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

Report No: D 3.4

A reference model of a protected hospital proposing countermeasures for mitigation, preparedness, and response against terrorist attacks, including: threat scenarios, “as-is” system simulation, countermeasures, “to-be” system simulation, indicators, and evaluation.

Version: 1.0

Date: 19 June 2016

Authors: AG, JF, WC (INSA Lyon); RF, DB, GSF (OSR); SC (HA)

Approved by: CA

Contents

Executive Summary

This deliverable builds on D3.3 in order to propose, evaluate, and benchmark counter measures that a hospital may consider in order to protect itself as a potential target with regard to a variety of terrorist attack scenarios. The terrorist attack scenarios that had previously been proposed in D3.3 were analysed in terms of their stakeholders and effects, and countermeasures were suggested with regard to the as-is security system. The cost effectiveness analysis of each was conducted as described by Cellini and Kee, 2010, and preferred countermeasures were therefore identified in terms of the ratio of the cost to the health benefits arising. Apart from cost effectiveness analysis, all the other instruments selected in the previous deliverables (D3.1, D3.3) to assess and benchmark the different scenarios and countermeasures (SVA, non-quantifiable criteria analysis) have been used during the scenario studying process and are here exemplified.

The scenario study process consisted of a table top simulation for each scenario, to confirm plausibility, verify consequences, identify vulnerabilities and possible countermeasures. Whenever possible the scenarios were also studied by modelling and simulations according with the selected tools (IDEFO and CPLEX see D3.1). Nine scenarios were considered, as suitable and interesting to be studied according with the scenarios selection and the ranking procedure (see D 3.3). These were: an IED second strike; an IED attacking the electric grid; an IED attacking the medical gas supplies; an attack contaminating part of the hospital with stolen nuclear material; two different bio terror attacks; a cyber-attack; an attack on the animal lab and a gun attack on a VIP patient.

The results were:

1. There was no single countermeasure that covered all attack types, i.e. effectiveness was somewhat scenario specific. Despite this, the increase of security personnel and the training in emergency management and security of the personnel, emerge as possible transversal countermeasures.
2. Some of the attack scenarios were best mitigated by physical security measures to reduce the likelihood of successful access, eg the theft of bio hazards; others were better mitigated by the provision of a back-up supply eg an attack on medical gas stores.

Modelling and simulation of different scenarios as well as the scenarios study process involving all the hospital different stakeholders with the comparison of the “as is” and the “to be” models were found to be very effective tools for the selection, evaluation and benchmark of countermeasures to increase the protection of a hospital

1. Introduction

OSR is a large-sized Italian hospital. It is composed of 11 buildings, 49 care units, 4 external access gates, 1 subway access, 1 hotel access and 10 parking accesses. Closing this hospital, in case of the terrorist attack, is really problematic because of its large size and its multiple accesses. Because of the great number of buildings of this hospital, it is difficult to find a global solution to handle the different emergency situations. Therefore, in this deliverable, we will study the different scenarios and propose several dedicated countermeasures to deal with the different emergency situations, following our vulnerability approach (see deliverable D3.3).

Regarding to the different possible countermeasures, we classify them according to the 3 pillars of physical security, personnel security and information security (as defined in WP1):

- Physical resources (infrastructures and equipment): mobile barriers, access control systems, Geiger sensors, CCTV surveillance, electricity generators, mobile oxygen tanks, antibiotics' stockpiles, 'paper kit' systems, etc.
- Human resources: Security guards, employee training on security, etc.
- Information resources: communication (e.g. levels of alert), emergency management plans, governmental office information (e.g. Home Affairs information about a new employee), etc.

The hypothesis that the threat occurs during a year is retained (next occurrence), so countermeasure investments are calculated with an amortization of one year.

2. Approach

In this section, the as-is system and the related countermeasures will be presented. The effects of the countermeasures will be evaluated by a cost-effectiveness analysis. Cost-effectiveness analysis is a method for assessing the gains in health relative to the costs of different health investments. It supports the vulnerability assessment step (fifth step) of our vulnerability assessment approach (see the deliverable D3.3). In other words, cost-effectiveness analysis is a technique that relates the costs of an investment to its key outcomes or benefits. It is a method to identify neglected opportunities by highlighting investments that are relatively inexpensive, yet have the potential to reduce the disease burden substantially (Hutubessy et al., 2001). One of the most important steps of the cost-effectiveness analysis is to calculate the cost-effectiveness ratio. The cost-effectiveness ratio is used to determine the most suitable strategy. The calculation of the cost-effectiveness ratio is to divide the cost of an investment in monetary unit by the expected health effects produced, such as the number of patients saved. Regarding the effects, the infrastructure damages are not considered, because most of the time this information is not currently known. The following four steps are the main tasks of the cost-effectiveness analysis (Cellini & Kee, 2010):

- Decide whose costs and effects should be recognized. Almost every organization consists of several stakeholders. Therefore, the costs and the effects ultimately affect certain groups of people. In light of this, determining whose costs and effects should count is an important consideration (see the risk assessment step in the deliverable D3.3).

- Identify costs and effects. This step is to categorize the costs and effects that will be taken into account in our analysis. Even though not all costs and effects can be known, a reasonable effort should be made to identify those that will have the most important implications on the policy.
- Monetize costs and quantify effectiveness. After identifying all costs and effectiveness, this step is to assign each cost a value and quantify the effectiveness.
- Compute a cost-effectiveness ratio. Usually, the cost-effectiveness ratio can be calculated as: cost-effectiveness ratio = costs of investment/health-effects produced, knowing that infrastructure costs are not considered.

3. Scenario studies

In the following paragraphs, we will first explain the stakeholders who will be taken into account in different scenarios and then we will identify the costs and the effects of countermeasures on stakeholders. In several of the scenarios, evacuation of personnel is required and the internal emergency management plan is used as an information resource for countermeasure in these cases.

The scenario study process consisted in a *table-top* simulation, called Threat Scenario Generator (TSG) for each scenario with the OSR WG (the TSG is also described in previous D3.3). The TSG containing all assessments is in the accompanying excel file Threat Scenario Generator for this Deliverable 3.4.

This study served the purpose to confirm plausibility, verifying consequences, identifying vulnerabilities and possible countermeasures. Whenever possible the scenarios have also been studied by modelling and simulations according with the selected tools (IDEFO and C-PLEX– see D3.1), focusing mainly on cost-effectiveness analysis. The criteria used in the TSG to perform each scenario study are reported in Table 1 below.

Table 1 - Criteria of the Threat Scenario Genreator table (see *Annex 1)*

Attractivity	**Interest to hit**
Terrorist Profile	**Simple identikit of attacker**
Motivation	**Political, social or ideological drive**
Scenario attack likelihood	**Relative % of frequencies base on actual dataset available (see Annex 1 for references)**
Action/process	**Process flow of simulated terrorist events**
Type of damage	**Simbolical, physical operative and managerial effect**
Resilience: strenght/weaknesses	**Procedures in place and plans for prevention or mitigation**
Countermeasures (3x3 level and type)	**Countermeasures suggested for physical, data people type combined with prevention alarm and protection levels**

For the scenario 1 of the second strike (deliverable D3.3, page 20), people are killed in the emergency department, patients will be evacuated and the emergency department will be closed. The hospital will have a human loss and an operational loss. Therefore, the hospital administration, the patients, and the staff are the stakeholders who will be taken into account. Since we propose using human resources (i.e. security guards) to avoid the second strike event, the salary of the security guard is the cost of the countermeasure. Without the second strike, OSR on one hand can save lives and on the other hand can receive patients injured by the terrorist attack at the airport and furthermore can keep its activity running. So, we will consider the money gained by saving lives and by receiving patients as the effect. This type of scenario has happened in past years for example in Mosul (Iraq) in 2005, when a suicide bomber detonated a device in a hospital that was treating the people earlier injured in the day, killing five people and injuring another twelve (CNN, 2005). In 2008 in Ahmedabad, (India) there were a series of blasts at hospitals, where the injured people were treated after precedent blasts in the city. Terrorists killed 29 people and injured 88 others (CNN, 2008).

For the scenario 2 of a VIP killed in an operating room, just one person dies (the VIP). The financial loss is caused by the death of this VIP and the reputational damage that ensues; the reputational damage and consequent loss of business could be substantial. So, the stakeholders which we will consider are the VIP and the hospital administration. For the countermeasures, we propose to use security guards for personnel security, and a biometrics access control and a reinforced door as physical security. Therefore, the costs are the salary of the security guards and the money paid for the acquisition of the material resources. The effect is the money we may save by using countermeasures. This type of scenario has historical precedent. In 1996 an IRA related terrorist gunman fired at a politician at the Royal Belfast Hospital. In 2006 in Khulna (Bangladesh), a group of five men threw a bomb at the bed of a politician from the ruling party (Mofis Biswas) and killed him, injuring two other people in the attack (see deliverable D1.3 for further detail on these attacks).

For the scenario 3a of electric grid failure (deliverable D3.3, page 21), the stakeholder which will be taken into account is the hospital administration and the patients**.** For the countermeasures, we use material resources (i.e. mirror electricity generators). So, we will consider the cost of the electricity generators. The effects consist of two parts: the operational loss avoided by keeping the buildings open and the evacuation of patients to external hospitals avoided.

For the scenario 3b of medical gas failure (deliverable D3.3, page 23) where a former employee destroyed the hospital medical tanks, the stakeholders which will be taken into account are the patients and the hospital administration. For the countermeasure, we will use material resources (i.e. mobile oxygen tanks). So, the cost of the countermeasure is the money paid for the mobile oxygen tanks and their liquid oxygen bottles. In this scenario, the financial loss can be caused by the ICU closure and the possible deaths of patients. Therefore, the measure of effect is the lives and money we can save by using the countermeasure. Regarding this scenario, former employees attacking previous employers and their hospitals, are known to have occurred. In 2012 a former employee of the Triulzio Hospital in Italy, hacked the IT systems provoking major disruption, for personal revenge (Milano Cronaca, 2012).

In 2015 a man shot a doctor at the 'West Texas Veterans' hospital, and turned the gun on himself. He was a former clerk of the clinic (The Guardian, 2015).

For the scenario 4 CESIUM 137 threat (see deliverable D3.3, page 24), we should evacuate patients and employees, so the stakeholders which we will take into account are the patients, the staff and the hospital administration. We use the human resources (i.e. personnel security, e.g. security guard), and material resources (i.e. physical security, e.g. biometrics access control, Geiger detector, and the CCTV surveillance i.e. Closed Circuit Television surveillance), for the countermeasures. So, the cost is the salary of the security guards, and the cost to install equipment. The effects are the evacuation time saved by using the countermeasures, and the operational gain obtained by avoiding the emergency department closure. Although there are not yet documented instances of CESIUM 137 being stolen to be used as a weapon, there are instances of nuclear material being stolen quite easily. On September 13, 1987, two thieves entered in a private radiotherapy institute in Goiânia (Brazil) and partially disassembled the tele-therapy unit, and exposed the CESIUM 137 with major personal injuries, irradiation of other people and evacuation of the area (International Atomic Energy Agency, 1988). An example linking hospitals, nuclear material and terrorism is that of the event in the Hospital of Budennovsk in Russia in 1995. The hospital was stormed by Chechen rebels and the CESIUM 137 was recovered by terrorists from X-Ray machines, to be used in a radiological terrorist attack (Ganor and Halperin-Wernli, 2013).

For the scenario 5 of the cyber-attack, we will consider the patients and hospital administration. There are three information security resources used as countermeasures, 'paper kit' system, bar-code system, and net servers. A human resource is used as countermeasure for the server maintenance and backups. The cost is the money used for 'paper kit', bar code system, and the duplication of net servers with their maintenance. The effect is the money saved by using our countermeasures, preventing a possible hospital closure during five days. Regarding the cyber-attacks in 2014 only, almost 50,000 attacks occurred across more than 700 systems, and some 375 organizations were compromised (Norse, 2014). In 2009, the Carrell Clinic in Dallas (Texas) suffered a computer intrusion, the hacker installed malicious software all over the Carrell Clinic, including the systems that contained confidential information, and others systems which controlled the buildings' air-conditioning. The hacker could have harmed patients, and he could have damaged drug stocks, if he had turned off air conditioning during Texas's hot summer months (Network World, 2009).

For the scenario 6 of the attack of the animal experiment laboratory, the stakeholder which we will take into account is the hospital administration. In this scenario, we propose two types of countermeasures: using physical security resources i.e. a CCTV surveillance system, and a security guard as personnel security / human resource. The cost is the money paid for these countermeasures and the effect is the money we can save by using these countermeasures regarding hospital efficiency related to applied researches in medicine. Some relevant cases of attacks of animal rights activists have been found in Milano: the Milano University Pharmacological Department in 2013 (Understanding Animal Research, 2013);
and the San Raffaele Hospital in 2012. In 2009, an animal rights group stirred controversy in Utah (US) after one of its activists infiltrated in the State University's

Biomedical Research laboratory, used hidden cameras to spy on the research activities and to document what it claims is abusive treatments of laboratory animals. In 2012, a group of animal rights activists chained themselves at the location where some macaques were lodged, with the intention to obtain media attention and some internet information diffusion (Fierce Biotech, 2009).

