TO WHAT EXTENT CAN BUSINESSES' SECURITY MEASURES RESPOND EFFECTIVELY TO TERRORIST ATTACKS

By Andreas Nickolaos Akratas, B.Sc. (Hons), M.A.
F.I.M.S, F.I.Manf., F.Prof.B.T.M., F.I.P.F.M., F.C.A.M.

The aim of this assignment is to critically examine to what extent security measures can respond effectively to terrorist attacks against private companies. The high level of uncertainty and complexity in today's business environment and the technology involved have increased the exposure of organisations to a number of risks, including the risk of terrorist attacks. In fact, terrorism can have a tremendous impact on international businesses (Tuggey, 2012). The emphasis on the impact - especially the economic impact - of terrorist actions to international businesses has followed the events of 9/11 (Llorca-Vivero, 2008, p. 169; Jain and Grosse, 2009, p. 43). Consequently, every organisation should be able to deal effectively with any threat, including terrorist threats that may cause business disruption (Wood, 2012a, p. 4).

An interesting question that can be posed at this point is whether or not security measures can effectively anticipate terrorism. This assignment will provide an answer to this question, by supporting the idea that the implementation of the security measures of private companies, operating in different sectors, are realistically effective in helping them to deal with the threat of terrorism.

In particular, the definition of terrorism, the concept of security management, the procedure of risk assessment and the case of terrorism against private companies will be examined. On account of the strong negative impact of terrorist attacks on companies, organisations have designed, adopted and applied security measures so as to prevent terrorist attacks and to minimise the losses resulting from potential threats. Therefore, this assignment will explain how planning and implementation of security measures help companies to prevent and respond to terrorist attacks, by providing examples and evaluate the effectiveness of the measures taken by private companies as a response to terrorism. In addition, it will analyse the concept of business continuity, since companies should ensure their sustainability and profitability after a terrorist attack has occurred. Finally, this paper will conclude with the main findings of the study and make suggestions for further research in ensuring business continuity and effective response to terrorism on the part of private organisations.

The term 'terrorism' was introduced by the English writer Edmund Burke, who was a first-hand witness of the violence during the French Revolution of 1789 (Dodds, 2005, p.199). Pokempner (2002, p. 22) points out that terrorism "was coined originally to describe State action, specifically that of the revolutionary regime in France of 1793-4, designed to consolidate the new government's power against all perceived subverives and dissidents".

It is rather difficult to determine the meaning terrorism precisely, because of its complexity and its constantly changing nature (Perl, 2007; Lawless, 2007/2008, p. 147). The Federal Bureau of Investigation (FBI) defines terrorism as the illegal use of power and violence against civilians and/or property, with the intention to frighten or coerce people and governments in the pursuit of political goals (Ronczkowski, 2004, p. 18). Kaur (2007, p. 82) determine terrorism as "the calculated use of violence or the threat of violence to inculcate fear that is intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological." Macias (2002, p. 281) mentions a new definition of terrorism, which involves any act of physical, emotional, material or spiritual violence imposed by either a person or a group of people against other people and/or groups of people. For Turk (2004, p. 273), terrorism is "the deliberate targeting of more or less randomly selected victims whose deaths and injuries are expected to weaken the opponent's will to persist in a political conflict."

In legal terms, terrorism is clarified in the U.S. Code as the intended use of violence motivated by political reasons against civilians (Dunlap, 2002, p. 23). According to the somewhat broader definition of the U.S. Department of Defence, terrorism can be regarded as the intentional use and/or threat of illegal violence to create fear, either in governments or societies, for the purpose of achieving political, ideological or religious goals (Dunlap, 2002, p. 23; Ronczkowski, 2004, p. 18). Furthermore, the U.S. State Department describes terrorism as the deliberate attack of various groups of civilians, aiming at influencing people (Cooper, 2004, p. 30).

Nevertheless, the concept of terrorism has changed following the events of 9/11 (Mythen and Walklate, 2008, p. 221). Prior to 9/11, terrorism was used as a means of violence in order to achieve political goals via fear or coercion; after 9/11, terrorism was considered to be a critical issue in the business world because if its impact on the commercial sector (Wernick and von Glinow, 2012, p. 731). Moreover, since 9/11, the threat that was posed by organised crime has given way to the threat of terrorism, which is partially funded by crime (Levi, 2007, p. 773). Last, but not least, it should be noted that terrorism consists of eight variables: a) use of violence, b) a requisite intention, c) a victim, d) a wrongdoer, e) a just cause, f) an organisation, g) a theatre and h) the absence of feelings of guilt or remorse (Fletcher, 2006, p. 901). In the case of organisations, terrorism constitutes a type of business risk called ‘terrorism risk’ or ‘security risk’ which has an impact on the operations of multinational companies and/or their value chain partners, resulting in revenue losses and missed business opportunities (Jain and Grosse, 2009, p. 48).

Krahmann (2008, p. 382) offers three meanings of the term ‘security’. In the first case, security is the non-existence of a threat, in the second it refers to threats that exist and are possible, while in the third case it refers to security as a threat that actually occurs. Security strategies can be distinguished as either proactive, which target avoiding events that may disrupt operations and functions, or reactive, which look to handle events that may occur in the future (Leathrum *et al*., 2010, p. 697). Generally, security refers to the long-term plans and projects of an organisation (Wood, 2012e, p. 3). Security planning requires that the security manager build a strategy so as to prevent, respond to and recover from any potential threat according to a thorough risk assessment (Wood, 2012c, p. 2).

