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

Report No: DR/ 1/ 005

Report examining current protective security arrangements within the Health sector and identifying vulnerabilities in existing protection.

Version: 1.0

Date: 28 September 2015

Authors: CD, SC, BD and MM

Approved by: CA

Table of Contents

Executive Summary

This report will provide some context to the current state of security at hospitals within the Health Sector across the European Union (EU). The importance of hospitals as the primary point of delivery of healthcare to the population has been outlined in detail in preceding THREATS project work and the impact upon the ability for society to function has been discussed. It therefore seems somewhat surprising that the protective security of the Health Sector is much less developed than many other areas of critical national infrastructure (CNI) even though hospitals are high-density public spaces. One aspect that has been absent from the THREATS research is corruption, and this report will provide a reference to corruption because it can easily be traced to the poor security culture within the sector and the potential exploitation by the so called 'insider threat'.

Protective security is 'a combination of physical and procedural measures designed to prevent or mitigate threats or attacks against people, information and assets' (Protective Security Requirements, [n.d.]). It can be cost effective and acceptable in terms of enabling an organisation to continue to function effectively while maintaining customer expectation within a protected environment. The THREATS team have adopted the critical pillars of personnel security – to ensure the safety of staff, patients and visitors to the hospital; security of buildings and assets – to protect the buildings and infrastructure from disruption; and protection of information – the security of information technology (IT) and the protection of protectively marked data.

The survey conducted in WP2 (D2.1) provided a useful insight to the way security and resilience are managed within the Health Sector. This report has reviewed some of the D2.1 data to provide a snapshot of the 17 European Union (EU) Member States (MS) that participated in the D2.1 survey. Although 12 MS are not represented, five MS that joined the EU from 2014 onwards have participated, which has enabled a limited comparison between longer term EU membership and newer MS in terms of Health Sector protection. The results did not illustrate a disparity between old and new EU MS, based on the limited data.

The main research approach was to interview suitable and relevant participants who would be able to provide insights based on knowledge and experience of working within the present day Health Sector. The results support the findings of preceding THREATS publications: security is not embedded at the operational level and although some evidence exists that strategic work has been conducted at higher level, the output does not translate

to action within our hospitals. This theory is best illustrated by the absence of any kind of education and training programme to prepare the healthcare workforce to a terror attack at a hospital, the absence of any type of measure or procedure to raise security awareness to anyone entering the hospital, a familiar approach to airport security awareness, and the absence of measures to lockdown and protect hospital facilities and workforce during an attack, measures that are becoming routine at many commercial facilities.

The THREATS team have endeavoured to provide an objective report based on qualitative research data. The remainder of the project will continue to work towards an output to improve preparedness of hospitals that can be utilised at the strategic and operational levels.

1. Introduction

1.1 Protection of assets

In its 2005 strategy declaration the European Commission (EC) declared that its Counter Terror (CT) for Critical Infrastructure (CI) should centre on Prevention, Protection, Pursuit and Response (Council of the European Union, 2005). In order to plan for the protection of assets and reduction of vulnerabilities in full it is necessary to consider an integrated plan that should cover:

- Information
- Protective Security
- Response Planning
- Security Culture (see for example CPNI, Centre for the Protection of National Infrastructure, 2010).

In considering the information aspect, risks should have been identified, assessed and prioritised by Member States (MS), and possibly by the European Union (EU). Protective Security needs to address the three pillars of personnel, physical and information, with the aim of continuity of service. Although there are many examples of 'Protection' and 'Security' in the available literature, the authors have looked as far as New Zealand to find a statement that fits with the THREATS approach to define 'physical security as a combination of physical and procedural measures designed to prevent or mitigate threats or attacks against people, information and assets' (Protective Security Requirements, [n.d.]). The New Zealand government provides additional useful detail that supports the 'layered security approach' (see D1.4):

'A physical security programme has the following aims:

- Deter - these are measures that adversaries perceive as too difficult or needing special tools and training to defeat.
- Detect - these are measures implemented to determine if an unauthorised action is occurring or has occurred.
- Delay - these are measures implemented to impede an adversary during an attack, slow the progress of a detrimental event to allow a response before agency information or physical assets are compromised.
- Respond - these are measures taken once an agency is aware of an attack or event to prevent, resist or mitigate the attack or event.
- Recover - these are measures taken to restore operations to normal (as possible) following an incident.' (Protective Security Requirements, [n.d.])

Response planning should encompass response planning, evacuation plans and business continuity. Security culture may feel slightly nebulous but it is nonetheless important to consider staff awareness and training to ensure people respond in the correct way, especially when under stressful conditions such as an emergency.

1.2 Hospitals in the EU

As with many security related functions, the ownership of the security response and the active support of management at the right level are vitally important. In the United States of America (USA), Homeland Security have identified that the scope of the Healthcare and Public Health (HPH) role and the diverse nature of the sector as being peculiarly challenging:

'For the HPH Sector, critical infrastructure protection (CIP) is ultimately defined by the extent to which the sector has been able to mitigate interruptions in the delivery of healthcare and public health services. Among the challenges to implementing the CIP program in the sector are the breadth and diversity of the sector and the overlap between the sector's CIP role and its emergency response role.' (Homeland Security, 2010:10)

It is therefore germane at this point to consider the nature of the Health Sector and hospitals in the EU.