For the scenario 7a of SARS (see deliverable D3.3, page 25), the stakeholders who will be taken into account are the people who may get infected by SARS in the hospital and the hospital administration. The cost is the money used for physical security / material resources (i.e. a biometrics access control, the CCTV surveillance system), the human resources (i.e. a security guard), the information resource (Home Affairs investigation), and the effect is the number of people who are protected by using the countermeasures, because it is quite difficult to estimate an exact number of casualties for an epidemic in a big city as Milano. A second effect is the gain obtained by avoiding the hospital closure required by an epidemic.

For the scenario 7b of bacillus anthraces attack, we will consider the people (staff and patients) who may get infected by bacillus anthraces, and the hospital administration. The cost is the money used for countermeasures, i.e. physical security /material resources (anthrax spore sensors, CCTV surveillance system, and the antibiotics to treat infected people). No human resource is used as countermeasure, because the Anthrax spores come from an external source. The effects are the number of people who do not get infected by using the countermeasures, and the gain obtained by avoiding the hospital closure required by a contamination. Regarding previous biological attacks, in 1964, a physician stolen “Shigella Dysenteriae” toxins and “Salmonella Typhi” bacteria in the Japan’s National Institute of Health. The malicious dissemination was made via sponge cake and other food sources, and it caused 400 sick persons and 4 deaths. In 1996, a clinical laboratory technician of a Hospital in Dallas (Texas), used “Shigella Dysenteriae” toxin of type 2, simply acquired from the clinical laboratory of the St. Paul Medical Center where she worked. She contaminated pastries in the office break room, and she infected 12 of her co-workers (Gaudioso and Salerno, 2009).

Table 1 presents the value of the related countermeasures. The percentages of the successful effect of the various countermeasures will be qualitatively and individually estimated for each scenario.

Table 1 value of the related countermeasure (in Euros)

Average annual salary for permanent employee	27,847
Salary of a temporary worker per hour	40
Turnover of one patient per day	528
Electrical generator for one building	200,000
Mobile oxygen tank with 6 liquid oxygen bottles for a ICU	12,000
Six liquid oxygen bottles for an average duration of 6 hours	600
Financial loss because of the Death of one person	1, 000,000
Cost used for evacuation of one patient by ambulance	21
Shared CCTV surveillance	29,278
Biometrics access control system	450
‘Paper kit’ system for 49 care units	23,520

Bar-code system for 49 care units	43,120
Duplicating 4 net servers with maintenance	43,847
Anthrax sensors with daily biological test for 1 years	158,900

Part of the proposed countermeasures have been already implemented in OSR at the time we write this deliverable (security guards, mobile oxygen tanks, etc.) as a result of the toolkit produced in D1.6. For a more accurate cost/benefit analysis, we have not considered this result in our investigation.

Please note that the scenarios selection according to the type of terrorist action and motivation will be better delineated in D 3.5.

3.1 Scenario 1: Second strike

The second strike scenario is the one selected by the THREATS Consortium to be best investigated. This is for several reasons:

- It is a conventional scenario, very like to happen (so far unconventional, the "NBCR" attacks are very limited).
- It has been implemented in different settings in previous events.
- It gives the possibility to study in depth some physical vulnerabilites and possible countermeasures related to open access (probably the most relevant vulnerability of hospitals).
- It gives the possibility to analyze both the External EMP and the Internal EMP, and the need of eventually merge them, and to come up with solutions how to pass from « as-is » system to « to-be » system with more resilient plans.

3.1.1 Scenario

1) A first terrorist strike occurs in Linate Airport (Around 08.00 am, a bomb explodes in the main terminal killing 14 people and injuring more than 100 others, similar to the Zaventem airport attack in 2016). 2) The emergency plan in Linate Airport is activated. 3) The OSR is alerted for eventual massive influx of injuries (around 08.15) and it activates its external emergency management plan (08.15 alarm phase, 08.30 red alert when the first green patients spontaneously arrive). 4) While managing to clear the ED (around 09.00 am) from the "non-disaster patients", a private car pretending to come from the scene brings a patient to OSR Emergency Department. 5) The patient is triaged as green and while reaching the green area blows her/himself up revealing to be a suicide bomber. He severely injures some staff and kills 3 persons (Triage Officer, Triage Nurse, and the Hospital Disaster Manager). 6) The ED (Emergency Department) is in chaos: no leadership, triage and green area are severely damaged. 6) The activation of the internal emergency management plan is decided (see annex 1) and the OSR Emergency Team arrive to check the security and secure the whole block C. 7) The same strike has been carried out in some other big hospitals in Milano. The Milano Emergency Management System do not know where to send the severely injured patients from Linate Airport and how to rescue the ones inside the attacked hospitals. 8) The OSR injured people are sent to other care units located at the same level near the Emergency Department, i.e. the red patients are sent to the Intensive Care Unit and yellow and green patients go to the ambulatory care unit, according to the internal emergency management plan.

3.1.2 As is system simulation

For the second strike scenario, there are three steps. First, the regular patients must be treated in the emergency department. Second, the emergency department receives the first patients from Linate airport. Third, all the patients and staff must be evacuated out of the emergency department, because of the second strike. We suppose that, at period 1, the attack at the airport begins, and there are still 22 regular patients (3 red patients, 9 yellow patients, and 10 green patients) at the emergency department which need to be treated. During the treatment of these 22 regular patients, the emergency department only accepts new patients who are injured by the terrorist attack. At the same time, 10 green patients injured by the terrorist attack at the airport, arrive at the emergency department by cars.

We hypothesized that, at the beginning of period 2, there is a second strike at the emergency department. The second strike arrives in the main hall of ED near the waiting room for green patients. The employees who are in hall to receive patients, are killed (namely the anaesthesiologist on duty, the nurse, and the manager). Red and yellow patients with staff (6 surgical teams: 3 of 5 people and 3 of 3 people) are protected by the walls. Half of the green patients and employees (1 physician and 1 nurse) in visiting rooms, are injured. At the beginning of period 2, the numbers of red patients, yellow patients and green patients, are 3, 9 and 20 respectively. The injured staff should be evacuated to other units, as well. So, the total number of people who need to be evacuated is 34 (3 red patients+9 yellow patients+10 regular green patients+10 green patients injured by the terrorist attack at the airport +1 physician+1 nurse =34). Here, the uninjured staff can evacuate the patients and the injured employees. All the evacuated people will be transferred to safe units in OSR. The objective of the terrorists is that the ED is out of order, and cannot receive patients from the Linate airport. OSR is the nearest hospital to the airport.

Since the resources are enough, at period 7, all the patients have been well evacuated. Figure 1 shows the waiting patients to be prepared and the number of evacuated patients. The horizontal axis represents the periods and the vertical axis is the patients' number. There is no patient waiting for transportation. From this figure, it can be found that the bottleneck activity is "prepare patients" (see annex 1). From period 4 to period 6, 9 patients (maximal evacuation capacity per period) have been evacuated to other units per period. At period 7, the last 7 patients have been safely evacuated.

We suppose that three people will die because of the second strike. The human loss for the death of the employees are 3,000,000 (3 * 1000000) Euros (Suddle, 2009). We hypothesis that injured patients are cared for in OSR, and there is no extra cost. The ED is closed for 2 weeks to be repaired, so the operational loss is 1,286,208 (1286208=174*528*2*7) Euros, according to 63 500 emergency admissions per year and a turnover per patient of 528 Euros. The total loss is 4,286,208 Euros.

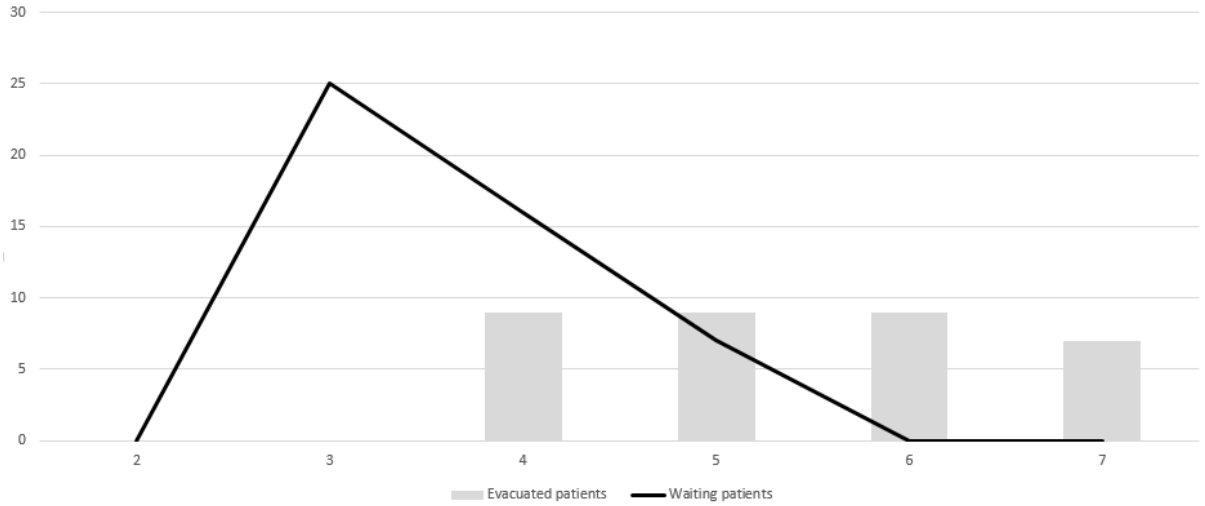


Figure 1: The number of waiting patients to be prepared and the number of evacuated patients (as-is system)

3.11 Countermeasures

Scenario 1 Second Strike	Physical	Data	People
Prevention	Metal detectors, vehicle barriers, locking doors.		Training in emergency management and security of the medical and non medical personnel
Alarm		Early warning system between the Police Forces/Counter-terrorism and the in-hospital security staff	Plan for a scalable increase of security according with a warning
Protection	Possibility to lock/shelter in the ED from all the entrances (if possible the whole hospital).	Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Increase the number of security staff Establish on demand provision of security staff with contractors. Contingency plan. 1) Procedure to increase the security: a) avoid access to people to the ED: no vehicles should enter the ED gate (even ambulances have to be offloaded at the gate and personnel goes to take the patients; b) all the patients should be checked for guns/explosives at the gate; 2) security planning starting from integration between the internal and the external security services ; 3) Contingency planning according with the possible threat of a terrorist attack and the event of an internal emergency + an external

			one 2c) a armed security staff must stand out of the hot room ready to shoot

In order to avoid the second strike, security guards can be employed. In the best case, we can employ security guards to protect the emergency department at three points. The first one is at the entrance of the ambulance parking point. The guard here can check if the people coming to emergency department carry weapons with them or not. The second one is at the entrance of the emergency department. If the false patient uses weapons of destruction at parking entrance and still wants to get into the emergency department, the guard at the entrance of the emergency department will shoot the terrorist. The third one is at the exit point of the ambulance parking. The main duty of this latter guard is to make sure that no one enters the ambulance parking by the exit point during the emergency management plan. Some mobile barriers can also be used to prevent a car pushing through the control points. In total, we need at best 3 security guards to protect the aforementioned 3 points. But, we can also just employ 2 security guards (emergency entrance and parking entrance points) or 1 security guard (emergency entrance point). The financial cost of employing 1 or 2 security guards is less than the cost of employing 3 security guards. But the effects of employing just 2 or 1 security guards decrease as well. So, we have three different countermeasures, employing 3, 2 or 1 security guards to protect the emergency department. In this scenario, we could take into account some metal detection devices to control the incoming people, but this seems difficult regarding the environment of injured people. No metal detection gate or mobile sensor can be used, since the ambulance, stretcher, and the wheel chair are made of metal.
The external emergency management plan which defines the hospital organization to face mass casualty events, is updated in order to integrate the security check activities.

3.1.3 To be system simulation

Under the situation of the to-be system, the regular patients can be treated and the emergency department can receive the patients injured at the airport, by activating the external emergency management plan (see annex 2). Here, we suppose that the emergency department can receive at most 100 patients. From period 2 to period 6, 20 patients (3 red patients, 5 yellow patients, and 12 green patients), will be transported to the emergency department per hour. At the end of period 22, all the patients will be well treated. Figure 2 presents the number of treated patients per period. The horizontal axis represents the periods, the vertical axis the patients.

