# Operating in Hostile, Harsh and Remote Environment

Daniel Steffen Mueller (daniel.mueller@de.mcd.com)
McDonalds Germany Inc.

**Summary**

Research questions: What are the most dangerous threats organizations are exposed to when conducting in hostile environment? What are the initial impacts and the consequential effects? What are complex incidents?

Which approach to mitigate the outcome of incidents is the most effective? Is the mixture of theory and experience crucial?

Is there coherence between the crisis management industry's perception and their potential costumer's expectation?

Is the developed approach verified by the crisis management industry's references and academic research? What are the recommendations for the clients "risk or security buyer".

Methods: A multilateral approach, consisting of quantitative surveys and positivist qualitative interviews with experts offered the possibility to crosscheck the results of the questionnaire.

Results: A holistic, flexible and modular crisis management approach allows companies to anticipate risks early, and mitigate them with suitable in-house solutions.

Structure of the article: 1. Essay; 2. Literature Review; 3. Research questions & methods; 4. Detailed empirical results; 5. Conclusions 6. About the author

## 1. ESSAY

Large multinational organizations are still suffering from the shocks of the financial crisis that began in 2008. With growth slow to return to Western Europe and North America, there is an increasing drive to seek bottom line expansion in emerging markets. Müller (2006) summarizes the reason to conduct business in hostile environments: *"Across the world, companies spurred by an increasingly competitive global marketplace feel compelled to do business in dangerous countries".* For many companies, this includes business in areas where risks to people, assets or contracts may previously have fallen outside their risk appetite.

Operating in these hostile environments carries risks that are complex in nature and that can have major initial impacts and consequential effects. In this paper man-made threats and their potential impacts for organizations that are operating in hostile environments are studied in detail.

The paper considers the range of risk management options available to organizations operating in these environments, and specially the balance between measures to anticipate, prevent and respond to any man-made incidents. Moreover, it is considered if it is possible to mitigate the impacts of complex incidents with a holistic crisis management approach.

The paper draws comparison between the crisis management industry's perception of the risks and management measures available, and the perceptions of those organizations conducting business.

Finally, the paper will show that the combination of scientific methods and the support of experienced crisis management professionals can soften the impacts, consequences and duration of an incident, offering the possibility to recover more quickly.

The author interviewed enterprises and crisis management companies. The particular interest of the paper is the attitudes to, and the mitigation of, the initial impacts and consequential effects.

## 2. LITERATURE REVIEW

Man-made incidents have become a focus of public attention and science since the attack on the World Trade Center in 2001. The influence of terror has changed to the extent that it now threatens countries and alliances in its entirety – whether government institutions economy, companies or individuals. Dealing with terror has become part of everyday life and everyday business. The mass media age provides daily information about hostile environments, threats, incidents and possible solutions. An immediate comprehensive evaluation is therefore not possible in one academic paper. Thus, the review of scientific work regarding partial aspects and the evaluation of annual assessments is most useful. There is a wide range of literature about hostile environments, FDI, potential risks, risk mitigation measures and crisis management solutions, which is very diverse. The literature available is dividable into different categories: the reports and assessments edited by governmental and nongovernmental organizations with a wider view on the characteristics of hostile environments; the analyses of commercial providers involved into crisis management, like insurance companies, Private Military Security Companies, private intelligence agencies et cetera. Finally, there is a lot of literature available published by scientists. For each aspect numerous publications can be found.

Concerning fragile and dangerous states the FFP offers an interesting view on the topic, which is presented in the *"Failed State Index"* every year. This work is very useful because it offers insight on a daily open source information basis. In addition, regarding fragile or failed states and FDI the OECD published significant literature that illustrates the characteristics of the challenges and the opportunities while operating in those states. The OECD's (2012a) dossier about *"Fragile States 2013: Resource flows and trends on a shifting world"* underpins the conclusions drawn by the FFP and supplements them by adding an assessment of the economic facts. The WEF (2013), the Economist Intelligence Unit (2006), the IEP (2012) and several risk forecast (Red24, 2012, Control Risks, 2012) produced by insurance companies or crisis management service providers offer noteworthy insights about risks in hostile environments states and the perception of organizations. All these works also deal with possible effects in case of an incident. For a variety of literature on reputational damage, the *"Reputation Review 2010"* published by Oxford Metrica stands out by illustrating the impacts of failed crisis management. Frey's work (2007, 2009) gives insight in the relationship between terrorism and business and creates interesting approaches to deal with man-made incidents. He focuses on prevention and the implementation of mitigation measures that are based on the knowledge of threats and potential consequences.

Concerning risk issues and crisis management Regester and Larkin (2005) have created a standard work, which is wide-ranging but not specialised on hostile environments and man-made incidents. Jaques' work (2007; 2010) is fundamental for the developed approach described in this paper. Although his work is not focused on man-made incidents, it represents an innovative approach to research. Jaques (2010) states that crisis management has to be reshaped and should focus on the anticipation, prevention and only if necessary on the control of critical incidents.