Homeland Security (ibid) has identified the breadth of the Health Sector as being an issue for its protection in the USA. Size may also be a factor in the EU where citizens spend more than one trillion Euros a year on healthcare (European Commission, 2013:25). The Economist Intelligence Unit (EIU) 2015 estimated that the proportion of the Gross Domestic Product (GDP) spent on health in Western Europe is 10.5%, making it the second largest area of government spending. In Eastern Europe the average spend is 5.8% of GDP. Ownership may also not be straightforward, with many EU Health assets being either privately owned or being in Public Private Partnerships (PPPs) or Public Private Collaborations (PPCs) (Nikolic and Maikisch, 2006). Approximately a third of Health expenditure is spent on hospitals (Berger, 2007). Hospitals of different sizes, ownerships and levels of criticality to the CI therefore play a large part in the diverse sector that is Health.

1.3 Scope

The preceding THREATS publications contain a comprehensive review of the publically available data relating to Critical Infrastructure Protection and specifically the Health Sector.

This report is intended to focus on primary data collated from personnel working within the Health Sector or involved at the strategic level of the Sector.

The main effort has been to develop the work already started in Work Package 2 (WP2) and more specifically the survey conducted as part of the D2.1 in order to gain a deeper understanding of Health Sector preparedness and awareness of terrorist attacks to hospitals. Some of the information may come from a review of the survey data collated in D2.1 but care has been taken to ensure the data is not over analysed. The additional data was collected from a series of interviews with suitable participants.

The THREATS team were aware of the potential constraints and difficulties with participant engagement so an initial concerted effort was applied to test the feasibility of this approach to ensure the effort is commensurate to the results.

A rare opportunity to conduct face-to-face interviews and gain valuable insights from a collection of people at the appropriate level was identified and two independent events within the Healthcare professional field were targeted to exploit a ‘captured audience’. Other interviews were planned and conducted via Skype or other videoconference facility and followed an agreed format of questions.

2. Literature Review

2.1 Protective Security

The aim of Protective Security is to manage security risks effectively and proportionately, to keep a secure working environment for the assets, commensurate with their criticality to the MS and to the EC. Protective Security ought to include a combination of physical, information and personnel security measures that protect and secure through a mix of deterrence, detection and response, and to minimise the consequences of any attack that does occur. Resilience to attack and an ability to recover from an attack may both be important measures by which Protective Security should be judged. The nature of the asset, the geography, the MS will all vary and thus the appropriate mix of measures will depend on the nature of the risk-led assessment of the threats and vulnerabilities in each location.

2.1.1 Physical

Physical security comprises the various steps whether procedural or physical installations that are designed to protect against a physical attack. For example:

- Intruder detection and alarms
- Access control systems
- Security guarding
- Hostile vehicle mitigation, including vehicle security barriers
- Blast protection
- Building design
- Measures protecting assets and drugs

2.1.2 Information

Information security measures aim to protect an organisation's data and its various forms of storage and distribution. This includes protecting information technology (IT) systems against electronic attack as well as measures to secure information stored on mobile devices or paper:

- Network access control measures (typically enforced by 'firewalls')
- Electronic attack intrusion detection and prevention
- Identification and authentication measures (e.g. username/password)
- Security markings with appropriate degrees of access e.g. restricted, confidential, top secret

2.1.3 Personnel

Personnel security is about managing the risk to staff or contractors exploiting their legitimate access to an organisation for unauthorised purposes:

- Identity checking and pre-employment screening
- Risk assessment procedures
- On-going security measures
- Security culture

2.2 Information and the Security plan

Security situations are likely to develop with very little warning and can quickly develop to an emergency situation affecting much of the hospital, it would be almost impossible to disseminate an action plan for staff to follow once the emergency is in full swing. It is therefore prudent to have a security plan in place to ensure members of staff know what actions they are to take in the event of an emergency situation, to protect themselves, patients and visitors. Security plans should be familiarised with staff and rehearsals or practical exercises should be conducted regularly to ensure the plan becomes embedded in a similar way that fire evacuation drills are common practice. Hospitals vary along a variety of metrics including size, location, funding, size of population served, nature of patients, and as such information needs to be collected to ensure that the Protective Security measures that are put in place are appropriate and proportionate. Money is always finite and health funding is declining not increasing (HOPE, 2014) therefore information needs to underpin the security plan, namely:

- Identification of the threats
- Setting priorities for protection
- Conducting a risk assessment

The data collected by the THREATS team in D2.1 suggests that by no means all EU hospitals conduct all of these tasks. Only 46% of respondents to the THREATS team reported that their hospital used a security assessment framework to assess physical facilities, and over a quarter of respondents were unsure (28%) (D2.1:16).