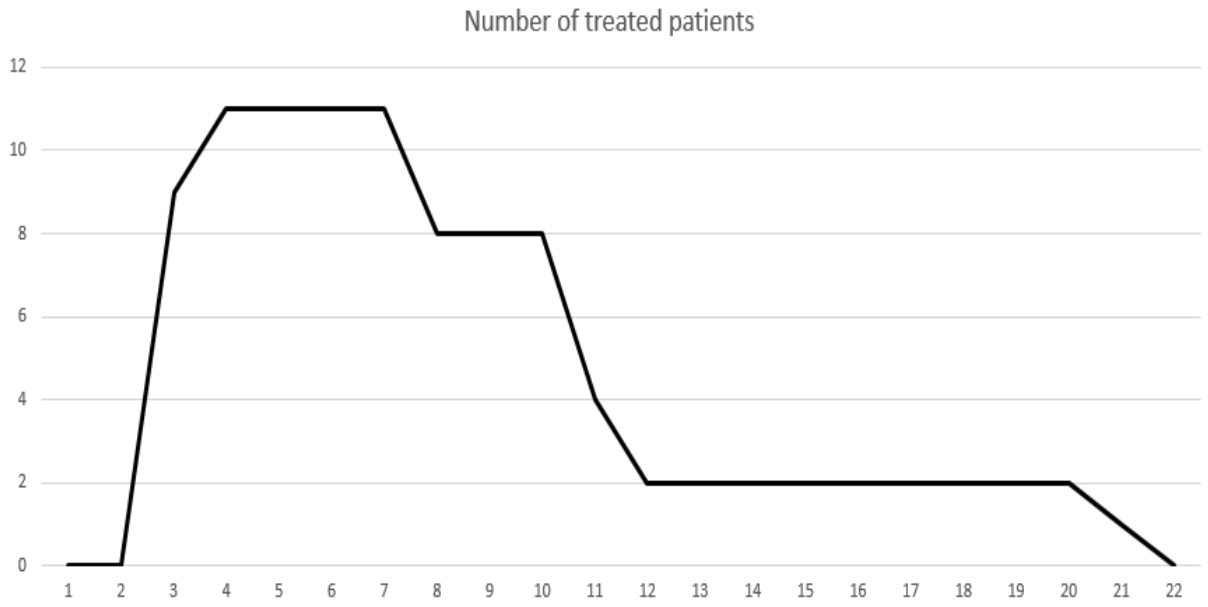


Figure 2: The number of treated patients (to-be system)

Based on Figure 2, it can be found that we should assign security guards to the related points from period 2 to period 22, 20 (20=22-2) hours. The security guard protecting the emergency entrance point will be a permanent employee because he will have a weapon. It is important that he is adequately qualified and trained, and that there is a management system in place to ensure that security guards are alert, in place, effective and working to a suitable standard. The one or the other two will come from a temporary employment agency. Because one security guard can work at most 10 hours, taking into account the work planning, we should employ 1 employee and 4 (4=2*20/10) temporary guards, 1 employee and 2 temporary guards (2=1*20/10) or 1 permanent employee alone, to protect 3, 2, and 1 security points respectively. The salary of the security guards is used to calculate the costs of the countermeasures, and the turnover (non-closure of emergency department, patients received from Linate Airport) with the saved lives gained by each countermeasure are used to measure the effects. The salary of 1 permanent security guard is 13.19 Euros per hour, based on a salary of a firefighter i.e. 27847 Euros per year (Greta.com) including 35% of employment contributions. If we employ 1 permanent security guard in Italy, 24 hours a day and 365 days a year, we need 4 permanent security guards (5 in France). In non-crisis situations, these security guards will be responsible for the safety of several other places as well, such as the admission center, operational theatres, electric grid, medical gas stocks, biological laboratories, animal experiment laboratory, etc. So, the financial impact of the salary is 10% for the emergency department, i.e. 11,139 Euros (11139≈27847*4*10%). Using a temporary worker agency, we suppose the cost to employ a security guard for a duration of 20 hours i.e. 2 workers, is three times higher than the cost to employ a permanent security guard, i.e. 40 (40≈13.19*3) Euros per hour. So, to employ one security guard to work 10 hours, 400 (400=40*10) Euros should be paid. The total cost of 2 security guards for 20 hours, is 1,600 (1600=400*2*2) Euros. If we just employ 1 security guard, the financial cost will be decreased to 800 (800=400*2*1) Euros. Here, we suppose that, if we employ 3 security guards for the 3 points to protect the emergency department, it will be 100% protected, it will not be closed, and it can receive the 100 patients from Linate Airport, with a cost of 12,739

(12739=11139+1600). Since the turnover of one patient is 528 Euros, if the emergency department can receive 100 patients who will stay in hospital for 2 days in average, the hospital can gain 105,600 (105600=528*100*2) Euros and avoid a loss of 4286208 Euros, i.e. an effect of 4,391,808 (4391808=105600+4286208) Euros. If we use 2 or 1 security guards to just protect 2 points or 1 point, the effects will be decreased to 80% and 40% respectively. These two options allow to gain 3,513,446.4 (3513446.4=4391808*0.8) and 1,756,723.2 (1756723.2=4391808*0.4) Euros respectively. Table 2 presents the related information about the cost-effectiveness analysis. According to the results we got from Table 2, it can be found that if we employ 3 security guards to protect 3 points, the cost will be the most important but the effect is the best. If we employ 1 security guard to protect 1 point, the cost is the less important but the effect is the worst. For the value of the cost-effectiveness ratio, if we protect 3 points, the cost effectiveness ratio is the smallest, 0.0029. That means we can gain 100 Euros by receiving patients injured by the terrorist attack at the airport and by keeping hospital activity, through paying 29 cents by implementing the countermeasure of employing 3 security guards to protect 3 points. Therefore, if there is no limitation of the budget, it is better to protect the 3 points.

Table 2. Cost-effectiveness analysis of the second strike

Countermeasures	Net cost (Euros)	Effects (Euros)	Cost effectiveness ratio
1 Security point	11,139	1,756,723.2	0.0063
2 Security points	11,939=11139+800	3,513,446.4	0.0034
3 Security points	12,739=11139+1600	4,391,808	0.0029

The substantial caveat to this must be that it is essential that the security guard is alert, vigilant and trained in order to mitigate the vulnerability. Visible security may need to be increased at high risk events such as VIP visits, and to ensure the safe operation of the ED in surge times. The visibility of uniformed security staff can improve the perception of safety and wellbeing for patients and staff.

3.2 Scenario 2: VIP operating room

3.2.1 Scenario

An important Italian politician is in OSR for surgery. She/he has just favoured in Parliament the approval of a law in favour of the abortion/euthanasia. A commando of terrorists enters the hospital and gets access to the operating room (OT). The VIP personal security has been left in the admission ward. The politician is killed and some employees are injured. Under the as-is system, a terrorist can access the VIP operating room and can kill the politician. We speculate that all the injured are cared in OSR, so there is no extra cost. As just one person will die in this scenario, we select the human cost of one person as the measure of effectiveness. The monetary value per fatality or the valuation of human life depends on aspects such as willingness to pay (WTP), willingness to accept compensation (WTA), voluntariness and responsibility. For current purposes, the human loss of one important person is taken as being at least 1,000,000 Euros (Suddle, 2009).

3.2.2 Countermeasures

Scenario 2 VIP	**Physical**	**Data**	**People**

Prevention	Access restriction measures: badge opening gate; gate opening by RFID inside staff uniform; OT provided by lock in + anticrush window and security outside		Training in emergency management and security of the medical and non medical personnel
Alarm			
Protection	Create a VIP track	Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Increase the number of security staff Establish on demand provision of security staff with contractors Contingency plan. VIP management plan: personnel security provided by uniform with RFID to enter armed inside the OT; possibility to lock-in/shelter-in

To protect the VIP, we can add a biometrics access control to VIP operating room with a reinforced door, or employ two security guards to protect the VIP operating room. The average annual salary of one security guard in Italy is about 27,847 Euros. Here, we suppose that 2 security guards are employed to protect the VIP operating room. One security guard can check the person who wants to access the VIP operating room. The other security guard is in the operating room and can shoot the terrorist if it is necessary. Therefore, the total annual cost of employing 2 security guards is 55,694 Euros. We suppose the effect of the security guards is 90%. The value of the effect of security guard is 900,000 (900000=1000000*90%) Euros. The cost of one access control system is 700 Euros and of a reinforced door is 4000 Euros with installation included. The purpose of an access control system is to provide quick, convenient access to those persons who are authorized, and at the same time, to prohibit access to unauthorized people. We suppose that the effect of access control system is 60%. In other words, the value of the effect of the access control system is just 600,000 (600000=1000000*60%) Euros. If we combine these two countermeasures together, we suppose the effect can be 100% and the value of the combination of these two countermeasures is 1,000,000. Table 8 gives the information about our analysis of the cost effectiveness.

Because the values of the cost effectiveness ratios of all these countermeasures are very small, we can get the conclusion that all these countermeasures can get a good effect. Since the value of the cost-effectiveness ratio of the access control system is the lowest, we should take the access control system as our priority choice.

Table 8. Cost-effectiveness analysis of the VIP operating room scenario

Countermeasures	Net cost (Euros)	Effects (Euros)	Cost effectiveness ratio
Access control system	4,700	600,000	0.008

Security guards	55,694	900,000	0.062
Security guard and Access control system	60,394	1,000,000	0.060

3.3 Scenario 3: Structural Damage

Action: 1) A former employee of OSR works for an external ambulance service supporting OSR in-hospital patients transport; 2) Was fired and sets up his personal revenge encouraged by money offered by an anonymous "donor": competitor of OSR? 3) Fabricates two rudimental bombs and…

3.3.1 Scenario 3a: Electric grid failure

A terrorist leaves one bomb in the ambulance is working with, parking close to the main power switch station and the second one where the generator for the A-B-C blocks is (inside the A-B-C- blocks we have the most critical asset: general ICU, OTs, ED) 5) As he detonates the two bombs OSR has no general and generator power supply and can rely only on UPS (2 hours) 6) OSR has to evacuate all the A-B-C patients. Activation of the Internal EMP. Involvement of the EMS to find ICU beds in other hospitals and transports.

OSR is composed of 11 buildings which are supplied by several electric grids (interconnected systems to deliver electricity from public network, each system is protected with an electric generator using fuel). An electric grid supplies several buildings. Grids are interconnected, but the destruction of one of them breaks the connection with the others. We simulate the bombs detonate on the morning, no more electricity can be provided to the units of the buildings A to C. Operating rooms must finish their activities with electricity produced from batteries. The ICU wards have also ventilation equipment with batteries for two hours, but they must evacuate their inpatients. Inpatients in other units must be evacuated to other secured units or to external hospitals, depending on the available beds. The outpatient activities are cancelled and some employees return home.

3.3.2 As is system simulation

After the electrical failure due to a terrorist attack on an electric grid, all the inpatients in buildings A, B and C should be evacuated, i.e. 18 units should be evacuated. We suppose that the evacuation starts from period 73 (8AM on the third day) for warm-up reason. The electric failure takes place on day, and outpatients are delayed or they go back home, employees as well. We suppose that 40% of all the evacuated inpatients will be regrouped in the unit A144 (level 1, building D) before to be dispatched in different wards, and 60% of all the evacuated inpatients are sent to external hospitals.

In total, there are 361 inpatients, who need to be evacuated. In the basic scenario, we use 36 nurses, 18 porters and 6 ambulances to evacuate these 361 inpatients. Among these 361 inpatients, 60% of them will be evacuated to external hospitals and so 217 inpatients (217=361*60%) will be evacuated to external hospitals. At period 94, all the people have been evacuated. 21 periods (hours) have been used to evacuate all the people. If we suppose that the 3 buildings A to C are closed over the 11 buildings, for 14 days to repair the electric grid, the operational loss is 5,768,797 (5768797=((1044450*3/11)/365)*14*528) Euros, according to 1,044,450 hospital

admissions (outpatients and inpatients) per year and a turnover per patient of 528 Euros. In this scenario, we do not take into account the human loss caused by the deaths of patients, because there is no death.

Figure 3 presents the number of waiting patients to be transported by ambulances, the number of waiting patients to be prepared by nurses, the number of evacuated patients to other units and the number of patients evacuated to other hospitals (see annex 1). The horizontal axis represents the periods and the vertical axis is the number of patients. From this figure, it can be found that at the beginning of period 74, more than 300 patients are waiting for being prepared. But, all these patients have been well prepared at the beginning of period 80. At the beginning of period 83, the number of patients waiting to be transported by ambulances, reaches the largest. There is no patient waiting for being transported by porters. All the patients who should be transported to other units have been well transported at the beginning of period 82. From the beginning of period 82 to the beginning of period 94, we just transported the patients who should be evacuated to other hospitals. ICU patients will be evacuated first. Therefore, come to the conclusion that the bottleneck activity is “Transport to the safe area” (by ambulances).

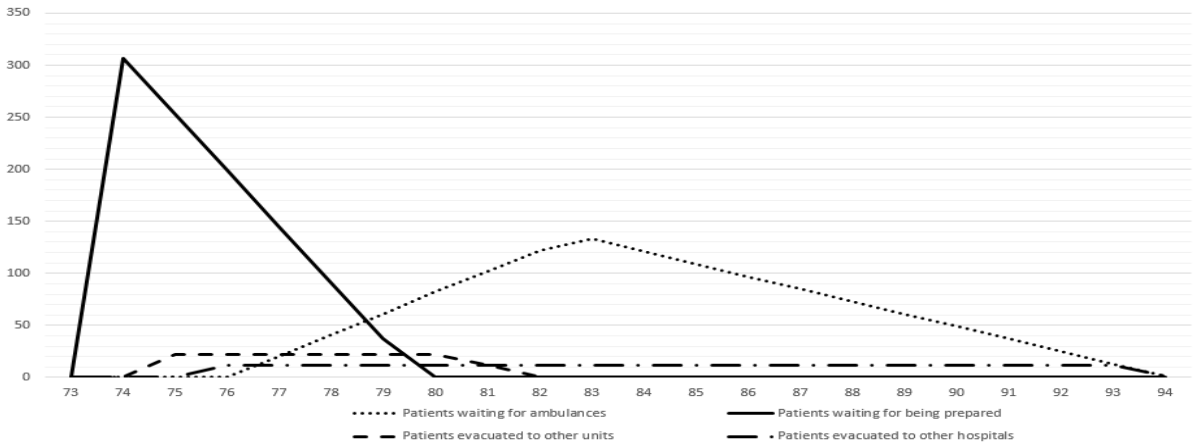


Figure 3: Waiting inpatients and evacuated patients during the evacuation process (as-is system)

The Figure 4 shows the required evacuation time under different capacities of nurses, porters and ambulances. The horizontal axis represents the resource configuration and the vertical axis presents the completion date of the evacuation. This graph demonstrates the correctness of our model. Since the bottleneck activity is “Transport to the safe area”, it is very logical that increasing the number of nurses and the number of porters does not have a big impact on the time required to evacuate inpatients.