Security management includes tasks such as “running a department with staff (possibly on several different sites); planning future outcomes; budgeting’s controlling outcomes and monitoring performance; interacting with other departments and corporate senior executives; making department policy; and working with other people and organisations outside the corporation such as the police, prosecution services, and other security officers" (Bamfield, 2006, p. 485). As a matter of fact, security management places emphasis on the protection of the organisation's assets, the health of both employees and customers, the protection of information and data, and ensuring a safe working environment (Bamfield, 2006, p. 489). This derives from the fact that a terrorist attack on an organisation may affect property, assets, people, information, products/services, operation, reputation and environment (Wood, 2012b, p. 2). Consequently, given the definition of Mullins (2008, as cited in Wood, 2012c, p. 3), it can be argued that security management comprises the coordination of all of an organisation's departments and the guidance of all the members of a company by the security manager in the direction of achieving the goals of securitising the company's people, information, production processes, reputation and continuity of business, all while taking into account the overall strategic goals of the business. What should be mentioned here is that security management is effective only in the case where the implemented security measures are commensurate with the threat that the organisation faces, taking into account its assets and losses (Moodie, 2005; Smith, 2012).

Within the framework of the adoption and implementation of security measures, the process of risk assessment is essential, as terrorism is a risk-management issue for organisations (Global Business Summit, 2009, p. 3). Risk assessment "is the process by which businesses and organisations focus on critical areas of concern and prioritise their use of resources in order to maximize response and recovery efforts. In making strategic decisions, business and government leaders routinely try to predict the benefits and/or harm that might be caused by implementing or failing to implement those decisions" (Hughbank and Hershkowitz, 2009, p. 155). The process of risk assessment involves the following six steps: a) a definition of the critical infrastructure and a key asset inventory, b) a criticality assessment, c) a threat assessment, d) a vulnerability assessment, e) a risk calculation and f) the identification of countermeasures (BJA, 2005a, p. vii). During the process of risk assessment, there are five stages: a) the understanding of any potential loss and their vulnerability to these losses, b) the evaluation of risk analysis tools and techniques, c) a definition of a risk evaluation strategy, d) the selection of a process for risk evaluation, and e) the establishment of risk avoidance measures (Charters, 2007, p. 138).

Initially, it should be mentioned that the need for security measures against terrorism in general and - more specifically - the measures taken by private companies against terrorist attacks stem from the fact that, nowadays, terrorists have available to them a wide range of high-technology and weapons of mass destruction, such as chemical and biological agents, lasers and precision-guided ammunition, all of which have even greater negative consequences (Nincic, 2005, p. 619; Kaur, 2007, p. 82). The ‘new terrorism’, after the events of 9/11, calls for new counter-terrorism measures (Howell and Lind, 2010, p. 280). Secondly, transnational terrorism leads governments to a restriction of human rights in favour of improving security (Piazza and Walsh, 2009, p. 129). Thirdly, and foremost, the major reason why security measures against every form of terrorism are essential is the impact of terrorism. Specifically, terrorist attacks usually target civilians and large populations so as to create insecurity and injury (Mythen and Walklate, 2006, p. 381). Kaur (2007, p. 82) claims that terrorism is a psychological act with an intention to produce fear, and there is also the potential for nuclear destruction. The deployment of hi-tech weaponry by terrorists has created a new era of terror, whereby all societies are at risk of terrorist (Mythen and Walklate, 2006, p. 379). However, the impact of terrorism goes beyond the creation and imposition of fear in populations and includes major disruption in the everyday life of many people (Hauss, 2003).

Apart from the loss of peoples’ lives and the destruction of property, terrorism constitutes a threat to international business, global commerce and the global economy (Mazzarella, 2005, p. 59). A terrorist attack may disrupt the transportation of goods and the flow of services (Global Business Summit, 2009, p. 2). In interrupting the flow of goods and services, terrorist attacks may have a negative impact on employee travel, on money transfers and on information and network security (Jain and Grosse, 2009, p. 49). What is more, terrorism has caused a dramatic decrease in the aviation industry’s profitability as well as in the tourism and hospitality sectors, whereby foreign products are more expensive because of the imposed security and transaction costs (Alavosius *et al*., 2003, p. 6). The cancellation or delay of future investment may be another negative result of terrorist attacks on business (Alexander, 2004, p. 150).

Hardware improvements are the first measures an organisation can take in improving physical security in terms of confronting the threat of terrorist attacks (Avant and Haufler, 2012, p. 259). These improvements include the establishment of metal detectors in building entrances, the installation of reinforcement doors and - especially - the installation of closed-circuit surveillance cameras (Mazzarella, 2005, p. 60). It is argued that Closed Circuit Television (CCTV) can contribute to the reduction of crime and strengthen people's sense of security (Hempel and Topfer 2002; Waples *et al*., 2009). It cannot be doubted that CCTV and in general surveillance camera technology is very effective in tackling crime. CCTV is an effective tool, since it can provide a means by which a company can control the extent to which its employees comply with the organisation's processes, as well as the extent to which their behaviour is in line with the organisation's policies (Gill, 2006, p. 440). The effectiveness of surveillance camera technology lies in its ability to provide images and information as regards to whether an event has occurred which facilitates the investigation of criminal acts and the criminals. Furthermore, the unwitting victims can be helped and supported through the images that CCTV cameras capture. Thus CCTV cameras can serve as a means of immortalising facts (Morgan, 2012).