2.3 Response Planning

Like any other business, a hospital needs to have various levels of response planning in place. Response planning needs to cover many areas including:

- Business continuity plan

- Incident response e.g. response to Vehicle Bourne Improvised Explosive Device (VBIED), Roving Threat (known by many descriptors including marauding intruder and active shooter but should include firearms, bladed and improvised weapons)
- Communications plan (to alert and provide immediate instructions to staff and visitors within the danger area, as well as reporting out to media and the public as part of the Business Continuity Management Plan)
- Bomb threats
- Evacuation/ invacuation and shelter in place plan
- Search planning

2.4 Security Culture

In order for a security culture to enhance the protection of an asset it is necessary to have sufficient 'buy in' at appropriate levels. Communications need to be clear, succinct and ideally with 'at a glance' summaries so that staff at any level can access and understand them. Senior management support is vital: if the security culture is not seen to be embraced at the top level then it is unlikely to be fully effective at other levels.

Without the implicit understanding and compliance of staff within the organisation any programme of vulnerability reduction will inevitably falter. The importance of a security culture within an organisation in this context is very important. Without it many initiatives and safeguards will be ineffective. For example the wearing of security passes and challenge to those who are not is a fundamental part of personnel security. Most security initiatives and safeguards are defeated by personnel non-compliance with or failing to challenge others by proactive support rather than simple compliance.

2.5 Vulnerabilities

Vulnerabilities of the hospitals in the EU to terrorist attack bear many relations to the vulnerabilities of any crowded space. Hospitals are typically public areas that have many points of access and egress, day and night, and that actively encourage visitors (see D1.3 for further discussion of these points). The Work Package 3 team have been studying the San Raffaele hospital (OSR) in Milan to gain a deeper understanding of the vulnerabilities at a large general hospital like OSR. The initial results from a study of pedestrian traffic flow throughout the hospital on a typical working day demonstrate the density of population in specific areas of the hospital during a 10-hour epoch: a single access point to the hospital from the subway train/metro was assessed to have 40,700 crossings of the threshold and the most crowded areas of the hospital recorded 6,450 visits via a single access point while

other areas with multiple access points recorded 1,550 visits (see D3.1). This data illustrates how busy a large hospital can be on a typical day. The density of population combined with the ease of access and freedom of movement, compared to other potential targets that might yield the same level of impact such as transport hubs, the soft target nature of hospitals becomes more apparent.

2.5.1 Corruption

One area of vulnerability that has not been widely discussed in the forgoing THREATS publications is that of corruption. In his speech at the Anti-Corruption Conference in Prague in 2001, Vaclav Havel, the late Czech writer, philosopher, dissident, and statesman said:

> "[F]ighting corruption is fighting terrorism."

The presence of corruption is relevant both as an example of a poor security culture and also as a possible weak point for the exploitation of insider personnel threats by terrorists. The information asymmetry between patient and doctor, the large number of actors with complex interrelations and the provision of decentralised, individualised services typical of the Health Sector all provide opportunities for corruption (European Commission, 2013:25). This report found that corruption in the Health Sector was considered systemic in many (former) transition countries from Eastern and Central Europe, and that the:

> 'Czech Republic, Latvia, Croatia, Slovakia, Romania, Italy, Bulgaria and Greece are considered having a widespread corruption problem and seem to encounter more bribery in medical service delivery, procurement corruption and misuse of (high) level positions.' (ibid:9).

Savedoff and Hussman (2006) observe that the attitudes to corruption predict its presence far more so than other factors such as types of health system, funding and sophistication of health systems.

2.5.2 Number of Sector assets

The Health Sector is large, varied, and also hospital provision is uneven across MS. In 2010 according to HOPE (2014), in Europe there were on average 2.7 hospitals for 100,000 inhabitants, varying from 1/100,000 in Slovenia to almost 11/100,000 in Cyprus. The average number of beds per 100,000 people was 545, but again this varied from 273 in Sweden to 825 in Germany, and around 65% of these were acute beds.

3. Methodology

3.1 Research Approach

This report builds on D2.1, which reported a survey collecting data from personnel operating in the Health Sector of each of the 28 EU MS, (available at www.threatsproject.eu). A non-representative subset (a purposive sample) of respondents to the D2.1 survey were identified as potential participants in interviews for this report, with the aim of gaining some deeper insights. The sample was considered purposive because the sample group were identified from different EU MS and their professional roles ranging from hospital security manager, medical doctor or nurse to senior hospital manager. The desired participants were identified as being likely to have operational or tactical knowledge, requisite to their role and responsibility, within a hospital setting. Poor take up and availability from the initial sample necessitated a strategic re-think and the adoption of a somewhat more opportunity / purposive sampling hybrid. The final list of participants is at Appendix 1.

The final sample of twelve participants consisted of eleven medical practitioners and one disaster preparedness coordinator, who was originally a Registered Nurse. It is acknowledged as a sampling flaw that representation from all MSs was not achieved. Italy has been strongly represented because the research team were able to exploit an opportunity to interact with hospital practitioners during the Medical Response to Major Incidents (MRMI) course in Milan during June 2015, where the majority of participants were drawn from the Italian Health Sector. However, the Italian sample of four participants has been drawn from three separate hospitals.