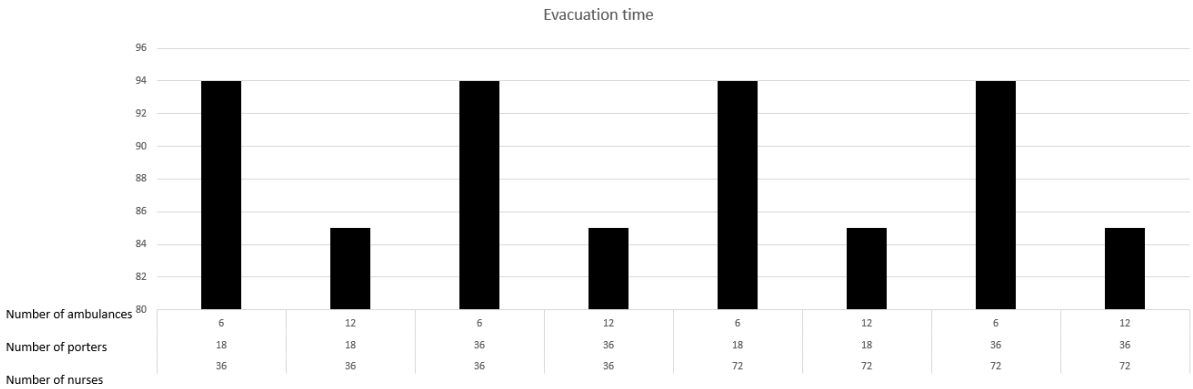


Figure 4: Completion time under different capacities of nurses, porters and ambulances

3.3.3 Countermeasures

In the as-is system, buildings A, B and C belong to one electric grid system. If there is a terrorist attack in this zone, all the patients in the buildings A, B and C should be evacuated. In the to-be system, we can supplement the electric grid with an electricity generator using fuel (called mirror generator) for each building. As the result in case of failure of the electric grid of buildings A, B and C, electricity can be provided independently. Also, the mirror electricity generators will be located in separate places. Thus, if there is a terrorist attack on the electric grid of building A to C and on the mirror electricity generator of building C, only building C has a power failure, because buildings A and B are supplied by their own generator. So only the patients in building C should be evacuated.

Scenario 3 Structural damage	**Physical**	**Data**	**People**
Prevention	Location of critical installations far from the public accessible paths but easy to be reach by the ordinary management and the emergency services. Access control systems		Training in emergency management and security of the medical and non medical personnel
Alarm		Alarms and CCTV with motion detection. Centralized station for monitoring	
Protection		Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Increase the number of security staff Establish on demand provision of security staff with contractors Contingency plan. Agreement with contractors for renting equipment or rapid shipment of needs

			(Oxygen, fuel for generators…)

3.3.4 To be system simulation

Here, we suppose that the electric grids of buildings A, B and C are less dependent thanks to independent electricity generators. In case of a terrorist attack, only building C needs to be evacuated. The total number of patients that should be evacuated in building C is 119. We use 12 nurses, 6 porters and 6 ambulances to evacuate 119 patients. Other hypothesis are the same as in the as-is system. In this case, if the evacuation begins at period 73, all the patients can be evacuated at period 82. 9 hours are used to evacuate all the patients. Figure 5 presents the number of waiting patients to be prepared by nurses, the number of evacuated patients to other units and the number of patients evacuated to other hospitals. In this situation, no patients are waiting to be transported by ambulance. With the help of our countermeasure, 12 hours (12=92-82) have been saved.

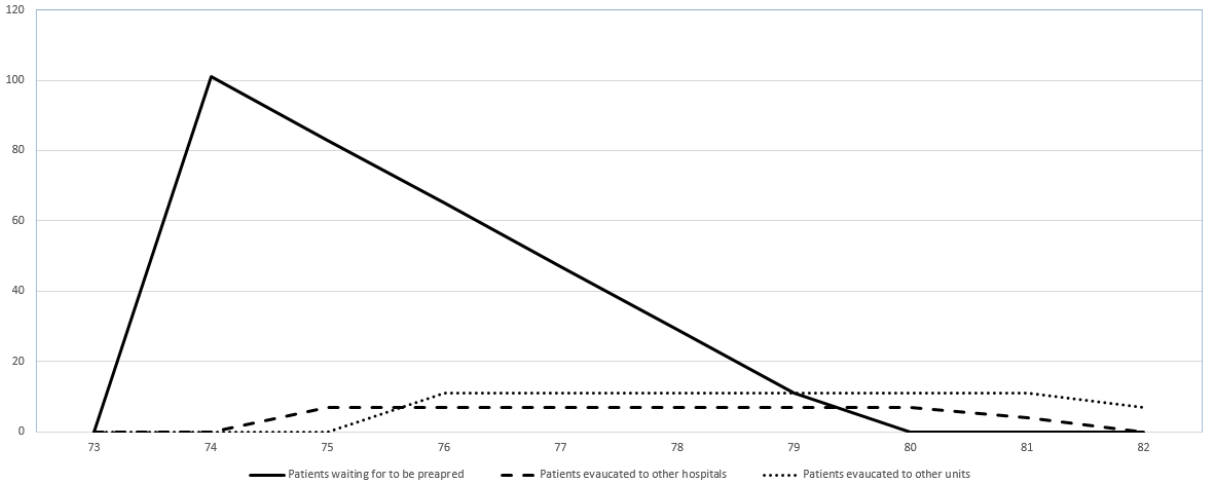


Figure 5: Waiting patients and evacuated patients during the evacuation process (to-be system)

In the as-is system, the total financial loss is the turnover of patients during the buildings' closure and the cost paid for evacuation. As mentioned before, the turnover of one patient is 528 Euros. So, the operational loss of the turnover of patients for 14 days is 5,768,797 (5768797=((1044450*3/11)/365)*14*528) Euros. The cost to evacuate one patient by ambulance is 21 Euros. 217 patients will be evacuated to other hospital. So, the cost used for evacuation is 4,557 (4557=21*217) Euros. The total loss is 5,773,354 Euros (5773354=5768797+4557). The rule to calculate the operational loss of the to-be system is the same. The loss of the turnover of patients is 1,922,932 Euros (1922932=((1044450*1/11)/365)* 14*528). 71 patients should be evacuated to other hospitals (one third of the situation without countermeasure). Therefore, the cost used for evacuation is 1,491 (1491=21*71) Euros. The total loss is 1,924,423 (1924423=1922932+1491) Euros. With the help of our countermeasure, 3,848,931 (3848931=5773354-1924423) Euros will be saved. For the electricity generator countermeasure, we assume that one electricity generator will cost 200000 Euros. We need three electricity generators, one each for

every building. 600,000 Euros (600000=200000*3) should be spent to buy three electricity generators. The cost-effectiveness ratio is equal to 0.156 (0.156=600000/3848931). That means we can gain 1 euro by implemented one mirror electricity generator, through paying 16 cents to carry out the countermeasure.

3.4 Scenario 3b: Medical gas failure

A terrorist leaves one bomb in the ambulance is working with, parking close to the main medical oxygen stock piles. 4) Then leaves the place and walks away with the second bomb and leaves it close to the back up medical gas stock pile. 5) As he detonates the two bombs OSR has no O2 available but only the O2 reservoirs stored for emergencies. 6) OSR has to evacuate all O2 dependent patients. Activation of the Internal EMP. Involvement of the EMS to find ICU beds in other hospitals and transports (see annex 1).

3.4.1 As is system simulation

At the beginning of day 1 on period 1, there are 12 patients in emergency ICU and 16 patients in the neuro-surgical ICU. We suppose that the terrorist attack begins at day 1 on period 2, and it destroys all the medical gas tanks. Patients from the aforementioned two different ICU units need to be evacuated: emergency ICU and neuro-surgical ICU. The numbers of patients who need to be evacuated from these two different ICUs are 12 and 16 respectively. The total number of people to be evacuated from ICU is 28. The three main activities to launch are organized in series, they detail the internal emergency management plan supporting hospital evacuation: prepare the patients, transport the patients to the evacuation point or a hospital care unit, and transport the patients to external hospitals. In every ICU, we suppose that 10 minutes are needed to prepare each patient (ventilate the patient, assign a nurse, dress the patient, and attach the medical file) with 1 nurse per patient, under the control of 1 physician and 1 head nurse. To transport the patients to the evacuation point or a hospital care unit, it will take 20 minutes in average depending on accessibility, and one porter with one nurse will be in charge of this transportation. Emergency ICU patients (12 patients) will be evacuated to a hospital care unit where mobile oxygen tanks and mobile ventilators are available, and neuro-surgical ICU patients (16 patients) will be evacuated to external hospitals. 30 minutes are needed to transport patients to external hospitals, and 4 ambulances are available. All these 28 patients need the oxygen bottles during the evacuation process. We suppose that one oxygen bottle can support a patient for two hours. By period 10, all patients are safely evacuated, i.e. 8 hours are required for patient evacuation and a patient needs 4 hours in average to be evacuated. Figure 6 presents the number of patients who are waiting to be prepared in different ICU units. The horizontal axis represents the periods; the vertical axis defines the number of patients waiting to be prepared. To evacuate one patient, it will take 4 hours, and one oxygen bottle can support a patient for 2 hours. So, to evacuate one patient, 2 oxygen bottles will be needed. In total, 56 oxygen bottles (56=28*4/2) will be needed during patients' evacuation. Regarding to the number of patients waiting to be prepared, the number of required nurses is the focal resource, especially if patients must be manually ventilated with ambu-bags.

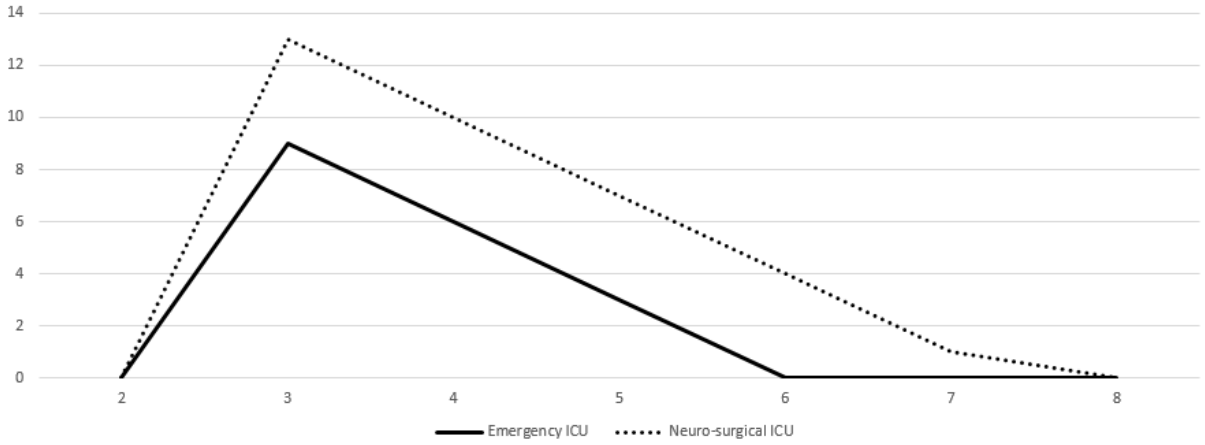


Figure 6: Number of patients waiting to be prepared in different ICU units

In the as-is system, the ICU units are closed for 2 days until the medical gas tanks are repaired, so the operational loss is 29,568 (29568=28*528*2) Euros, according to 28 ICU patients and a turnover per patient of 528 Euros. To evacuate one patient by ambulance, it will cost approximately 21 Euros (Ambulance.com). 16 patients will be evacuated to other hospitals. The cost of evacuation of patients is 336 (336=21*16) Euros. During the evacuation, 56 oxygen bottles will be needed. One oxygen bottle will cost approximately about 100 Euros (Air.com). So, the cost for oxygen bottles is 5,600 Euros (5600=56*100). There is a high possibility that, at least, one patient will die because of the lack of oxygen. Therefore, the human loss of the death of one patient, 1,000,000 Euros, should be taken into account. The total loss is 1,035,504 (1035504= 29568+5600+336+1000000) Euros.

3.4.2 Countermeasures

For the countermeasure, we can buy mobile oxygen tanks. All the patients can be supplied by mobile oxygen tanks in their ICU beds, before the fixed medical gas tanks are repaired. In this way, we do not need to evacuate patients. But, we must provide liquid oxygen bottles for the mobile oxygen tanks which have in average 6 hours duration. We suppose that it will take 48 hours to repair the fixed oxygen tanks. So, we must stock the liquid oxygen bottles for patients for 48 hours. Because one set of liquid oxygen bottles can support an ICU for six hours, one unit needs 9 (9≈48/6) set of liquid oxygen bottles before the fixed oxygen tanks can supply as usual. So, 24,000 (24000=2*12000) Euros will be the cost to buy the mobile oxygen tanks and 10,800 (10800=600*9*2) Euros must be paid to buy the sets of liquid oxygen bottles, i.e. a total cost of 34,800 (34800=24000+10800) Euros for the two ICU. With the help of our countermeasure, 1,000,704 (1000704=1035504-34800) Euros can be saved with an effectiveness ratio of 0.034 (0.034=34800/1035504). This countermeasure has been already implemented by OSR.

