. For example, if an evacuation route takes people past a suspect device outside your building, or through an area believed to be contaminated, external evacuation may not be the best course of action.

A very important consideration when planning evacuation routes in response to near simultaneous terrorist attacks is to ensure people are moved away from other potential areas of vulnerability, or areas where a larger secondary device could detonate.

The decision to evacuate will normally be yours, but the police will advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation with your LSMS/Security Manager.

A general rule of thumb is to find out if the device is external or internal. If it is within a building you may consider evacuation, but if the device is outside the building it may be safer to stay inside.

…

Personnel security

Some external threats, whether from criminals, terrorists, or competitors seeking a business advantage, may rely upon the cooperation of an 'insider'.

…

Personnel security is a system of policies and procedures which seek to manage the risk of staff or contractors exploiting their legitimate access to a health bodies' assets or premises for unauthorised purposes. These purposes can encompass many forms of criminal activity, from minor theft through to terrorism…

This chapter refers mainly to pre-employment screening, but health bodies should be aware that personnel screening should continue throughout the live cycle of the employee…

- Understanding and assessing personnel security risks
- Data Protection
- Pre-employment Screening
- .....

Information security

The loss of confidentiality, integrity and most importantly availability of information in paper or digital format can be a critical problem for health bodies. Many rely on their information systems to carry out business or nationally critical functions and manage safety and engineering systems.

…

Attacks on electronic systems could:

- Allow the attacker to steal or alter remove sensitive information
- Allow the attacker to gain access to your computer system and do whatever the system owner can do. This could include modifying your data, perhaps subtly so that it is not immediately apparent, installing malicious software (virus or worm) that may damage your system, or installing hardware or software devices to relay information back to the attacker. Such attacks against internet connected systems are extremely common.
- Make your systems impossible to use through 'denial of service' attacks. These are increasingly common, relatively simple to launch and difficult to protect against.

Electronic attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet.

The typical methods of electronic attack are:

- Malicious software…
- Denial of service…
- Hacking…
- Malicious modification of hardware…

…

Vehicle borne improvised explosive devices (VBIEDs)

Vehicle Borne Improvised Explosive Devices (VBIEDs) are one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage.

Once assembled, the bomb can be delivered at a time of the terrorist's choosing and with reasonable precision, depending on defences. It can be detonated from a safe distance using a timer or remote control, or can be detonated on the spot by a suicide bomber.

Building a VBIED requires a significant investment of time, resources and expertise. Because of this, terrorists will seek to obtain the maximum impact for their investment.

Terrorists generally select targets where they can cause most damage, inflict mass casualties or attract widespread publicity.

Security precautions, proportional to the risk and taking into account the practicalities of the site, must be in place to ensure NHS vehicles are always kept securely. This will ensure that they never fall into the wrong hands.

…

Chemical, Biological and Radiological (CBR) attacks

…

Much of the CBR related activity seen to date has either been criminal, or has involved hoaxes and false alarms. There have so far only been a few examples of terrorists using CBR materials. The most notable were the 1995 sarin gas attack on the Tokyo subway, which killed twelve people, and the 2001 anthrax letters in the United States, which killed five people.

CBR weapons have been little used so far, largely due to the difficulty in obtaining the materials and the complexity of using them effectively. Where terrorists have tried to carry out CBR attacks, they have generally used relatively simple materials. However, Al Qaeda and related groups have expressed a serious interest in using CBR materials. The impact of any terrorist CBR attack would depend heavily on the success of the chosen dissemination method and the weather conditions at the time of the attack.

The likelihood of a CBR attack remains low. As with other terrorist attacks, you may not receive prior warning of a CBR incident. Moreover, the exact nature of an incident may not be immediately obvious. First indicators may be the sudden appearance of powders, liquids or strange smells, with or without an immediate effect on people.

What you can do

- Review the physical security of any air handling systems, such as access to intakes and outlets.
- Improve air filters or upgrade your air handling systems, as necessary.
- Restrict access to water tanks and other key utilities.
- Review the security of your food and drink supply chains.
- The Home Office advises organisations against the use of CBR detection technologies as part of their contingency planning measures at present. This is because the technology is not yet proven in civil settings and, in the event of a CBR incident, the emergency services would come on scene with appropriate detectors and advise accordingly. A basic awareness of CBR threat and hazards,

combined with general protective security measures (e.g. screening visitors, CCTV monitoring and active response of perimeters and entrance areas, being alert to suspicious deliveries) should offer a good level of resilience. In the first instance, seek advice from your local police force CTSA.

- If there is a designated protected space available this may also be suitable as a CBR shelter, but seek specialist advice from your local police force CTSA before you make plans to use it in this way.
- Consider how to communicate necessary safety advice to staff and how to offer reassurance.

…

Suicide attacks

The use of suicide bombers is a very effective method of delivering an explosive device to a specific location. Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may carry or conceal explosives on their persons. Both kinds of attack are generally perpetrated without warning. The most likely targets are mass casualty crowded places, symbolic locations and key installations.

When considering protective measures against suicide bombers, think in terms of:

- Using physical barriers to prevent a hostile vehicle from driving into your healthcare site through main entrances, goods/service entrances, pedestrian entrances or open land.
- Denying access to any vehicle that arrives at your goods/service entrances without prior notice and holding vehicles at access control points until you can satisfy yourself that they are genuine.

- Wherever possible, establishing your vehicle access control point at a distance from the protected site, setting up regular patrols and briefing staff to look out for anyone behaving suspiciously. Many bomb attacks are preceded by reconnaissance or trial runs. Ensure that such incidents are reported to the police.
- Ensure that no one visits your protected area without your being sure of his or her identity or without proper authority. Seek further advice through your local police force's Counter Terrorism Security Advisor (CTSA).
- Effective CCTV systems especially with an active response, may deter a terrorist attack or even identify planning activity. Good quality images can provide crucial evidence in court.

There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

…

Firearm and weapon attacks

Terrorist use of firearms and weapon is infrequent, but it is still important to consider this method of attack and a proportionate response to cope with such an incident. Below is some general guidance to aid your planning in this area.

…

Communication and training

You should consider a communication strategy for raising awareness among staff and others who need to know about your security plan and its operation. This will include the emergency services, local authorities and possibly neighbouring premises/areas.

…

Hostile reconnaissance

Hostile reconnaissance is used to provide information to operational planners on potential targets during the preparatory and operational phases of terrorist operations.

Primary Role of Reconnaissance:

- Obtain a profile of the target location.
- Determine the best method of attack.
- Determine the optimum time to conduct the attack.

Reconnaissance operatives may visit potential targets a number of times prior to the attack. Where proactive security measures are in place, particular attention is paid to any variations in security patterns and the flow of people in and out.

Operation Lightning is a national intelligence gathering operation to record, research, investigate and analyse:

- Suspicious sightings
- Suspicious activity

at or near:

- Crowded places

or prominent or vulnerable:

- Buildings
- Structures
- Transport infrastructure

…

High profile events

> There may be events held at your health body, which for various reasons, are deemed to be more high profile and therefore more vulnerable to attack. This may involve preventing publicity of the attendance of a VIP or celebrity, resulting in additional crowd density on the event day and the need for an appropriate security response and increased vigilance.
>
> …”