3.2 Qualitative Approach and Purposive Sampling

A qualitative approach was selected because of the variation between EU MS in terms of critical infrastructure protection (CIP), demographics and quantity of hospitals, economics and political/strategic directive and involvement at government level. A simple quantitative approach would not have captured the variations between participants and therefore the value to this study may have been limited. Furthermore the limited take up of the D2.1 survey indicated the limited responses to trawling a wide sample group, the probability of a surge of responses seemed slim, further confirmed by the changes to the initial sample selection for this report.

Despite the somewhat opportunistic nature of the sample, each participant was selected against two key criteria: accessibility for the researcher and their suitability in having the requisite knowledge at work to participate. Other criteria for purposive sampling as described by Given (2008:697) were considered and participants were selected that were able to add value to the study. This was assessed through the their responses to the D2.1 survey.

3.3 Feasibility

It quickly became apparent that liaising with the sample group was going to be challenging due to lack of availability of this necessarily disparate and busy target group. Other challenges also emerged such as gaining authority to participate from senior managers and concerns regarding confidentiality and security of information. A series of contingencies to interview alternative participants was identified and an opportunity to conduct a group discussion at the European Society for Trauma and Emergency Surgery (ESTES) conference in Amsterdam was exploited during 11-12 May 2015. A further opportunity to liaise directly with suitable participants was exploited during the THREATS Project conference that was antecedent to the MRMI course in Milan. Additional interviews were conducted via Skype video call.

3.4 Ethics

EU CIP activity is fragmented (see D1.1) and therefore a disparity in the level of preparedness to terrorist attack and emergency procedures at hospitals was anticipated. In order to avoid disclosing potential soft targets due to weaknesses to the physical security and protection of the hospital facility or significant gaps in contingencies or procedures, personal or organisation embarrassment it was decided that all participants would be provided with a pseudonym to protect their personal and hospital identity to avoid publicising the vulnerabilities and sensitivities associated with a named hospital. The only visible piece of information would be the country/EU MS they are representing. A confidentiality statement outlining the measures and procedures to protect their identity was issued to each participant prior to being interviewed. A protected list of interview participants, complete with contact details has been collated and stored in a stand-alone facility as protectively marked material (PMM).

3.5 Interview Technique and Data Collection

Because operational and tactical concerns were not readily accessed by a common question pool two separate groups of questions were designed for the operational participants and the tactical/strategic participants respectively. Each of the question groups were devised from filtering or reducing a series of contributions from the wider THREATS team, with a view to examining the status quo in reference to the outcomes of the earlier deliverables, questions were designed to be open and elicit a wider response or trigger a discussion between the interviewer and the participant. The questions complete with a summary of responses is contained within the Findings Chapter of this report.

Interviewers produced contemporaneous notes that were collated for analysis. The use of digital recording devices, including the recording of Skype video calls, was disregarded because it did not support the ethical approach to the study and participants were more anxious about the unauthorised or accidental disclosure of sensitive information. Using contemporaneous notes enabled the interviewer and participant to review responses immediately and redact information as necessary. Final draft responses were word-processed and stored electronically, hard copy notes have been destroyed.

4. Findings

4.1 D2.1 Data Review

In the first instance further analysis was made of the data collected for Deliverable D2.1, with special reference to the information provided about Protective Security. In order to avoid over analysing the data this section will concentrate on aspects of the data not already reported in D2.1. There were 49 respondents to the survey in D2.1 and the MSs represented are shown in Figure 1.0.