3.5 Scenario 4: Nuclear

3.5.1 Scenario

1) Few weeks before the attack, one staff of the hospital cleaning company reports having missed his/her uniform containing the personnel badge. The company provides a new one. 2) A suicide terrorist expert in nuclear material, wearing a cleaner uniform, gets access to the offices where all the nuclear materials are stored. 3) He/she locates the Cesium 137 irradiator and realizes that it is largely unprotected.

4) One night, he/she goes there, opens the room with the badge, breaks the steel iron box (with a laser device/oxydric-acid flame) and easily steals the Cesium powder. He/she just wears protective gloves. 4) Then, he/she spreads it in all the rooms of the Emergency department. Nobody is alarmed because he pretends to be a cleaner. The action takes place during the night because the irradiator room is not frequented during that time. The Emergency department is selected as a target because it is the most crowded area at night time and according to an infected threshold of 2 hours all the people (patient and staff) of the ED are contaminated. The terrorist shows up after some hours or after 24 hours.

3.5.2 As is system simulation

We suppose that at period 10 (for warm-up reason), a terrorist stole the CESIUM 137 and he/she spreads this later in the emergency department. If patients are in contact with CESIUM 137 for at most two hours, they will not be infected. But, if they contact CESIUM 137 for more than two hours, they will be infected. Therefore, we suppose that at beginning of period 15, we detect the CESIUM 137 attack and we try to evacuate the patients and staff from the emergency department to other units according to the internal emergency management plan (see annex 1). According to the data from OSR, we suppose that 22 regular patients are in ED at beginning of period 10, and that 7 new patients arrive in the emergency department per hour (1 red, 2 yellows and 4 greens). According to the simulation results, 14 patients have already been treated from period 10 to period 15, the total number of patients that should be evacuated is 36 (36=22+7*4-14). 28 physicians and nurses should be also evacuated. Therefore, the total number of people that should be evacuated is 64 (64=36+28). We suppose that 10 minutes are used to decontaminate the contaminated people and 10 minutes are used to prepare patients. 6 nurses wearing protective suits will be responsible for decontamination and preparation respectively. To transport the patients from the emergency department to other units, it will take 20 minutes, and 3 porters wearing protective suits can be assigned for this activity. At period 29, all the patients are safely evacuated. Figure 7 presents the number of waiting patients to be decontaminated and the number of evacuated patients. The horizontal axis defines the periods, and the vertical axes the patient numbers. There are no patients who are waiting for other activities. So the bottleneck activity is the decontamination. At the beginning of period 25, all the patients have been fully decontaminated. At period 29, the last patient has been evacuated to another unit. The emergency department is closed for 2 weeks to be decontaminated. The operational loss is 1,286,208 (1286208=174*528*2*7) Euros, according to 63,500 emergency admissions per year and a turnover per patient of 528 Euros (see the second strike scenario).

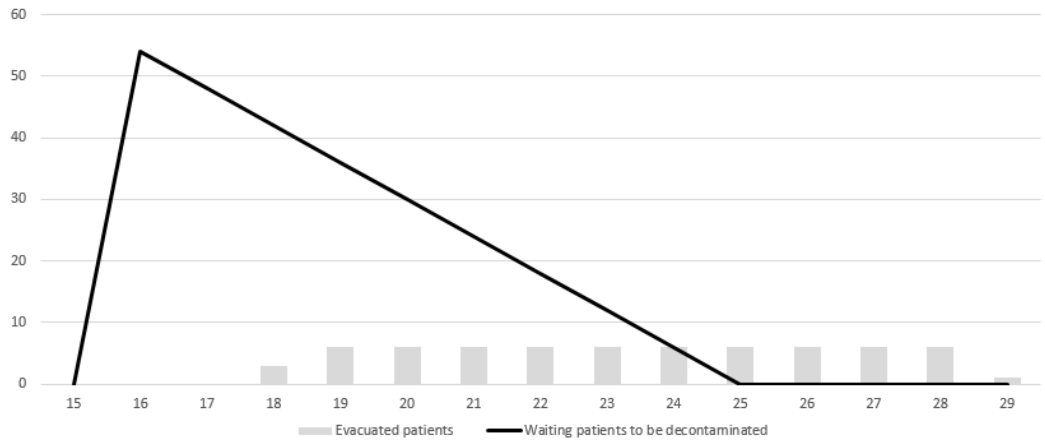


Figure 7: The number of patients waiting to be decontaminated and the number of evacuated patients.

3.5.3 Countermeasures

Scenario 4 Nuclear	Physical	Data	People
Prevention	Safer location (barriers). Access restriction.		Training in emergency management and security of the medical and non medical personnel. Emergency drills. Fire Brigade involvement.
Alarm	CCTV with motion detection. Radiation detection (hidden) in the room of the nuclear source. Sensors for movements		CCTV with motion detection/sensors for movements promptly inform about unauthorized people in the area. Radiation detection promptly informs about radioactive material outside shielded areas.
Protection	Portable Geiger sensor available for checking contamination	Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Expert staff available on call 24/24. Contingency plan. Plan for fast management of reaction to an alarm; checking for contamination of infrastructure/people; decontamination and treatment of contaminated rooms and people (better if shared with experts from the Fire Brigade). Communication strategy

For the actions of countermeasure, basically, a biometrics control system can be installed to better lock the CESIUM stockpiles with a cost of 700 Euros (see SARS scenario). It can be supplemented with a Geiger sensor able to send an alarm to the maintenance department. The cost of this latter is 150 euros (Pce.com) with an

installation cost of 300 euros. First, a CCTV surveillance system can be used to watch the area where the CESIUM 137 is stored. With the help of this CCTV surveillance, if the CESIUM 137 is stolen, we can detect this situation earlier, particularly thanks to Geiger sensor. A CCTV surveillance system is a closed-circuit television system used to observe unusual facts. A CCTV surveillance system consists of three parts, cameras, computer control system and the related security guards. Second, we can employ dedicated security guards to protect the CESIUM 137 stockpiles, with the help of Geiger sensor. After we found the place where the CESIUM 137 has been spread, we should cordon this place and evacuate all the people there. With the help of our countermeasures, the terrorist attack can be detected earlier and so people do not have the risk to be contaminated. But, they should still be evacuated because of the spread of the CESIUM 137. In the to-be system, we suppose that the terrorist attack is detected at the beginning of period 11. In the meantime, the evacuation begins. At period 20, all the patients can be well evacuated. Figure 8 presents the number of waiting patients to be prepared and the number of evacuated patients. The horizontal axis defines the periods, and the vertical axes denote the number of the patients. There are no patients who are waiting to be transported. So, the number of the porters is enough. From period 13 to period 19, 9 patients (maximal evacuation capacity per period) have been evacuated to other units per period. At period 20, the last patient has been evacuated to another unit. Compared with the as-is system, 9 hours (9=29-20) have been saved, including 4 hours because of an early detection.

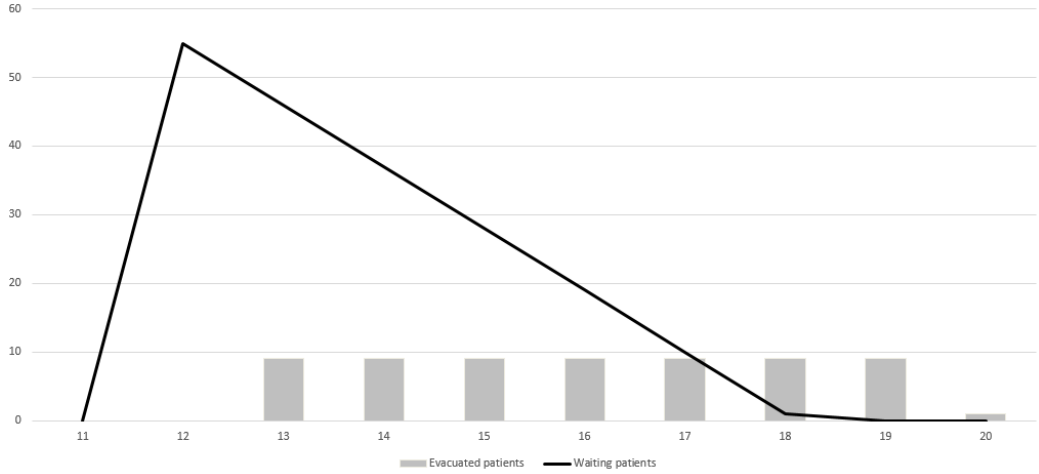


Figure 8: The number of patients waiting to be prepared and the number of evacuated patients.

For the first countermeasure, the cost of the CCTV surveillance system includes three parts, the price of CCTV surveillance system, the price of employing the people who can observe the current situation and the price of employing a security guard. Here, we suppose that we need one person who observes the current situation and one security guard who can manage the emergency situation. Regularly, the employees can switch from one post to the other, to be more efficient. But, taking into account the work planning, we should employ 4 people a year for the observation work and 4 people a year for the work of the security guard. Usually, a CCTV surveillance system costs 7,000 Euros per IP camera (An2v.org). Regarding to OSR, IP cameras will be internal, and there is no problem for electrical connection as well as for the computer network integration (Axis.com). The average annual salary for a permanent employee in Italy working in security is approximately 27,847 Euros based

on the salary of a firefighter (Greta.com). Because the people who observe the current situation and the security guard will be responsible for the safety of several other places as well (10 in total), such as the admission center, operational theatres, emergency department, electric grids, medical gas tanks, biological laboratories, animal experiment laboratory, etc. Therefore, we use 10% of the annual salary to calculate the cost and 10% of the equipment. The cost of employing a person who can observe the current situation is 11,139 Euros (11139≈27847*4*10%). The cost of employing the security guard is the same, i.e. 11,139 Euros. So, the total cost including the biometrics control system, is 30,428 (30428=7000*10*10%+11139+11139 +450+700) Euros. For the second countermeasure, if we employ one security guard who will be responsible for the safety of the stockpiles of Cesium 137 specially, taking into account the working planning, we need four people. The cost of this countermeasure with the biometrics control system is 112,538 Euros (112538=27847*4+450+700). We use the saved time of the evacuation as the measure of effects. And we suppose that if two countermeasures can be connected together, the effect will be 100%, because they will deter the adversary. The effect of using the CCTV surveillance system (Meglan, 2015) and the security guard (Brownyard, 2016) are 60% and 90% respectively. Table 3 calculates the cost effectiveness ratio of each countermeasure. From this table, it can be found that, because the value of net cost is very high, the value of cost-effectiveness ratio is very high. The cost effectiveness ratio presents that how much should be paid if we want to save one hour by using this countermeasure. For example, by using security guards, 13,894 Euros should be paid if we want to save one hour of evacuation. Combination of two countermeasures will cost more than others but the effect is the best. So, if the fund is enough, we can choose the combination of the two countermeasures. If we use the two countermeasures separately, the cost of the CCTV surveillance is less than the cost of the security guard but the effect is better. From a view of the cost-effectiveness ratio, we should choose CCTV surveillance. If the contamination can be avoided the effectiveness ratio is different because the effect is the non-closure of the emergency department, and the ratio is equal to 0.11 (0.11≈141816/1286208). So, the combination of the two countermeasures produces the best effect.

Table 3. Cost-effectiveness analysis of CESIUM 137 scenario

Countermeasures	Net cost (Euros)	Effects (hours)	Cost effectiveness ratio
CCTV surveillance	30,428	5.4=9*60%	5,635
Security guard	112,538	8.1=9*90%	13,894
Combination of the two countermeasures	141,816=142966-1150 (just one Geiger sensor and one biometrics controller)	9=9*100%	15,757

3.6 Scenario 5: Cyber-attack

3.6.1 Scenario

An expert in IT systems (net) has been recently fired; approached by an OSR competitor is convinced to destroy OSR net 2) She/he uses a PC logged in to insert a worms to get the net-nodes plan, than remotely hack the net (sunday afternoon) 3)

the first to realize there is a IS problem are the staff working in the ED: they try to recover by themselves (1 hour), then call the call-centre; it takes 1 more hour to have some IT expert to try to fix remotely, then to decide to come to the hospital; in the meanwhile the ED and the lab shift to hand-working (paper and standing alone instruments) but all the rest of the systems cannot be operational; the Health Direction is informed; the EMS is informed of difficulties in processing emergency patients; it takes 2 more hours to have a first balance of the damage: very big problem, but it takes some more 2-3 hours to see if it can be solved: the supplier (s) of the IT infrastructure are called in; the Health Direction asks for a formal closure of the hospital emergency activities to the local Authorities; 2-3 hours later is clear that the problem will last at least 5 days and has eventually intentional; all the hospital activities are not operational except the ones working with paper and standing alone instruments: diagnostic devices are just emogas analyzer; emergency lab analyzers; usg; 1-2 Xray machine in the X ray Dept; ED has to stay closed and it will affect the EMS work; the elective activity must be stopped; the risk of errors is dramatically increased; no possibility to have a X-ray for patients not able to go to the X-ray Dept.

The whole hospital is out of order for 5 days. It cannot receive inpatients, outpatients and acute patients. The operational loss is equal to 7,554,378 (7554378≈(1044450/365)*5*528) Euros.