Some organisations may choose to hire additional security personnel to protect both their property and their employees (Mazzarella, 2005, p. 60). This strategy, though (namely the hiring of additional security personnel) may have a negative impact on employees' psychological well-being and sense of security because of the attendant feeling of danger. Despite the further cost to international organisations, the choice can also be made to hire external security consultants in preparation of mitigating the impact of terrorist threats to business activities. It is characteristic of this that, by January 2013, seven major international companies had joined ‘The Corporate Preparedness Security, and Response Network’, with an annual fee of $10,000 (Mazzarella, 2005, p. 61).

Another security measure that can be implemented is the development of enterprise resilience (Jain and Grosse, 2009, p. 62). Resilience might be defined as “an ability to recover from or adjust easily to misfortune or change’ or the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress” (Kumar *et al*., 2011, p. 5449). Basically, resilience is related to the ability of a company to re-invent its strategies and business model according to changing circumstances, as in the case of a terrorist attack (Demmer *et al*., 2011). In this context, Ates and Batitci (2011) assert that, if companies intend to be resilient, they should adopt the philosophy of change management, which means that they should focus on long-term planning, the use of external communication and, above all, include all their human resources. Moreover, companies should redefine their strategies and operations through cost-benefit analysis and conduct risk-reduction planning (Jain and Grosse, 2009, p. 63).

A potential terrorist threat to international business may harm its supply chains, which can have a tremendous economic impact on corporations (Jain and Grosse, 2009, p. 59). On the one hand, this impact derives from the resultant higher cost of securing the transportation of goods, while on the other hand, it also derives from the delay or disruption in the supply chain. For this reason, some countries, as the U.S., have imposed some extra restrictions in their shipping regulations with a view to increasing security; however, these restrictions have resulted in unpredictable costs and increased complexity for international companies (Mazzarella, 2005, p. 62). The companies themselves employ methods to mitigate the risk involved in a potential terrorist attack on supply chains. For instance, companies may choose to have suppliers based in different locations or else local suppliers instead of depending exclusively upon foreign suppliers (Jain and Grosse, 2009, p. 59). The rational use of military resources and cooperation between organisations, armed forces, police forces, intelligence agencies and relevant ministries are considered key strategies in responding to terrorist threats (Band, 2002, p. 26).

Raymond (2006, p. 254) claims that cooperation between states, namely -multi-lateral cooperation- can be efficient in terms of combating terrorist attacks in relation to the transportation of goods. Moreover, some organisations choose to hold excess inventory, whereas others prefer to increase their on-hand inventories of items with low holding cost and employ pleonasm in supply sources of items with high holding costs (Mazzarella, 2005, p. 64). Companies can also make use of technology in the case of cargo shipping (Jain and Grosse, 2009, p. 59). On the whole, high shipping security measures along with the maintenance of appropriate inventory levels mark the strategy applied by international companies to overcome the cost of terrorism and prevent loss from terrorist attacks. Air cargo security in relation to terrorist attacks can be increased by the use of technology, as mentioned earlier, along with the existing use of metal detectors and the careful inspection of passengers and their luggage, all of which have proved to be effective measures (Hoffman, 1998, p. 56). With reference to maritime port security, Harris *et al*. (2013, p. 197) highlight the importance of exploiting the natural geography of maritime activity. More precisely, it is advanced that the act of establishing patrols at all checkpoints restricts the opportunity to use other pathways as well as ensuring the efficient use of patrol resources made available through existing law enforcement.

In considering the examples of the cruise ship and aviation industries, Bowen *et al.* (2013, p. 22) argue that most companies are not willing to take measures promoting safety against a terrorist attack, such as reinforced cockpit doors that will separate pilots from passengers, body scanners and searches and luggage restrictions, since these measures are considered unpopular and unattractive to tourists; as a result, such measures may lead to reduced satisfaction of customers. As far as the aviation industry is concerned, Hastings and Chan (2013, p. 793) underline that the increased security measures that have been taken after 9/11 were not the desirable outcome, since the restrictions imposed have not communicated the messages that the policymakers wanted, but on the contrary they have aided terrorists in communicating theirs. Concerning the measures taken at ports for maritime security, the effectiveness of port patrols is in doubt since they can lead to anxiety for seafarers. Both port security and border personnel may have a negative attitude towards seafarers, and this may be indicative of the fact that “security and seafarers’ welfare are not viewed in a holistic manner and the industry should strive for harmonization of these important areas” (Graham, 2009, p. 72). Finally, it is argued that many commercial premises may not be in a position to take measures in anticipating terrorist threats because they have no access to high quality intelligence, buildings are not fortified and the existence plans are outdated (The Foreign Police Centre, n.d.).

Companies operating in the chemicals industry use guarded and secured facilities with limited public access, remote locations, special deterrents, a global transportation network and cyber technology (NIAC, 2012, p. C-3). The security of the Commercial Facilities Sector is more problematic, since these types of businesses are open to the public. Access control, cyber technology, communication centres and CCTV are among the most prevalent tools used by firms in this sector (NIAC, 2012, p. D-4). Shull (2006, p. 15) analyses how the energy infrastructure in Canada is protected from terrorist threats by the use of cyber security measures, the deployment of resiliency standards in densely populated areas (as motivated by the Canadian government), the use of DC instead of AC lines and decentralised generation. Copeland (2010, p. 17) discusses the security measures implemented by the water infrastructure sector. It is noted that such facilities are subjected to legislation regarding safer technology pertaining to the chemical plants and facilities that handle chemicals. Furthermore, in order to address critical infrastructure protection issues, the private sector has moved towards the creation of information analysis and infrastructure protection departments (Eckert, 2006, p. 8).