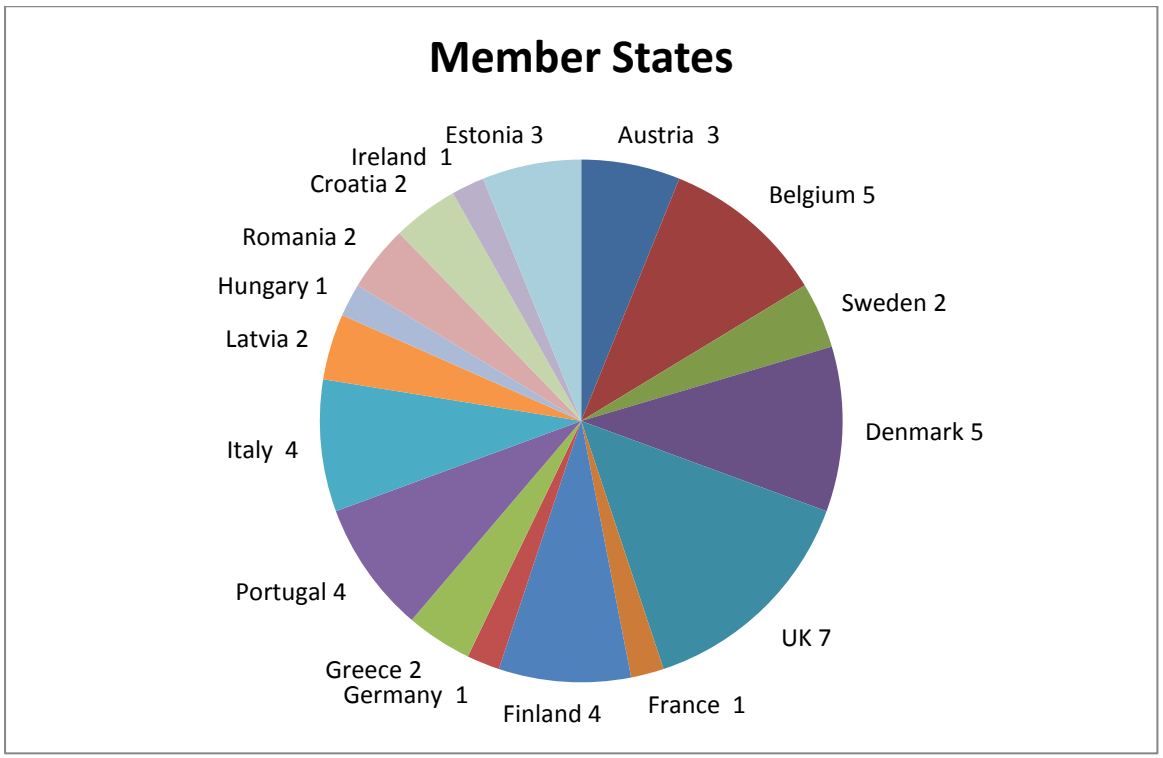

Figure 1.0: Member States represented in D2.1 number of responses

Ten of the 49 responses that can be attached to a MS are from the newer EU members (joined 2004 or later), and five of the 17 states represented are from such MS. In terms of security measures and equipment, there was a negligible difference between the newer and older EU MS in their responses (see Appendix 2 for table).

Furthermore three of the interview participants for this deliverable represented two of the newer members to the EU: two participants were from Slovenia, which joined the EU in 2004 and the third participant was from Croatia that joined the EU as recently as 2013. The interview responses from these three participants were similar to the remainder of participant responses, there were no single issues that made them stand out.

4.2 Strategic Level Interview Questions

Unfortunately the research team were only able to gain two strategic level interview responses. The main problem was identifying suitable participants that had been involved within the strategic level management of Health, the project team were exploiting relationships and points of contact at the operational level of the Sector and had hoped to develop additional opportunities that would provide strategic participants, but they didn't present within the timeframe of the research. The two strategic participants represented France (F1A) and Slovenia (SL2B), the interview questions and a summary of responses follow:

1. Are there any Central or Regional Government requirements/programmes to reduce the vulnerability of your Health Service/ Hospital from terrorist attack?

This question was designed to identify if a government level directive existed to provide top down guidance to the Health Sector and to identify if Health was managed as sector of CNI. F1A suggested the VIGIPIRATE strategy was the higher-level programme for reducing vulnerability of the Health Sector to terrorist attack. The response by SL2B was similar, describing the Ministry of Health working with multi-agency cooperation to run the Radical Awareness Network (RAN) that concerns hospital attacks, although SL2B concludes that he hasn't seen any output from this initiative.

2. Does your hospital, Health Service have a Corporate Board member, Chief Executive level person responsible for overall security including protective security and counter terrorism?

This question was intended to identify if Security/Protective security/Counter Terrorism was recognised as sufficiently important by the respective organisation to be directly overseen and accountable to either a corporate board member or Chief executive function. Answers to this question would aid in identifying "corporate buy in" and whether the culture of security and counter terrorism was embedded into the organisational culture and being driven from the top down. F1A described how his hospital is part of a structured organisation that is controlled and managed from a central body (Assistance Publique Hôpitaux de Paris) or APHP. A Group security officer is part of the APHP management structure and has the remit to liaise downwards to each local (hospital level) security officer and upwards to regulators or government. The response from SL2B was limited but suggested that security is outsourced and the Health Sector have limited involvement with security matters.

3. What area of management/ department currently manages the protection of your facility from terrorist attack?

This question follows on from question 2 and is intended to confirm or deny the allocation of management resource to preparing for terrorist attack. There was a significant difference between the French and Slovenian response: F1A suggested the local Head of Security managed the hospital's security needs whilst SL2B concluded that the Police are responsible for and manage security at the facility level.

4. Does your Health Service/ Hospital have regular contact with counter terrorist organisations regarding the reduction of your vulnerabilities to terrorist attack?

This question was intended to confirm the connectivity and level of liaison between counter terrorist organisations and the operational Health Sector. In France the liaison with counter terrorist agencies is not conducted at hospital level, SL2B went further and stated there is no contact with any agency at hospital level.

5. Does your Health Service/ hospital have and has it implemented training programmes specifically to reduce the vulnerability from terrorist attack?

This question was designed to identify if training activity is taking place to reduce the vulnerability to a terrorist attack. Both respondents denied any training activity. In France training activity is directed to responding to terrorist attacks elsewhere but in Slovenia there is no such training.

6. What performance management and quality assurance programmes are in place to support the vulnerability reduction programmes or other initiatives in reducing vulnerabilities?

This question was designed to identify if recognised 'best practice' or standard practices are being used to measure performance and reduce the vulnerability. In France nothing has been planned. The Slovenian response focussed on mass casualty response planning, which is tested once a year.

4.3 Operational/ Practitioner Level Interview Questions

Each of the 12 interview participants were able to answer the operational level questions, the questions and a summary of responses follow:

1. Terrorism has become a key feature of the security landscape across most sectors of industry and society. Can you describe the non-sensitive type of activity and measures that are now routinely conducted at your hospital?