3.6.2 Countermeasures

Scenario 7 Cyber	Physical	Data	People
Prevention	Increase infrastructure resilience (back up of the net? General? Local at least for the essential services?); increase the standing alone machines at least for the essential services? (data management in the ED/outpatient department; emergency lab/X-ray);		Training in emergency management and security of the medical and non medical personnel. Training in cyber security of the medical and non medical personnel including simulations
Alarm		Early warning system	Early warning procedure to inform about a potential risk of intentional attack
Protection	Paper back-up	Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Expert staff available on call 24/24. Contingency plan. Rapid response plan for IS failure; procedure for net crash-down; plan for crisis involving the whole hospital (sending the patients to hospitals part of the group?) ; increase the cyber security (automatic de-log of the pc after 5 minutes of non use?);

For the countermeasures, first we can use a ‘paper kit’. A ‘paper kit’ is a manual system based on the use of paper and pencils to dispatch and record information (Grange and Leynon, 2015). Such old systems, which have been replaced by numerical systems, can be used in the case of computer failure. To initiate the ‘paper kit’, relevant information such as patient prescriptions, patient appointments, admissions, tests' requests, etc., can be initiated on paper documents using PDF files located on the local computer devices of the care and technical units. So, information is first duplicated and dispatched to physicians and nurses at the beginning of the computer failure, second, information is collected and disseminated during the computer failure on the paper documents with pencils, and finally information will be recorded on the numerical information system after repairing the computer system. Information is communicated by messengers (by walking). Such a way enables us to ensure the continuity and traceability of cares. To be able to launch this system at any time, the information system department must set up an automated system to record frequently on the care unit computer: the patients’ treatments, the drug administration, the patients’ appointments, etc., e.g. every four hours, in order to be ready to face a failure. The 'paper kit' can be improved if bar-codes can be added. If local computers of care units are safe and are equipped with bar-code scanners and bar-code printers, information can be stored periodically on local computers and can be easily printed on the paper documents. The dispatching of information is still made by messengers. The patients’ identification can be better secured. USB keys can also support information such as Excel Sheets. For the cost of ‘paper kit’, it consists of two parts. The cost of the first part is used to launch the ‘paper kit’ and the cost of the second part is used to save the information which is on the paper. For the first part, each unit should launch their own ‘paper kit’, which will require 4 hours. We suppose that 40 Euros must be paid to launch the paper kit, per hour and per service. Therefore, 49 care units need 7,840 (7840=40*4*49) Euros to launch the ‘paper kit’. For the second part after the computer system repairing, to input the information which is on the paper, 8 hours will be used per service. Again, we suppose 40 Euros will be paid to people who input the information, and the information of all 49 units must be inputted. So, the cost of the second part is 15,680 Euros (15680=40*8*49). Therefore, the total cost is 23,520 Euros (23520=7840+15680). Second, we can improve the ‘paper kit’ system using bar-codes. The material required for the improvement, is bar-codes scanners and bar-codes printers. A bar-code scanner costs 350 Euros (HP1.com) and the price of a bar-code printer is 450 euros (HP2.com). The ‘paper kit’ improvement costs 39,200 (39200=(350+450)*49) Euros, but it allowed to avoid identity vigilance problems which can result in patient deaths. The improved ‘paper kit’ costs 62,720 (62720=23520+39200) Euros. Third, the 4 net servers of the hospital which manage the 14 buildings, can be duplicated and periodically information is backup on these mirror net servers. The cost of duplicating a net server is 4,000 Euros (ServerPrice.com) per mirror server, i.e. for the 4 required mirror servers 16,000 Euros, and the backups and security checking require one permanent employee for 27,847 Euros per year. The total cost is 43,847 (43847=16000+27847) Euros. The effect of the ‘paper kit’, the improved ‘paper kit’ and the duplicated net servers are 80%, 90% and 100% respectively to reduce the operational loss of the hospital equal to 7554378 Euros, by keeping part or whole of its activity.

The cost-effectiveness analysis has been presented in Table 6. Based on our analysis, we can find that all the values of the cost-effectiveness ratio are very small.

In other words, we can pay a little for the countermeasures to get a good result. So, we can get the conclusion that it is very useful to duplicate net servers or adopt the 'paper kit'. The 'paper kit' can be used whatever the part of information system is damaged.

Table 6. Cost-effectiveness analysis of cyber-attack scenario

Countermeasures	Net cost (Euros)	Effects (Euros)	Cost effectiveness ratio
'Paper kit'	23,520	6,043,502.4=7554378*0.80	0.0039
Improved 'Paper kit'	62,720	6,798,940.2=7554378*0.90	0.0092
Duplicating net system	43,847	7,554,378	0.0058

3.7 Scenario 6: animal experiment laboratory

3.7.1 Scenario

Some of the students of OSR University feel offended after visiting the internal animal laboratory. They contact a group of animal rights activists and organize a raid to make some noise around the animal laboratory and the research activity with animals. They get access to the main animal laboratory (up to 9,000 animals). They free a number of animals, take out from the fridges the dead animals used for the sanitary control, take pictures and videos, and say animals are maltreated. Some of the released animals are infected by HIV and/or hepatitis. The animal lab is contaminated, and it is impossible to recognize the particular strains selected inside OSR. The experiment on animals should be stopped. No research activity can be done for an extended period, usually 1 to 3 years. We suppose that the turnover of hospital will decrease by 3% per year because of the animal lab closure. The turnover of the hospital is 5518 million Euros per year. To replenish the animal laboratory, it will take 2 years. Therefore, before the animal laboratory begins to work again, the total financial loss is 326.1138 million Euros (326.1138=5518*0.03+5518*(0.97)*0.03). Here, the final loss is selected as our measure of effect.

3.7.2 Countermeasures

Scenario 8 Animalists	**Physical**	**Data**	**People**
Prevention	Improve physical barriers; access control (webcam, intruder alarms, security patrolling…)	Improve the policy for security clearance for personnel	Training in emergency management and security of the medical and non medical personnel. Emergency drills. Improve the disaster plan (contingency plan in particular to improve the resilience and to avoid to loose the most important strains; communication strategy, in particular proactive - Research for Life platform) Contingency plan and emergency drills.

Alarm		Early warning system	Early warning procedure to inform about a potential risk of intentional attack.
Protection		Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Increase the number of security staff Establish on demand provision of security staff with contractors. Contingency plan.

Two countermeasures can be proposed here. First, a security guard can be assigned to protect the security of animal experiment laboratory. At least 4 security guards will be employed per year. The average annual salary of one security guard in Italy is about 27,847 Euros. So, the cost of 4 security guards is 111,388 Euros. Second, a CCTV surveillance system can be used to detect if there is an attack to the animal laboratory. The CCTV surveillance system will cost about 29,278 Euros (see the CESIUM 137 threat scenario). We suppose that the combination of these two countermeasures can achieve 100% effect and so 326.1138 millions of Euros can be gained. If the security guards and the CCTV surveillance can achieve 90% and 60% effect, 293.50242 (293.50242=326.1138*90%), and 195.66828 (195.66828=326.1138*60%) millions of Euros can be gained respectively. Table 7 presents the result of the cost-effectiveness analysis. Based on this table, the combination of two countermeasures can get the best effect, but the cost is the highest. Using the combination of two countermeasures, the value of cost effectiveness ratio is the highest, 0.0004. That means, if we want to avoid the loss of 1 million Euros caused by an attack to the animal laboratory, we should pay 400 Euros to implement the countermeasures. The cost of the CCTV surveillance system is less and the value of cost effectiveness ratio is less as well. So, it is better to consider the CCTV surveillance system as the first choice.

Table 7. Cost-effectiveness analysis of the animal experiment laboratory scenario

Countermeasures	Net cost (Euros)	Effects (Euros)	Cost effectiveness ratio
CCTV surveillance system	29,278	195,668,280	0.0002
Security guards	111,388	293,502,420	0.0003
Combination of the two countermeasures	140,666	326,113,800	0.0004

3.8 Scenario 7: Bio attack

3.8.1 Scenario 7.1 SARS

1) A native Italian affiliated to an international terrorist organization is a medical doctor with a virological background. He/she pretends to be funded by a famous pharmaceutical industry, and approaches the Director of OSR Foundation for a PHD in virology. He/she has been referred to the P3 "SARS" laboratory and works there

for a while. He/she has access to the P3 laboratory and to the repository of the SARS virus. 2) One night, he/she takes some material from the SARS vials, and grows up enough viruses; 3) He/she prepares a dispersion solution. 4) Dressed as a cleaner, with enough PPE (personal protective equipment) to be protected but not "strange", he/she sprays over the surfaces of the primary acceptance central in the time of major influx of patients. 5) All the people passing by the place (almost all the outpatients and the inpatients over 4 hours, which is the estimated time for survival of the virus on the surfaces) have contact with the virus. 6) According with the rate of infection, 10% of contacts get the infection. Infected people transmit the infection from man-to-man through air-droplets after 4 days. Contacts are in the whole hospital (including staff) and out of the hospital through contacts. We can presume that there will be an increased incidence of severe pneumonia inside the most vulnerable people, and then there is an evidence of the same strain of virus at the investigations. No treatment and no vaccine are available. Only the support to vital functions is possible. Then some cases will start to develop within the medical staff and will be reported in other hospitals. The Preventive Medicine Department will be informed. Quarantine measures and active case finding policies will be implemented. An unusual SARS epidemic will be declared with impact on the whole of Milan, and eventually the epidemic requires the need to transfer ICU patients out of Milan and Lombardy region because of shortness of ICU beds. After some time lost looking for the single first case that started the epidemic, an anonymous letter will reach the hospital saying that it was an intentional act, and to prove this the check of the vials inside the P3 lab can be done. The fake PhD student disappears. The whole hospital is closed for 14 days to be decontaminated, and the operational loss is equal to 21,152,258 (21152258=(1044450/365)*14*528) Euros.

3.8.2 As is system simulation

We suppose that there is a SARS attack at the beginning of period 10 for warm-up reason, at the primary acceptance central of OSR. The virus SARS is transmissible between humans after 96 hours (4 days). Since all the patients (inpatients and outpatients) should go to the primary acceptance central first, all the patients have the possibility to be infected. Here, we suppose that 10% of the patients may be infected. From period 10 to period 13, 13416 outpatients and 140 inpatients passed through the admission center. Therefore, the total number of infected patients is approximately 1,356 (1356≈ (13416+140)*0.1). At the beginning of period 14, the virus SARS is ineffective because of its lifetime. But the infected inpatients still have the possibility to infect others. Among 1356 infected patients, 14 of them are inpatients. We suppose that 10% of these infected inpatients will infect other OSR patients when they leave the hospital. Based on our simulation model, from day 14 to day 17, these inpatients may meet 272 (according to the simulation result) other patients in total. If we suppose that the contamination rate is 10%, the number of second infected patients is about 381 (14*272*0.1=381). In total, the number of total infected patients in OSR, is 1,737 (1737=1356+381).

3.8.3 Countermeasures

Scenario 5 Biological - Virus	Physical	Data	People

Prevention	Increase physical security to the bio hazards labs and repositories (physical security instruments);	Policy for ensuring security clearance to people admitted to the P3 lab (asking to the Ministry of Interior?); Avoid leaving alone in the P3 people without security credentials (cleaners); plan to protect and secure the staff; plan for management of this scenario, including protection of the hospital image (media)	Training in emergency management and security of the medical and non medical personnel. Emergency drills.
Alarm		Early warning system.	Early warning procedure to inform about a potential risk of intentional attack. Early warning system for internal epidemic (patients/staff).
Protection		Incorporate inside the EMPs the terrorist scenario Include drills inside the EMPs	Contingency plan.

For the countermeasure of SARS attack, first, we can reinforce the access control system of virus bank, by limiting virus accesses only to authorized persons or accompanied persons under the control of authorized persons. Today, access control systems have become more and more sophisticated. Here, we refer to the biometrics access control system. Biometrics access control system always adopts the fingers to record the information. Second, we can employ a dedicated security guard to protect the laboratory during the night, to prohibit access. Third, we can use a CCTV surveillance system. For the cost of these three countermeasures, one biometrics access system will cost 400 Euros (Security.com), and to install the biometrics access system, it will cost about 300 Euros. So, the first countermeasure costs 700 Euros (700=300+400). For the second countermeasure, we need 2 persons a year for a dedicated security guard protection during night-time. Since the salary of one person is 27,847 Euros, 55,694 Euros will be used for the 2 security guards. For the third countermeasure, the method to calculate the cost is as same as what we did for the Cesium 137 scenario. The cost is 29,278 Euros (the method to calculate it can be found in the Cesium 137 scenario). Here, we select the number of people who do not get infected by using the countermeasure, to measure the effect. We suppose the effect of biometrics access system is 50%, the effect of the security guards is 50% and the effect of the CCTV surveillance system is 60%. The effect of the combination of these three methods is 100%. Table 4 presents the result of our cost-effectiveness analysis. In this table, the value of cost effectiveness ratio shows that how much should be paid if we want to protect one person. For example, by using biometrics access control system, 0.81 Euros should be paid if we want to protect one person.

Logically, the combination of these three countermeasures costs most and has the best effect. The cost of using a security guard is higher than using biometrics access control and using CCTV surveillance system. While the effect of using a security guard is the worst. So, it seems that using a security guard is not a good choice. The value of cost-effectiveness ratio of the biometrics access control is less than others. So, using biometrics access control is more reasonable.