Expansion through direct investment is a common practice owing to the theory of internationalisation as a source of competitive advantage for many firms (Zahra *et al*., 2009). Nevertheless, international businesses have become more sceptical of this practice because of the threat of terrorism. Within this framework, corporations consider the geographical area into which they wish to expand and may choose to reduce their direct capital investments and operations in areas which are considered to be high risk (Mazzarella, 2005, p. 64). Avant and Haufler (2012, p. 259) claim that many corporations choose a strategy of avoidance namely not entering into markets considered to be high-risk areas while others withdraw from conflict-torn areas and move their operations elsewhere .

Based upon the concept of internationalisation, some companies may be willing to expand their business and gain additional benefits in high risk areas. In this case, they tend to use expatriates in the foreign branches. Expatriates are those “employees who live and work in foreign countries on short-term or long-term assignments” (Mazzarella, 2005, p. 65). This practice helps the firms, on the one hand, to be culturally aware of the foreign country, and on the other, to build interpersonal networks of global contacts. Based on this, some organisations may be willing to operate in countries where governments, rebels and civil society regard them as apolitical parties (Avant and Haufler, 2012, p. 261). However, it has been argued that the use of expatriates may lead to increased terrorist attacks against multinational companies (Mazzarella, 2005, p. 66).

One main measure that can be taken by corporations to mitigate the threat of terrorist attack is political risk insurance, whereby political risk is defined as the loss of someone’s investment in a foreign asset that may occur as a result of political or other types of instability in a host country (Mazzarella, 2005, p. 68). Insurance is a strategy used by many firms to remain financially viable (Barnes, 2001, p. 116). Finally, one measure within the scope of the disaster planning of the companies is the establishment of convergent IT/Security applications, along with the storage of paper records and ‘off site’ computer backups (Widenbaum, 2003, p. 11). Miiwald and Sieglein (2002, p. 54) emphasise data backup and recovery as a measure that will help companies to mitigate their losses resulting from a terrorist attack.

However, it is supposed that the so-called ‘alliance strategy’ is much more effective, since it refers to the cooperation of organisations with governments and/or local violent actors. Taking into consideration such cooperation, it also stated that some NGOs consider building an alliance with the humanitarian community (Avant and Haufler, 2012, p. 260). The significance of public and private partnership in combating terrorism is mentioned by Alexander (2004, p. 104) and Connolly (2003) as well. For instance, in the U.S's chemicals sector some corporations collaborate with public sector agencies on security issues through chemicals industry associations, such as the American Chemistry Council, the International Liquid Terminals Association, the Society of Chemical Manufacturers and Affiliates, the Institute of Makers of Explosives and the National Association of Chemical Distributors. Moreover, companies from other sectors of the economy have also created industry associations for security purposes, like the Real Estate Roundtable, the Real Estate Information Sharing and Analysis Centre, the Retail Industry Leaders Association, the Building Owners and Management Association, the American Hotel and Lodging Association, and the National Retail Federation (NIAC, 2012, p. 39).

Within the context of counterterrorism methods for business and collaboration with other agencies -private or state- engaged in fighting terrorism, Popp and Poindexter (2006, p. 24) stress that the adoption and implementation of advanced information and privacy protection technologies may be effective. This is based on the fact that the detection of a potential terrorist attack is one of the major challenges in countering terrorism. Information technology can play a crucial role in counterterrorism strategy, since it adds the ability to connect and make sense of all the available information provided to and coming from counterterrorism agencies**.**

The above considerations lead to the introduction of the term 'counterintelligence', which pertains to the information that the private sector is attuned to (NIAC, 2012, p. 39). Within the framework of security, company resilience and asset protection, intelligence offer firms the ability to be prepared for any potential threat that may occur in the future (Wood, 2012d, p. 6). Intelligence collection began after the events of 9/11, since before this date the FBI did not have a procedure to manage its intelligence collections in an effective way (National Commission on Terrorist Attacks upon the United States, 2004, p. 7). Intelligence is important for the decision-making process, planning, strategic targeting and the prevention of terrorist attacks (BJA, 2005b, p. 3). As a matter of fact, some multinational corporations in the Oil and Natural Gas sector cooperate with intelligence agencies in the exchange of information about counterintelligence issues

(NIAC, 2012, p. 39**).** Intelligence-led practices can provide suitable information to policymakers and justice officials (Belli, 2012, p. 4). Intelligence is important to counterterrorism, given the fact that it can reduce the tactical effects and the strategic importance of terrorism (Karmon, 2002, p. 119). Conolly (2003) states that the private sector in the U.S. has the resources and analytical intelligence to contribute to the security of the American nation, whereas Schmidt (2011, p. 31) asserts that intelligence is the first most frequently mentioned measure in the international literature on combating domestic terrorism. Nevertheless, it should be pointed out that intelligence and 'sousveillance' - which is surveillance via cameras or electronic listening devices at the 'human level'- can lead to abuses on the part of the governments (Sinai, 2013, 128).

It cannot be doubted from the above considerations, that security measures can be effective in preventing terrorist attacks and confronting the risk stemming from a potential terrorist act, despite the fact that some policies may not be fruitful as mentioned before. Companies should follow certain basic guidelines with a view to increasing the effectiveness of security measures (Miiwald and Sieglein, 2002, p. 59). Initially, they should make sure that the adopted policies and implemented measures are in accordance with the goals of the firm, industry standards an existing laws and regulations. Second, the policy should set out at a sufficiently detailed level. Third, the company should review, revise and update its adopted policies frequently so as to be up-to-date in relation to the risks that the company faces. In any case, from the above analysis it can be concluded that the security measures that companies implement can contribute towards their business continuity or else crisis management (Borodzicz, 2005, p. 85).