This question was designed to identify if terrorism is actively discussed across all facets of the hospital staff and provide an indication if security is embedded within the culture. The responses from each of the participants were very similar, some responses conflate the hospital plan to respond to mass casualty events that occur elsewhere, the THREATS research has not yet identified any empirical evidence that

a hospital has a plan to respond to a direct attack against the hospital, which adds weight to the idea that hospital staff are not particularly familiar with security activity. IT2A from Italy claimed his hospital had planned for a terrorist attack and had included chemical, biological, radiological and nuclear (CBRN). The interviewer requested a translated copy of the plan, which is unlikely to be protected if it was intended to be invoked and enacted by the hospital staff, but he was unable to provide the evidence, which supports the previous comment relating to conflating emergency plans.

2. The 'roving threat' is considered a viable method of attack by terrorists with firearms or bladed weapons, similar to the Mumbai attack in 2008 and the Westgate shopping mall attack in Kenya in 2013. Can you describe how you and your colleagues would be alerted/ informed, how would you inform the public within the hospital and what actions you have been trained to carry out?

This question was intended to provide an indication whether practical measures have been enacted at the operational level and not just listed in documents. The collective responses were similar and included comments conflated with the hospital plan to respond to mass casualty events. It was immediately clear to the researcher that none of the hospitals represented by the respondents had a communication plan to alert staff and inform the public, beyond the statutory fire alarm. Some of the respondents suggested the alert mechanism was reliant very much upon word of mouth and one surgeon claimed it was likely to take the form of 'Chinese whispers' whereby rumours will leak into the operating theatre and the substance of the incident will not become clear until one of the theatre staff proactively call the switchboard or security desk. P1A from Portugal explained the hospital has a visible security team who are posted to each of the entry/exit points and they would likely be aware of a roving threat incident and be responsible for alerting hospital staff. There were no indications that any form of staff education and training takes place at hospital level.

3. When you first joined the staff at the hospital can you describe the process you underwent as part of the induction/joining process? Are you aware of any vetting or background checks conducted to validate your identity and qualifications? Can you describe the process that is carried out now?

This question was intended to identify the level of consideration applied to the vetting

and screening process. The respondents each described a process that often included periodic re-licensing for medical practitioners. The Portuguese process includes periodic examinations as part of the re-licensing process and all respondents explained that vetting was part of the overall process. The only variation in the responses was provided by IT4B from Italy who explained the transition from the University Medical School to becoming a permanent member of staff at a hospital, the onus is placed on the university to conduct the required vetting process and the hospital assumes the new member of staff has fulfilled all the necessary criteria. Each respondent provided details of the hospital induction process that included activity ranging from an online tutorial and test (requiring 100% pass mark) to an organized programme of lectures and presentations. UK1A from the UK suggested the emphasis was on clinical governance and fire safety with very limited information relating to security or public safety.

4. Does your hospital operate an access control/ID card system? Can you describe how the system controls your access to specific areas of the hospital and how you access areas not included on your permissions? What is the process if you lose your card?

The response to this question was varied: most of the responses indicate the use of an electronic access control system (swipe card) that enables the user to access relevant work areas and controlled by the permissions on their card. When asked about entering areas where they don't have access control permission the collective response was to gain manual access by calling a member of staff to facilitate access upon inspection of their identity card. Some of the respondents explained that they didn't have a technical access control system at their hospital, P1A said his hospital relied on identity cards being worn and access being controlled manually by the security team and hospital staff challenging people they don't recognize. IT3A from Italy provided a similar answer but explained the only area protected by access control was the radiology and operating theatre department that were protected by a simplex combination door lock. C1A from Croatia explained that none of the hospital doors were locked and access control to any area was reliant upon staff awareness. In the event of identity or swipe card loss all respondents, except for one of the Slovenian participants, claimed there were no punitive measures for card losses. SL1A stated that a €50.00 charge was issued for each card replacement though it was not clear whether the charge was punitive or to offset administration costs.

5. If you encountered an unknown person in a service area of the hospital and subsequently needed support from the security team, what is the quickest way to raise the alarm and how long would it take for the response to arrive?

Interviewers were encouraged to include discussion about the visible presence of security personnel – how often do you see security or police staff whilst moving round the hospital during the quiet hours? Additional useful information could include the use of CCTV surveillance and how effectively it is monitored. Each of the respondents were confident they could summons the assistance of the hospital security team by calling the designated internal telephone number and they also explained they were encouraged to challenge unknown persons. P1A was able to include the Policeman permanently stationed within the hospital Emergency Department, as part of his call for assistance.

6. If a member of the public brought a seriously injured family member to hospital and drove a commercial vehicle (van) directly to the front door of the Emergency Department and left it unattended, what would be the likely response and by whom?