Table 4. Cost-effectiveness analysis of SARS scenario

Countermeasures	Net cost (Euros)	Effects (Protected persons)	Cost effectiveness ratio
Biometrics access control	700	868≈1737*0.5	0.806
Security guards	55,694	868≈1737*0.5	64.127
CCTV surveillance system	29,278	1042≈1737*0.6	28.098
Combination of these three countermeasures	85,672	1737=1737*1	49.322

If the hospital contamination can be avoided the effectiveness ratio is different because the effect is the non-closure of the whole hospital for sanitary reason, and the ratio is equal to 0.004 (0.004=85422/21152258). So, the combination of the two countermeasures produces the best effect. Another countermeasure is to ask for checking the PHD student identity, by the Italian Home Affairs.

In this scenario, we have not taken into account the number of deaths due to the SARS epidemic, because this requires a more complex (the illness states of the population must be represented, some non-linear constraints specifying the population contamination must be added) and larger (a horizon of several weeks) simulation model.

3.9 Scenario 7b: TB

3.9.1 Scenario

A native Italian affiliated to an anti-gay/HIV positives organization is a medical doctor with a bacteriological back-ground; pretending to be funded by a famous pharmaceutical industry, approach the Director of OSR Foundation for a PHD in TB; he/she has been referred to the P3 "TB" lab and works there for a while; he/she has access to the P3 lab and to the repository of the TB MDR and XDR; 2) one night takes some material from the TB XDR repository; grows up enough bacteria; 3) prepares a aerial dispersion solution (nebulizer) 4) dressed as a cleaner, with enough PPE to be protected but not "strange" goes to San Luigi Centre and create a source of bacteria dispersion inside the San Luigi Centre air con system. 5) all the people visiting the Centre (all the outpatients and the inpatients + care givers + staff) have contact with the XDR TB. Outpatients: around 50 every day/around 10 new every week; inpatients: 12 beds/occupation rate around 100%; care givers: 2 for every inpatient, 1 for outpatient; staff: around 30 people 6) We can presume that after 2 months from the action there will be a increased incidence of clinical TB among the

Centre patients, the most vulnerable first (inpatients, old, sick), and then the Additional Scenario: Antrax

3.9.2 Scenario

Bacillus Anthraces, the bacteria causing Anthrax, is classified by the Center for Disease Control and Prevention (Atlanta, U.S.A.) as one of the most likely agents to be used for a biological attack (Chen et al., 2016). Our scenario supposes that an anonymous anthrax bioterrorist attack is launched in the subway access of the hospital, which is located near one of the main car-park accesses, and near a small mall, composed of restaurants, coffee-shops, hairdresser's, etc. This area receives employees, outpatients, and inpatients using the subway or the car-park, staff and outpatients for lunch or other services. The anthrax spores are dispersed by the air-handling system at period 10. We hypothesis that at period 106 (4 days after), the hospital administration becomes aware of the anthrax outbreak. From period 106, the hospital distributes the antibiotics to the infected patients. Usually, ciprofloxacin is always prescribed to treat the patients. The duration of the ciprofloxacin therapy is 60 days. At period 110, the hospital administration identifies and isolates the seat of the anthrax attack, i.e. the subway access. The terrorists had decided previously not to announce their actions until the attack's effects were widely known. Regarding the infection threshold, a third of the people going through the subway area are infected from period 10 to period 110. The whole hospital is closed for 14 days to be decontaminated, and the operational loss is equal to 21,152,258 (21152258=(1044450/365)*14*528) Euros.

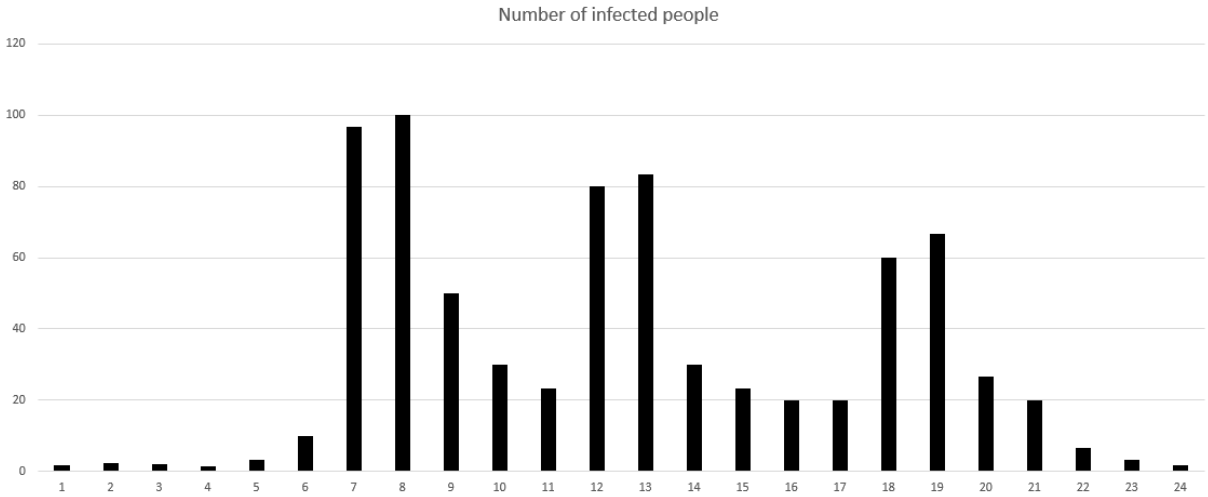


Figure 9 Number of infected people one day

3.9.3 As is system simulation

Figure 9 presents the number of infected people per day. The horizontal axis represents the time per day and the vertical axis is the number of infected patients. The infected people consist of two parts: the infected employees and the infected patients. For the employees, not all the employees will go to hospital by subway and some of them will go to hospital by car or by bus. So, we suppose that, per day, from 7.00 am to 8.00 am, 200 employees will go to hospital by subway. From 12.00 am to 13.00 pm, 175 employees will go to hospital by subway. From 18.00pm to 19.00 pm, 100 employees will go to hospital by subway. Calculating the traffic from period 10 to period 110, 3,800 employees ((3800=200+175+100)*2*4) will go through the subway, during 4 days for entrance and exit. For the patients, at the peak time, 09.00 am, the

number of patients who go through the subway is 150. At 04.00 am, the number of patients who go through the subway is less, 4 patients. The total number of patients who go through the subway is 5,928. So, the total number of people who go through the subway from period 10 to period 110 is 9,728 (9728=5928+3800). Since a third of these people are infected, the total number of infected people is 2,918 (2918=9728*30%).

3.9.4 Countermeasures

Here, we suppose two countermeasures. First, we can use unconnected atmospheric sensors in order to detect Anthrax spores by a biological test based on the polymerase chain reaction principle (BioWatch.com) in less than 1 day. Second, we can use the CCTV surveillance to detect the attack in time. An anthrax sensor costs 100 Euros and the hospital requires at least one sensor per building. The investments cost is 5,600 (5600=(100+300)*14) Euros for 14 buildings with an installation cost of 300 Euros per sensor. The biology test costs 30 Euros, and with a daily test for 14 buildings, the annual cost is 153,300 (153300=30*365*14) Euros. The cost of the CCTV surveillance is 29,278 Euros (see the Cesium 137 scenario). To treat one infected people, about 320 Euros will be spent (Drug.com). To treat 2918 people, it will cost 933,760 (933760=320*2918) Euros. We use the number of people (people who go through the subway area) who do not get infected by using the countermeasure, in order to measure the effects. If we combine these two countermeasures together, we suppose the effect will be 100% and then no people will be infected by anthrax (Hess, 2008). So hospital closure (21,152,258 Euros) and the antibiotics use (933760=2918*320 Euros), are avoided. In other words, we do not need to distribute the antibiotics. So the cost is the cost of the anthrax sensors and the cost of CCTV surveillance system, i.e. 188,178 (188178=29278+5600+153300) Euros. The effects of the sensors and the effect of the CCTV surveillance system are 90% and 60% respectively. If we use anthrax sensors or CCTV surveillance system, the number of infected people is 292 (292=2918*(1-90%)) and 1,167 (1167=2918*(1-60%)) respectively. The cost to treat the infected people is 93,440 (93440=320*292) Euros and 373,440 (373440=320*1167) Euros respectively. Therefore, the total cost of anthrax sensors and the CCTV surveillance system is 252,340 (252340=93440+5600+153300) Euros and 402,718 (402718=373440+29278) Euros each. Table 5 presents the results of the cost-effectiveness analysis. From Table 5, we can get an idea about how much should be paid if we want to protect one person by different countermeasures. For example, using CCTV surveillance, 273.97 Euros should be paid to protect one person. Based on Table 5 and on the hypothetic gain of the 21,152,258 Euros due to the non-closure of the hospital, it can be found that the combination costs less and the result is the best. It seems for us, that avoiding Anthrax spore dispersion is highly desirable. The value of the cost effectiveness ratios is the smallest for combination of countermeasures. So, it is really reasonable to choose the latter.

Table 5. Cost-effectiveness analysis of Bacillus Anthraces scenario

Countermeasures	Net cost (Euros)	Effects (Protected people)	Cost effectiveness ratio
Anthrax sensors	252,340	2,626=2918*0.9	95.98
CCTV surveillance system	402,718	1,459=2918*0.6	276.02

Combination of these two countermeasures	188,178	2,918	64.49

4 Conclusion

Regarding to the various scenarios studied, some countermeasures seem to be more convenient than others. For physical security, biometrics access control must equip all hazardous sources such as the CESIUM 137 stockpiles, virus banks, the VIP operating room, and the animal laboratory (see Table 9). For combined physical and personnel security, a CCTV surveillance system seems to us the less expensive with the best effect, if employees are motivated. This is the reason why the CCTV surveillance employee salary have to be significant, in order to avoid corruption and remain motivated and vigilant. Regarding information security, the internal emergency management plan and the external management plan have been updated thanks to these scenarios, in order to be more resilient against terrorist attacks. The patient ventilation for ICU people and the decontamination activity have been formally specified in the internal emergency management plan (see annex 1). The patient control at the entrance of the hospital has been clearly specified in the external management plan (see annex 2). Some more specific countermeasures have been already implemented by OSR to avoid a potential great number of patient deaths, for example the mobile oxygen tanks. Regarding on one hand the number of hazardous sources in the hospital, and on the other hand the ease of accessibility of the different care and technical units, we can get the conclusion that hospitals are potentially very vulnerable and that implementations of countermeasures are vital.
Despite the fact that it seems no single countermeasure covers all attack types, the increase of security personnel emerges as possible transversal measure able to increase the protection of the hospital.
To the left in this and not less important the Consortium wants to underline the potential role in increasing the resilience of the hospital against any emergencies and in particular the ones deriving from a terrorist action of the training of personnel in emergency security management.

Table 9: Countermeasure synthesis

Scenario	AS IS consequences	Countermeasures	TO BE effect
1 Second strike	3 deaths, Emergency Department closed for 2 weeks, an operational loss of 1,286,208€	Security guards: 12,739€	No death, no closure of the Emergency Department, a gain of 105,600€
2 VIP operating room	1 death	Biometrics access control and security guards: 60,394€	No death
3 A)Electric grid failure	14 days to repair, a total loss of 5,768,797€	Electric generators: 600,000€	Total loss: 1,924,423€

3	**B) Medical gas failure**	1 death, ICU closure of 2 days to repair, a total loss of 1,035,504€	Mobile oxygen tanks: 24,000 €	No death, no closure of the Intensive Care Units
4	**Cesium 137 threat**	Emergency Department closed for 2 weeks, an operational loss of 1,286,208€	Biometrics access control, Geiger sensor and CCTV surveillance: 30,428€	5.4 evacuation hours have been saved, because of an early detection.
5	**Cyber attack**	5 days no activities on site, a total loss of 7,554,378€	Paper kit system: 23,520€	Total loss 1,510,875€ = 7,554,378€ * 20%
6	**Animal experiment laboratory**	Decrease of 3% of the hospital turnover over 2 years: 326,113,800€	CCTV surveillance: 29,278€	Total loss 130,445,520€ = 326,113,800€ * 40%
7	**A)SARS threat**	Hospital closed for 2 weeks, a total loss of 21,152,258€	Biometrics access control: 700€	868 protected persons over 1737
8	**Optional Scenario: Bacillus anthraces**	Hospital closed for 2 weeks, a total loss of 21,152,258€	Anthrax sensors, CCTV surveillance: 188,178€	2918 protected persons

The process of modeling the scenarios and the use of these to point out the hospital vulnerabilities and the possible countermeasures represent a tool to increase the resilience of hospitals against terrorist attacks. The integral use of our vulnerability approach, in order to identify, to specify, and to respond to threat scenarios can be used as a tool by the hospitals (see deliverable D3.3), but individual steps of our approach can be also used separately for different purposes: to find threat sources, to define critical assets, to calculate the critical asset attractiveness, to define threat scenarios, and to assess threat scenarios. As one of hospital standards for emergency management, some of European governments such as the Joint Commission in Italy, require hospitals to perform an annual hazard vulnerability analysis. This is defined as “the identification of hazards and the direct and indirect effect these hazards may have on the hospital”. Steps 1 to 3 of our vulnerability approach, allows them to realize such hazard vulnerability analysis. In such a case the threat sources can include natural adversaries such as earthquakes, hurricanes, floods, etc. Currently, we carry out such a study for a home health care hospital in Lyon.