Business continuity is essential for the sustainability of businesses following a terrorist attack. Business continuity aims at avoiding crises through risk mitigation, at using plans to effectively manage crises and at making use of plans to recover quickly and effectively from crises (Blyth, 2009, p. 9). Business continuity is defined under the standard BSI 25999 as the "strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level" (Ramakrishnan and Viswanathan, 2007, p. 97). Under the alternative definition of standard PAS 56, business continuity is a “holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities” (Ramakrishnan and Viswanathan, 2007, p. 97).

Recovery from a disruptive event, like a terrorist attack, has two phases. The first is the immediate reaction, whereby clean-up and operational strategies are implemented. The second is long-term recovery, which refers to how the organisation handles any delay due to the disruptive event (Leathrum *et al*., 2010, p. 697). Apart from the proactive and reactive strategy presented above -which underlie provision of the business continuity- Elliott *et al*. (2005, p. 53) add one further element, an interactive strategy, according to which companies consider how their needs are based on their organisational and environmental pressures and how this can assist them to take the necessary actions. What is needed is business continuity planning. This can be defined as “the identification and protection of critical business processes and resources required to maintain an acceptable level of business, protecting those resources and preparing procedures to ensure the survival of the organisation in times of business disruption” (O’Hehir, 2007, p. 27). The business continuity management lifecycle involves the following four steps: a) understanding the organisation, b) determining the business continuity management strategy to be adopted, c) developing and implementing the chosen business continuity management strategy, and d) exercising and reviewing the strategy (Cornish, 2007, p. 107).

There are some steps that can be taken to ensure business continuity. Frey (2009, p. 784) asserts that after a terrorist attack has occurred, businesses should make a quick response to the attack and be ready for the rapid reconstruction of both physical and human capital. Insurance coverage constitutes another effective strategy in relation to business continuity. In particular, business interruption insurance covers the loss of net profit which a company faces after a terrorist attack and the continuity expenses that the company should pay during the disruption of its operations (Barnes, 2001, p. 117).

An interesting aspect of ensuring business continuity is given by the paradigm from the tourism sector. More precisely, and with reference to the hospitality and travel sectors, Llorca-Vivero (2008, p. 185) points out the significance and effectiveness -at least to some extent- of marketing practices in order to boost these sectors of the economy after a terrorist attack has occurred. Such practices include, for example, the organisation of inexpensive tour packages aimed at specific groups of people, business loan programmes and funding from both the private sector and the government to stimulate travel. Other measures include the redevelopment of transport route networks, improvements in immigration services and the provision of tax incentives (Henderson, 2003, p. 49).

In conclusion, the term ‘terrorism’ can be used to describe any criminal activity, including the use of violence, with the intention to stimulate fear and impose terror, which causes physical injury to someone, or the treat of such injury, as well as the destruction of property (Guillaume, 2004, p. 540). Above all, terrorism can be regarded as an international crime and, thus, it should be fought as such (Lawless, 2007/2008, p. 139). Terrorism can have a tremendous negative impact on international businesses, especially given the fact that this kind of risk can occur randomly and unexpectedly (Jain and Grosse, 2009, p. 48). Due to the emergence of this risk, corporate security has become a core topic in management rather than just the peripheral business activity of the past (Jain and Grosse, 2009, p. 65). Corporations adopt and apply policies and strategies that help them in mitigating the risk of potential terrorist threats and which ensure their business’s continuity, even though this process can be both time-consuming and costly (Elliott *et al*., 2005, p. 53; O’Hehir, 2007, p. 27).

However, it is advanced that the above-mentioned security measures may not always come out the desired result (Hastings and Chan, 2013, p. 793). Occasionally, the implementation of security measures does not give a sense of protection but on the contrary, a sense of anxiety and therefore many firms are not willing to adopt them (Bowen *et al.* 2013, p. 22; Graham, 2009, p. 72). The importance of securing a business’s infrastructure is vital and should concentrate on long-term planning. Long-term security planning could address some of the major causes of terrorism; hence, the security of facilities should be revaluated concerning the company’s financial interest and ensure the continuity of its operations and functions (Ates and Batitci, 2011; Jain and Grosse, 2009, p. 63). Consequently, in future, organisations need to develop more effective and less costly countermeasures against terrorist threats.

Overall, more effort should be made in the security domain in concentrating on preventing terrorist attacks. The cooperation of the private sector with governments in combating terrorism is one of the most important aspects of security, along with intelligence (Schmid, 2011, p. 32). After integrating the concept of terrorism in relation to the impact of terrorist attacks to business, organisations would be able to implement plans that will effectively prevent, respond to and address potential terrorist attacks, thereby ensuring their sustainability, viability and profitability.

References

Alavosius, M.P., Braksick, L.W., Daniels, A.C., Harshbarger, D., Houmanfar, and R., Zeilstra, J. (2003) The Impact of Terrorism on the US Economy and Business. *Journal of Organizational Behavior Management*. **22**(4), pp. 3-26.

Alexander, D.C. (2004) *Business Confronts Terrorism. Risk and Responses*. Madison: The University of Wisconsin Press.

Ates, A. and Bititci, U. (2011) Change process: a key enabler for building resilient SMEs. *International Journal of Production Research*. **49**(18), pp. 5601-5618.