This question was designed to examine the vehicle access to the hospital building – hostile vehicle mitigation measures, buffer zones etc. and the subsequent response by security team and/or police, to include the actions likely to be taken if the vehicle is elevated to 'suspicious'. The UK response was limited because UK1A worked in the operating theatre each day and didn't know what would happen if this scenario occurred. F1A described a situation outside of the Emergency Department where members of the public routinely park in the ambulance loading bays with little regard for emergency access. The other respondents aligned the control of this key area to the triage nurse whom would be on duty close to the ambulance access to the department and it would be the role of the triage nurse to control and keep this area clear of unauthorized vehicles. None of the respondents gave any indication that they were aware of the potential threat from hostile vehicles.

7. Can you describe how electronic information and the information technology (IT) system are utilised at the hospital? Can you think of 3 things that help keep the system secure?

The responses to this question were varied but most of the participants explained the IT governance was the responsibility of the IT department. In France the IT policy is

driven from the top at APHP level and cascaded down to hospital level. The other respondents explained that IT governance was managed at hospital level. The Portuguese participant seemed to be controlled least and was able to use personal mobile storage devices to store data and was able to remotely access the hospital IT system, though he couldn't amend data unless logged on at a hospital terminal. SL1A expressed frustration with the IT system at his hospital, commenting that there are currently four discrete systems for conducting different activities and he often has difficultly effectively managing complex patients across multiple IT systems. The practice of changing passwords and personal log-on details regularly seemed to be a common theme across all responses.

8. If you needed to conduct open source research via the hospital IT system, how good is the Internet connectivity? Can you save information to a portable storage device so you can use it at home and in other departments of the hospital?

Designed to identify if internal/intranet is separate to external/internet system and the likelihood of cross contamination – safeguards to protect against virus/malware via non-accredited portable devices.

Although F1A described the IT policy as a top down approach from APHP it was surprising to learn that hospital staff could access the IT system and transfer data between the internet/external and intranet/internal system via personal storage devices. The other respondents described a variety of measures: in the UK hospital 'safe sticks' (USB) are issued to staff for data transfer and only prescribed mobile storage devices are permitted to be connected to the internal IT system. SL1A provided a similar answer but suggested any device could be used so long as it had been screened/checked by the IT department. All respondents reported that the Internet and intranet were separate systems and that their respective hospitals provided a good level of internet access.

9. If your hospital uses protectively marked material (PMM) protocols, such as confidential, can you describe the different levels and what they mean to you?

Designed to identify if PMM protocols are used, whether staff understand what they actually mean and how the measures are implemented for soft/electronic and hard copy PMM.

The responses to this question were very similar and each participant explained they were compliant to patient confidentiality laws but were not familiar with any other protocol. SL1A and P1A explained that data access permissions were aligned with staff role, responsibility and grade.

4.4 ESTES Group Discussion

A series of questions were used by the THREATS representative to provide discussion points to the collective audience of at least 50 healthcare professionals from across Europe and with a small number of representatives from the USA. Although the group discussion and data collection methodology was less scientific than originally intended, the results provided a useful insight antecedent to the primary interview programme. Overall, four questions were asked:

1. Who is responsible for security at your hospital?
2. What area of management/department currently manages the protection of your hospital?
3. Does your Health Service/ hospital have regular contact with counter terrorist organisations?
4. Does your Health Service/hospital have regular training for responding to an ‘active shooter’ or terror attack at the hospital?

The audience was asked to respond by contributing to the discussion and sharing their own experiences. The results indicate that the large majority of the audience did not know the answer to questions 1-3, only the contingent from the USA were able to confirm that they had participated in any form of ‘active shooter’ training or education.

5. Conclusions

Although the strategic level responses were constrained to two MSs it was clear that work is being conducted at strategic level in France with VIGIPIRATE and Slovenia with RAN, however the effect of both programmes doesn’t seem to have filtered down to the hospital level. The THREATS team have not found any evidence to the contrary and both strategic participants report the absence of training or testing the hospital response to a terrorist attack at the hospital.

At the operational level hospitals have applied much effort and resource to responding to mass casualty events that occur off-site, the plans are familiar to practitioners. Many of the operational community conflate these contingencies with a response to a direct attack by terrorists at the hospital. The impact of a terrorist attack at a hospital is likely to be measurable by the number of casualties, disruption and physical damage to the hospital facility, but the wider reaching effect to the Health Sector network at the regional and national level are not immediately obvious but likely to be significant (see D1.3 for details relating to the impact on societal function from the degrading of healthcare).

The absence of lockdown procedures to reduce the freedom of movement of a roving threat indicates that Health Sector managers are less aware than their peers in other Sectors of the potential threat, especially as large commercial estates are now implementing these types of measures in addition to fire safety procedures. Other simple but potentially life-saving measures could also be introduced, such as in-vacuation whereby staff are trained and rehearsed to evacuate to designated safe zones to avoid people potentially evacuating into the path of a roving threat. Hiding at your place of work, also known as 'shelter in place' can be an effective way to reduce the risk of becoming exposed to the danger but all these measures are complimented by an effective communication plan. It is vital that staff, patients and visitors are told exactly what is happening and provided with some simple instructions that can help them to stay as safe as possible until the threat has been removed or they have been rescued. Authorities in the USA, where a comprehensive programme within the Health Sector is underway, promote much of this information. Some efforts are being made in the UK though practical training and exercising is still lacking but government sponsored guidance is now available and is known as 'Run Hide Tell' and is available as a short leaflet called 'Recognising the Terrorist Threat' (NaCTSO, 2014).