The THREATS consortium, tries to delineate realistic and useful terrorist scenarios, by trying to identify and quantify the hazards and threat likelihoods. Regarding the likelihood of the terrorist attacks, some preliminary data sources about terrorist events are becoming more available like the Global Terrorist Database (http://www.start.umd.edu/gtd/). According to some authors, we propose to consider

the ease of causing threats by potential adversaries, to better evaluate the likelihood of the terrorist attacks. The ease of causing the threats, is based on motivations and capabilities of attackers, and can vary with the attractiveness and the ease of access to the target. Based on the attractiveness of the critical assets for potential targets, we can brainstorm on scenarios of terrorist attacks: the most likely scenarios with the worst consequences are constructed. As a set of terrorist scenarios has been developed, on one hand some risk assessment knowledge is required to evaluate the resulting impact of the scenarios, and on the other hand some vulnerability assessment knowledge is needed to understand, how to reduce, and to eliminate, the resulting impact of the adverse events. The vulnerability assessment is reliant on: the definition and implementation of countermeasures at the mitigation level, and the specification of emergency management plans at the preparedness and response levels.

The deliverable D3.4 through the description and analysis of the different scenarios, the use of the "as is model" and simulation comes up with countermeasures to better protect hospitals against the terrorist threat ("to be model"). In D3.5 all the THREATS tools (The THREATS way) to increase the protection of the hospitals will be summarized and specified.

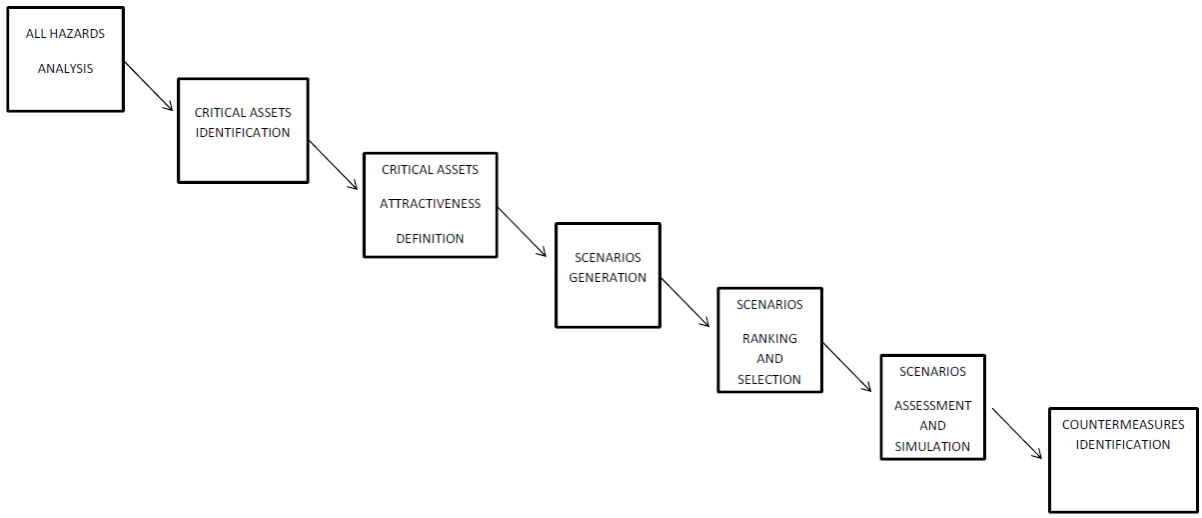


Figure 10: The THREATS way

5 References

Ambulance.com: http://health.costhelper.com/ambulance.html

An2v.org : Association Nationale de la Vidéo-protection. (2015). "Guide de référence de la vidéo protection", www.an2v.org.

air.com: http://www.fdmatfrance.fr/img/pdf/tarifs_air_liquide.pdf

Axis.com :
http://www.axis.com/files/whitepaper/wp_cost_comparison_41264_en_1012_lo .pdf

BioWatch.com: http://www.ncbi.nlm.nih.gov/books/NBK201349/

Brownyard, T., (2016). “Security Officers or Video Surveillance: Your Best Option”, Security Magazine, http://www.securitymagazine.com/articles/85950-security-officers-or-video-surveillance-your-best-option

Cellini, S. R., & Kee, J. E. (2010). Cost-effectiveness and cost-benefit analysis. Handbook of practical program evaluation, 493

Chen W., Guinet A., And Ruiz A., (2016). “Modeling the Logistics Response to a Bioterrorist Anthrax Attack”, European Journal of Operational Research, doi:10.1016/j.ejor.2016.03.052.

CHU42.com: http://www.chu-st-etienne.fr/Media/communiquepresse/2014/panneinfo.pdf

CNN. 2005. World. [ONLINE] Available at: http://edition.cnn.com/2005/WORLD/meast/06/26/iraq.main/. [Last accessed 20 June 2016].

CNN, 2008. Asia. [ONLINE] Available at : http://edition.cnn.com/2008/WORLD/asiapcf/07/26/india.blasts/index.html#cnnSTCText. [Last accessed 20 June 2016].

Drug.com: http://www.drugs.com/price-guide/ciprofloxacin

Fierce Biotech, 2009. [ONLINE]. Available at: http://www.fiercebiotech.com/research/peta-spy-infiltrates-utah-biomedical-lab. [Last accessed 20 June 2016].

Ganor, B., Halperin-Wernli, M., (2013). “Terrorist Attacks against Hospitals Case Studies, in: International Institute for Counter-Terrorism (ICT)”, Israel, working paper 25, October, (Available on line http://www.ict.org.il/Article/77/Terrorist-Attacks-against-Hospitals-Case-Studies).

Grange, H., and Leynon, J., (2015). “Crisis management plan: preventive measures and lessons learned from a major computer system failure”, HCSE 2015 Second International Conference on Health Care System Engineering , Lyon, France, 12 pages.

Greta : http://www.worldsalaries.org/italy.shtml

Gaudioso, J. and Salerno, R. M. (2009). International Biological Threat Reduction Global Security Programs Sandia National Laboratories. Available at: http://www.biosecurity.sandia.gov/ibtr/subpages/papersBriefings/2009/Evolution_of_Biosecurity_May_2009.pdf.

The Guardian, 2015. [ONLINE] Available at: https://www.theguardian.com/us-news/2015/jan/07/shooter-va-clinic-el-paso-texas-ex-employee-threatened-victim [Last accessed 20 June 2016]

HP1.com: http://store.hp.com/FranceStore/Merch/Product.aspx?id=BW868AA&opt=&sel=ACC

HP2.com: http://www8.hp.com/us/en/solutions/business-solutions/printingsolutions/ljfonts/ barcode.html

Hess, K., (2008). "Introduction to private security", Nelson Education, Wadsworth Publishing, ISBN: 0534632041.

Hutubessy, R. C., Baltussen, R. M., Torres-Edejer, T. T., & Evans, D. B. (2001). Generalised cost-effectiveness analysis: an aid to decision making in health. Applied Health Economics and Health Policy, 1(2), 89-95.

International Atomic Energy Agency, (1988). Available at: http://www-pub.iaea.org/mtcd/publications/pdf/pub815_web.pdf. [Last Accessed 20 June 2016]

Kash, T. J., & Darling, J. R. (1998). Crisis management: prevention, diagnosis and intervention. Leadership & Organization Development Journal, 19(4), 179-186.

Meglan, 2015, http://meglan.net/about-us-remote-video-monitoring/remote-video-monitoring-security-company/

Milano Cronaca, 2012. [ONLINE]. Available at http://milano.corriere.it/notizie/cronaca/14_novembre_28/trivulzio-condannato-ex-dipendente-haker-vendetta-c95a7e48-770d-11e4-90d4-0eff89180b47.shtml?refresh_ce-cp [Last accessed 20 June 2016].

Network World, 2009.

Norse, 2014: http://searchnetworking.techtarget.com/news/2240214827/Study-Malicious-attacks-at-hospitals-risk-patient-data-health

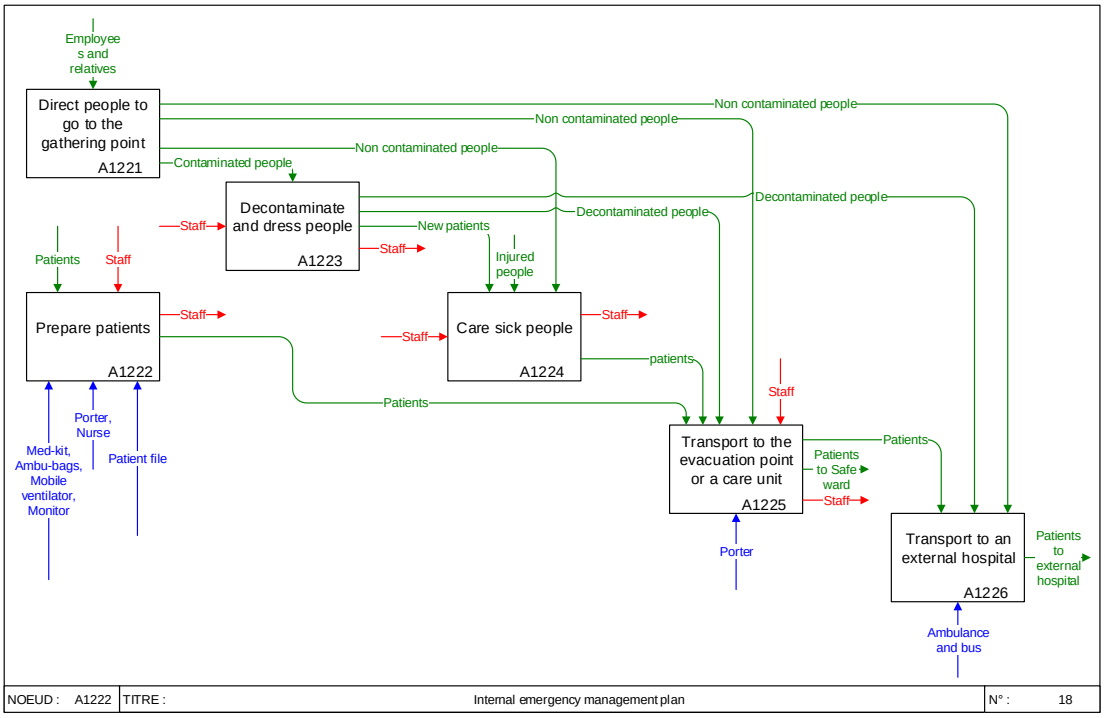
Pce.com: https://www.pce-instruments.com/english/measuring-instruments/test-meters/ geiger-counter-kat_40582_1.htm

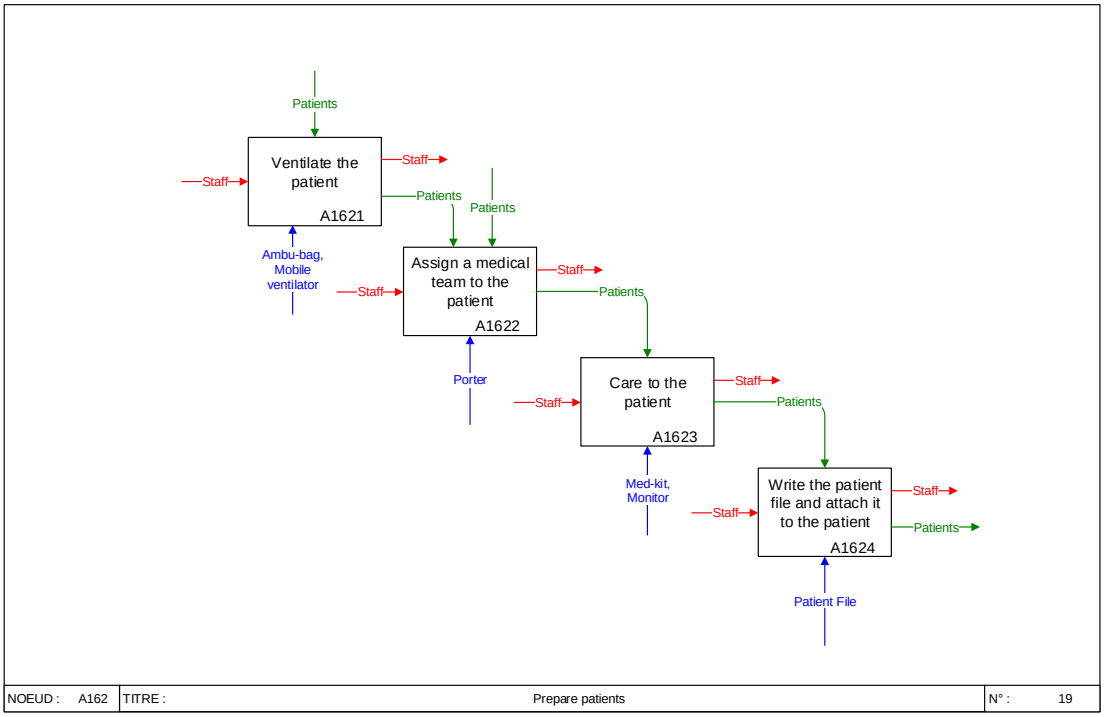
Security.com: https://www.bt-security.com/serrure-biometrique-a-empreinte-digitale-et-code-samsung-ezon-shs-h700.html

ServerPrice.com : http://www.experience-pc.de/pc/900075/0-0-0/SER-Server-Garantie-36M-bis-4000-EUR.htm

Suddle, S. (2009). The weighted risk analysis. Safety Science, 47(5), 668-679.

6 Annex 1: New internal emergency management plan





7 Annex 2: New external emergency management plan