Avant, D. and Haufler, V. (2012). Transnational organisations and security. *Global Crime.* **13**(4), pp. 254-275.

Bamfield, J. (2006) Management. In: Gill, M. (ed.) *The Handbook of Security.* Basingstoke: Palgrave Macmillan, pp. 485-508.

Band, A.S. (2002) Maritime security and the terrorist threat. *The RUSI Journal*. **147**(6), pp. 26-32.

Barnes, J.C. (2001) *A Guide to Business Continuity Planning*. Chichester: John Wiley & Sons.

Belli, R. (2012) *Effects and effectiveness of law enforcement intelligence measures to counter homegrown terrorism: A case study on the Fuerzas Armadas de Liberación Nacional (FALN).* Final Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security. College Park, MD: START, 2012 [online]. Available from: http://www.start.umd.edu/sites/default/files/files/publications/Countermeasures_FALN.pdf [Accessed 10 March 2014].

Blyth, M. (2009) *Business Continuity Management. Building an Effective Incident Management Plan*. Haboken: John Wiley & Sons.

Borodzicz, E.P. (2005) *Risk, Crisis and Security Management*. Chichester: John Wiley & Sons.

Bowen, C., Fidgeon, P. and Page, S.J. (2013) Maritime tourism and terrorism: customer perceptions of the potential terrorist threat to cruise shipping. *Current Issues in Tourism*, iFirst Article, pp. 1-30.

Bureau of Justice Assistance -BJA (2005a). *Assessing and Managing the Terrorism Threat.* U.S. Department of Justice. Office of Justice Programs, NCJ 210680 [online]. Available from: https://www.ncjrs.gov/pdffiles1/bja/210680.pdf [Accessed 12 March 2014].

Bureau of Justice Assistance -BJA (2005b) *Intelligence-Led policing: The New Intelligence Architecture.* U.S. Department of Justice. Office of Justice Programs, NCJ 210681 [online]. Available from: https://www.ncjrs.gov/pdffiles1/bja/210681.pdf [Accessed 12 March 2014].

Charters, I. (2007) Risk evaluation and control: practical guidelines for risk assessment. In: Hiles, A. (ed.) *The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, pp. 137-144.

Connolly, C.P. (2003) *The Role of Private Security in Combating Terrorism.* Presentation given at the Major Cities Chiefs/National Executive Institute's Annual Conference, Sun Valley, Idaho [online]. Available from: http://www.neiassociates.org/privatesecuritycombatingterror/ [Accessed 15 March 2014].

Cooper, B. (2004) *New Political Religions, or An Analysis of Modern Terrorism*. Columbia : University of Missouri Press.

Copeland, C. (2010) *Terrorism and Security Issues Facing the Water Infrastructure Sector.* Congressional Research Service [online]. Available from: http://www.fas.org/sgp/crs/terror/RL32189.pdf. [Accessed 11 March 2014].

Cornish, M. (2007) The business continuity planning methodology. In: Hiles, A. (ed.) *The Definitive Handbook of Business Continuity Management*. Chichester: John Wiley & Sons, pp. 105-118.

Demmer, W.A., Vickery, S.K. and Calantone, R. (2011) Engendering resilience in small- and medium-sized enterprises (SMEs): a case study of Demmer Corporation. *International Journal of Production Research*. **49**(18), pp. 5395–5413.

Dodds, K. (2005) *Global Geopolitics. A Critical Introduction*. Harlow: Pearson.

Dunlap, J. (2002) *International Law and Terrorism. Some 'Qs & As' for Operators.* The Army Lawyer. Department of the Army Pamphlet 27-50-357 [online]. Available from: http://www.loc.gov/rr/frd/Military_Law/pdf/10-11-2002.pdf [Accessed 15 March 2014].

Eckert, S. (2006) *Protecting Critical Infrastructure: The Role of the Private Sector*. University of Pittsburgh [online]. Available from: http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf [Accessed 12 March 2014].

Elliott, D., Swartz, E. and Herbane, B. (2005) *Business Continuity Management, A Crisis Management Approach*. London: Routledge.

Fletcher, G.P. (2006) The Indefinable Concept of Terrorism. *Journal of International Criminal Justice.* **4**, pp. 894-911.

Frey, B.S. (2009) How can business cope with terrorism? *Journal of Policy Modelling.* **31**, pp. 779-787.

Gill, M. (2006) CCTV*:* Is it Effective? In: Gill, M. (ed.) *The Handbook of Security*. Basingstoke: Palgrave Macmillan, pp. 438-461.

Global Business Summit (2009) *Strategic Responses to Global Terrorism*. Harvard Business School [online]. Available from: http://www.hbs.edu/centennial/businesssummit/business-society/strategic-responses-to-global-terrorism.pdf [Accessed 10 March 2014].

Graham, C.A.E. (2009). Maritime Security and Seafarers' Welfare: Towards Harmonization. *WMU Journal of Maritime Affairs,* **8**(1), pp. 71-87.

Guillaume, G. (2004) Terrorism and International Law. *The International and Comparative Law Quarterly*. **53**(3), pp. 537-548.

Harris, S.P., Dixon, D.S., Dunn, D.L. and Romich, A.N. (2013). Simulation modeling for maritime port security. *The Journal of Defense Modeling and Simulation, Applications, Methodology, Technology*. **10**(2), pp. 193-201.

Hastings, J.V. and Chan, R.J. (2013) Target Hardening and Terrorist Signaling: The Case of Aviation Security. *Terrorism and Political Violence*. **25**(5), pp. 777-797.