Cyber security featured as a dominant consideration within the field of Critical Infrastructure Protection (CIP) (see D1.1) but the strategic level work doesn't seem to have been translated into best practice at the operational level. The interview research for this report has identified that some routine measures are in place at the operational level but there is no obvious directive beyond the type and level of IT security that is mirrored by domestic household users. The THREATS team recognise the potential vulnerability to cyber attack and although the vulnerability includes the theft and misuse of personal data, the significant threat relates to the control of vital services and procedures that are governed by IT systems, often from remote controlling stations. The physical security of the IT servers and

infrastructure remains important, but often business continuity management plans will include the back up of data to off-site server facilities. The potential to be attacked from within due to hacking seems to be considered less but the potential disruption at every level of the Hospital must not be overlooked.

Unfortunately the issue of corruption was not included in the interview questions, though the response to such an emotive topic are likely to have been negligible. However the literature provides adequate evidence that corruption exists within the Health Sector and is considered systemic in many (former) transition countries from Eastern and Central Europe. Furthermore the EC consider the existence of a corruption problem that a report was commissioned to investigate (European Commission, 2013). Corruption poses a vulnerability to the security of the Health Sector because effective security cannot coexist in a culture that is corrupt. The problem should be of concern to all EU MSs because of the vulnerabilities relating to interdependencies, as discussed in D1.2 and D1.3, a 'chain is only as strong as the weakest link'.

6. References

Berger, R. (2007) *Trends in European health care: how to create value in a dynamic environment.* Available from: http://www.rolandberger.com/media/pdf/rb_press/RB_Trends_in_European_healthcare_20070901.pdf [Accessed 15 April 2015].

Centre for the Protection of National Infrastructure (2010) *Protecting Against Terrorism.* 3rd ed. London: HMSO.

Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1426673043420&uri=URISERV:l33275

Economist Intelligence Unit (2015) [online]. Available from: http://www.eiu.com/industry/Healthcare [Accessed 14 April 2015].

European Commission (2013) *Study on Corruption in the Healthcare Sector HOME/2011/ISEC/PR/047-A2 October 2013.* Luxembourg: Publications Office of the European Union.

Given, L. (ed.) (2008) *The Sage Encyclopedia of Qualitative Research Methods.* Vol.2. Thousand Oaks: Sage.

Homeland Security (2010) *Healthcare and Public Health Sector-Specific Plan An Annex to the National Infrastructure Protection Plan.*

HOPE European Hospital and Healthcare Federation (2014) *Hospitals in Europe Healthcare data 2012.* Brussels: Hope Publications. Available from: http://www.hope.be/03activities/quality_eu-hospitals/eu_country_profiles/00-hospitals_in_europe-synthesis.pdf [Access 16 April 2015].

National Counter Terrorism Security Office (2014) *Recognising the Terrorist Threat*. [online]. Available from: https://www.gov.uk/government/.../**recognising-the-terrorist-threat** [Accessed 07 August 2015].

Nikolic, I.A.& Maikisch, H. (2006*) Public-Private Partnerships and Collaboration in the Health Sector: An Overview with Case Studies from Recent European Experience.* Washington: The World Bank.

Protective Security Requirements [n.d.] *Definition of physical security* [online]. New Zealand Government. Available from: https://www.**protectivesecurity**.govt.nz/...**security**...**security**.../**definition**-o [Accessed 24 August 2015].

Savedoff, W. D. & Hussman, K. (2006) Why Are Health Systems Prone to Corruption? Chapter 1 in *Global Corruption Report 2006: Corruption and Health.* London: Pluto Press and Transparency International. Available from: https://www.transparency.org/whatwedo/publication/global_corruption_report_2006_corruption_and_health [Accessed 15th April 2015].

7. Appendices

Appendix 1 to THREATS Report D1.5

The list of interview participants showing the allocated pseudonym, country, hospital level role and level of interview participation:

Pseudonym	Country	Role	Level of participation
S1A	Sweden	Disaster Preparedness Coordinator	Operational
UK1A	United Kingdom	Senior Consultant Doctor	Operational
F1A	France	Senior Consultant Doctor	Tactical & Operational
SL1A	Slovenia	Senior Surgeon	Operational
SL2B	Slovenia	Senior Military Surgeon	Tactical & Operational
C1A	Croatia	Senior Surgeon	Operational
P1A	Portugal	Senior Surgeon	Operational
IT2A	Italy	Doctor	Operational
IT3A	Italy	Senior Surgeon	Operational
IT3B	Italy	Surgeon	Operational
IT4A	Italy	Doctor	Operational
IT4B	Italy	Doctor	Operational

Further analysis of hospital questionnaire data:

	Total Sample	Newer MS
Restricted access to sensitive areas	84%	80%
Alarm system to detect (attempted) entry	61%	60%
Specific training of security personnel	58%	60%
Gate control system for vehicle access	66%	80%
CCTV	68%	70%
Screening of visitors outside visiting hours	42%	40%
Suggest screening visitors at all times	21%	20%