Hauss, C. (2003) *'Terrorism' Beyond Intractability. Conflict Information Consortium*. University of Colorado, Boulder [online]. Available from: http://www.beyondintractability.org/bi-essay/terrorism. [Accessed 15 March 2014].

Hempel, L. and Topfer, E. (2002) *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*. Working Paper No1, Urbaneye: Inception Report. Centre for Technology and SocietyTechnical University Berlin [online]. Available at http://www.ideels.uni-bremen.de/ue_wp1.pdf [Accessed 12 March 2014].

Henderson, J.C. (2003) Terrorism and Tourism. *Journal of Travel & Tourism Marketing*. **15**(1), pp. 41-58.

Hoffman, B. (1998) Aviation security and terrorism: An analysis of the potential threat to air cargo integrators. *Terrorism and Political Violence*. **10**(3), pp. 54-69.

Howell, J. and Lind, J. (2010) Securing the World and Challenging Civil Society: Before and After the 'War on Terror'. *Development and Change*. **41**(2), pp. 279-291.

Hughbank, R.J. and Hershkowitz, M. (2009) Fundamentals of Terrorism: Understanding the Threat and Preparing for the Next Attack. *Journal of Police Crisis Negotiations*. **9**(2), pp. 149-163.

Jain, S.C. and Grosse, R. (2009) Impact of Terrorism and Security Measures on Global Business Transactions: Some International Business Guidelines. *Journal of Transnational Management*. **14**(1), pp. 42-73.

Karmon, E. (2002) The Role of Intelligence in Counter-Terrorism. *The Korean Journal of Defense Analysis*. **XIV**(1), pp. 119-139.

Kaur, K. (2007) High Technology Terrorism: A Threat to Global Security. *India Quarterly: A Journal of International Affairs*. **63**, pp. 81-95.

Krahmann, E. (2008) Security: Collective Good or Commodity?. *European Journal of International Relations*. **14**(3), pp. 379-404.

Kumar, M., Antony, J. and Tiwari, M.K. (2011) Six Sigma implementation framework for SMEs – a roadmap to manage and sustain the change. *International Journal of Production Research*. **49**(18), pp. 5449-5467.

Lawless, M. (2007/2008) Terrorism: An International Crime. *International Journal*. **63**(1), pp. 19-159.

Leathrum, J.F., Mathew, J.R. and Mastaglio, T.W. (2010) Modeling the impact of security and disaster response on cargo operations. *Simulation: Transactions of the Society for Modeling and Simulation International*. **87**(8), pp. 696-710.

Levi, M. (2007) Organized Crime and Terrorism. In: Maguire, M., Morgan, R., Reiner, R. (eds.) *The Oxford Handbook of Criminology*. Oxford: Oxford University Press, pp. 771-809.

Llorca-Vivero, R. (2008) Terrorism and international tourism: New evidence. *Defense and Peace Economics*. **19**(2), pp. 169-188.

Macias, J. (2002) The Tragedy of Terrorism: Perspective, Reflection, and Action in the Aftermath. *Anthropology & Education Quarterly*. **33**(3), pp. 280-282.

Mazzarella, J.J. (2005) Terrorism and Multinational Corporations: International Business Deals with the Costs of Geopolitical Conflict. *Major Themes in Economics,* Spring, pp. 59-73 [online]. Available from: http://business.uni.edu/economics/Themes/mazzarella.pdf [Accessed 12 March 2014].

Miiwald, E. and Sieglein, W. (2002) *Security Planning & Disaster Recovery*. Berkeley: McGraw-Hill.

Moodie, M. (2005) *Lighters banned at US airports. What next asks ACI? The Moodie Report;* Dow Jones International [online]. Available from: http://www.moodiereport.com/document.php?c_id=1178&doc_id=6227 [Accessed 11 March 2014].

Morgan, H.M. (2012) Regulating CCTV?: We can't solve Problems by Using the Same Kind of Thinking We Used When We Created Them. *Critical Criminology* [online]. 21(1), pp. 15-30. Available from: http://aura.abdn.ac.uk/handle/2164/2675 [Accessed 15 March 2014].

Mythen, G. and Walklate, S. (2008) Criminology and Terrorism. Which Thesis? Risk Society or Governmentality? *British Journal of Criminology*. **46**, pp. 379-398.

National Commission on Terrorist Attacks upon the United States (2004) *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11*. Staff Statement No 9, Tenth Public Hearing [online]. Available from: http://govinfo.library.unt.edu/911/staff_statements/staff_statement_9.pdf [Accessed 10 April 2014].

National Infrastructure Advisory Council – NIAC (2012) *Intelligence Information Sharing. Final Report and Recommendations* [online]. Available from: http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf [Accessed 10 April 2014].

Nincic, D.J. (2005) The challenge of maritime terrorism: Threat identification, WMD and regime response. *Journal of Strategic Studies*. **28**(4), pp. 619-644.

O'Hehir, M. (2007) What is a business continuity planning (BCP) strategy?. In: Hiles, A. (ed.) *The Definitive Handbook of Business Continuity Management*. Chichester: John Wiley & Sons, pp. 27-45.

Perl, R.F. (2007) *International Terrorism: Threat, Policy, and Response*. CRS Report for Congress. Congressional Research Service [online]. Available from: http://www.fas.org/sgp/crs/terror/RL33600.pdf. [Accessed 10 March 2014].

Piazza, J.A. and Walsh, J.I. (2009) Transnational Terror and Human Rights. International Studies Quarterly. 53, pp. 125-148.

Pokempner, D. (2002) Terrorism and Human Rights: The Legal Framework. In: International Institute of Humanitarian Law. *Terrorism and International Law: Challenges and Responses,* pp. 19-29 [online]. Available from: http://www.iihl.org/iihl/Documents/Terrorism%20and%20IHL.pdf [Accessed 10 January 2014].

Popp, R. and Poindexter, J (2006) Countering Terrorism through Information and Privacy Protection Technologies. *IEEE Security & Privacy*. **4**(6), pp. 18-27.

Ramakrishnan, R.K. and Viswanathan, S. (2007) Business strategy and business continuity planning. In: Hiles, A. (ed.) *The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, pp. 97-102.

Raymond, C.Z. (2006) Maritime Terrorism in Southeast Asia: A Risk Assessment. *Terrorism and Political Violence*. **18**(2), pp. 239-257

Ronczkowski, M. (2004) *Terrorism & Organized Hate Crime*. Boca Raton: CRC Press.

Schmid, A.P. (2011). Introduction. In: Schmid, A.P. (ed.) *The Routledge Handbook of Terrorism Research*. Abington: Routledge, pp. 1-38

Shull, A. (2006) *Critical Energy Infrastructure Protection.* Policy Research Series. Canadian Centre of Intelligence and Security Studies (CCISS) [online]. Available from: http://www3.carleton.ca/cciss/res_docs/ceip/shull.pdf [Accessed 10 March 2014].

Sinai, J. (2013) "Counterterrorism Bookshelf": Literature on Intelligence and Terrorism. Books & Monographs on Intelligence Agencies, the Intelligence Process and Intelligence Analytic Methods that Contribute to Improving Terrorism and Counterterrorism Analysis. *Perspectives on Terrorism* [online]. **7**(5) pp. 126-141. Available from: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/295/pdf [Accessed 15 March 2014].

Smith, P.E. (2012) *Protective Security: The Advent IM Approach to Corporate Security*. Advent IM [online]. Available from:http://www.advent-im.co.uk/user/files/Protective_Security_White_Paper_v2.pdf. [Accessed 15 March 2014].

The Foreign Police Centre (n.d.) *Companies "Failing to Prepare for Terrorist Attack"*. Press Release [online]. Available from: http://fpc.org.uk/fsblob/117.pdf [Accessed 10 April 2014].

Tuggey, P. (2012) *A Business Approach to Terrorism.* A Gatlin Group Limited Report [online]. Available from: http://www.catlin.com/flipbook/terrorism/files/inc/1585927987.pdf [Accessed 10 March 2014].

Turk, A.T. (2004) Sociology of Terrorism. *Annual Review of Sociology*. **30**, pp. 271-286.

Waples, S., Gill, M. and Fisher, P. (2009) Does CCTV displace crime? *Criminology and Criminal Justice.* **9**(2), pp. 207-224.

Wernick, D.A. and von Glinow, M.A. (2012) Reflection on the evolving terrorist threat to luxury hotels: A case study on Marriot International. *Thunderbird International Business Review*. **54**(5), pp. 729-746.

Widenbaum, M. (2003) The role of business in fighting terrorism. *Business Horizons* [online]. May-June, pp. 6-12. Available from: https://news.wustl.edu/Documents/weidenbaum_biz_terror.pdf [Accessed 12 March 2014].

Wood, P. (2012a) *Certificate in Security Management. Resource Book One*. The International Centre for Crowd Management and Security Studies. Uxbridge: Bucks New University [online]. Available from: https://my.bucks.ac.uk/webapps/login/?new_loc=%2Fwebapps%2Fportal%2Fframeset.jsp%3Ftab_tab_group_id%3D_1_1 [Accessed 10 January 2014].

Wood, P. (2012b*) Certificate in Security Management. Resource Book Two.* The International Centre for Crowd Management and Security Studies. Uxbridge: Bucks New University [online]. Available from: https://my.bucks.ac.uk/webapps/login/?new_loc=%2Fwebapps%2Fportal%2Fframeset.jsp%3Ftab_tab_group_id%3D_1_1 [Accessed 10 January 2014].

Wood, P. (2012c) *Certificate in Security Management. Resource Book Three.* The International Centre for Crowd Management and Security Studies. Uxbridge: Bucks New University [online]. Available from: https://my.bucks.ac.uk/webapps/login/?new_loc=%2Fwebapps%2Fportal%2Fframeset.jsp%3Ftab_tab_group_id%3D_1_1[Accessed 10 January 2014].

Wood, P. (2012d) *Certificate in Security Management. Resource Book Four.* The International Centre for Crowd Management and Security Studies. Uxbridge: Bucks New University [online]. Available from: https://my.bucks.ac.uk/webapps/login/?new_loc=%2Fwebapps%2Fportal%2Fframeset.jsp%3Ftab_tab_group_id%3D_1_1[Accessed 10 January 2014].

Wood, P. (2012e) *Certificate in Security Management. Resource Book Five.* The International Centre for Crowd Management and Security Studies. Uxbridge: Bucks New University [online]. Available from: https://my.bucks.ac.uk/webapps/login/?new_loc=%2Fwebapps%2Fportal%2Fframeset.jsp%3Ftab_tab_group_id%3D_1_1 [Accessed 10 January 2014].

Zahra, S.A., Ucbasaran, D. and Newey, L.R. (2009) Social knowledge and SMEs' innovative gains from internationali