In conclusion, it is expected that there will be both quantitative and qualitative growth in the research

and literature available in this field in the near future. The prevention of man-made incidents will undoubtedly move more into focus precipitating solutions for "normal" crisis management. In the future, it is foreseeable that the scientific research and the development of business solutions develop in an interdisciplinary way.

## 3. RESEARCH QUESTIONS & METHODS

**"***If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle".* (Tzu, 2010, p. 11)

What Sun Tzu said around 400 B.C. remains valid and summarises the potential that crisis management has to support strategic decisions making. It also neatly captures the possible consequences of sub-optimal crisis management solutions.

The end of the Cold War in the 1990's changed the global political and the economic context. Political violence between states or alliances, and the fear of nuclear annihilation was no longer determinative. The conflict landscape changed primarily to internal conflicts and with the attack against the World Trade Centre another strategic shift occurred. Political violence was no longer based purely on radical political, but also on religious ideas. Apart from the political changes, the end of the Cold War opened up new markets around the globe (Kobrin, 2005). At this time globalization brought the world closer together economically; however, mankind developed ideologically further apart (Steinberg, 2005). The Middle East, Africa, some parts of the Pacific Region and South America are strongly influenced by radical religious or political ideologies, suffering from instability and are still of great interest for European, American and Chinese companies.

Increasingly organizations are operating in emerging markets and Foreign Direct Investment (FDI) is increasing again after the financial crisis 2008 (OECD, 2013). These economic areas are characterized by not being developed but with great potential for growth. Manual labour is available at highly competitive rates, little governance is implemented and the positive effects of globalization are enabling companies to conduct business in these regions. Some of these markets are in states that are also known as Conflict Affected and Failed States.

Prior to the investment, organisations routinely conduct some form of business risk assessment and feasibility study. Based on the work of Porter (1979) business strategists still focus on possible competitors, new entrants, power of customer, substitutes and the power of suppliers, but this is not state of the art anymore and needs readjustment (Denning, 2012).

There are many threats that can manifest in these environments and their impact can be severe. Natural or industrial disaster, traffic or medical incidents, bribery, corruption, kidnap for ransom, political risk, nationalisation or confiscation, civil war, war and terrorism are able to destroy not only lives but a company's brand reputation. Enterprises are willing to take higher business risk in relation to their reputation, financial assets, and their employees, in order to create revenue while conducting business in hostile environments (Müller, 2006).

### 3.1 The nature of risk

For companies with business in hostile environments there are business risks and non-market specific risks. Kennedy (1988, p. 26) describes it as *"the risks of a strategic, financial, or personnel loss for a firm because of such nonmarket factors as macroeconomic and social policies […] or events related to political instability (terrorism, riots, coups, civil war…)".* Sandgrove (2005) argues that there are two types of business risks – the non-entrepreneurial and the entrepreneurial. The first type of risk is able to cause massive damage to company from outwards and the second type is focused on internal decisions and their impact.

In the past the understanding of risk changed. After the chaos of the Great War in the early 20th century companies protected their "touchable assets". The gathered experiences during the World War II increased that approach. Not until the marketing scientists in the 1990's focused on the ecologically, technological, political and social environment, responsible managers recognized other assets worth protecting – reputation and brand name. If

these are damaged it is even harder for companies to respond and recover (Regester, Larkin, 2005).

The nature of risks that cause greater complex consequences differs significantly from usually identified threats in risk assessment. Usually identified threats, their impacts and consequences are easily identifiable, observable or assessable for responsible risk managers.
Many of those threats are linked to environmental conditions. Some of them have only local impact others can affect the whole world. Different types of environment are the root of various threat scenarios. Harsh environment offers natural circumstances that are a challenge for human beings to live in. This includes extreme weather conditions and natural disasters. Remote environment describes conditions where infrastructure and logistical support are not immediately available. Thereby potential risks arise because help and support are not available at the point.

Also in hostile environments there are many man-made threats evident. Petty crime and violence are often identified as a potential threat. Especially travel security is an issue that is on everybody's agenda who is sending expatriates and business travellers. Complex greater man-made incidents in contrast to environmental events are difficult to retrace because they include the human psyche and do not include physical environmental regularities. From the characteristics described and excluding major natural risks four different types of identified risks arise: low spectrum risk, high spectrum risk, black swan events (e.g. 9/11) and existential risks (e.g. global killers).

Low spectrum risks are daily life risks. They are easy to identify and the preparation requires little effort. The amount of work that has to be applied to solve incidents like that are not significant and are easily manageable. The resolution requires no specialised crisis response personnel. From a victim's personal perspective these incidents seem to be devastating but for companies they are imperceptible. Low spectrum incidents' impact on business operations is almost unnoticeable. These usually identified risks have no strategic consequences. Companies on their own have the chance to greatly mitigate the probability of occurrence for low spectrum risks. Response and recovery are easily to manage.

Black swan events are, before they are happening, nearly unpredictable. They carry massive impact and consequences for companies and in the aftermath they appear much more predictable, less random and preventable (Table, 2007). Black swans change the whole business environment and have influence on an operational and strategic level. They usually develop from a regional incident to an occurrence with global impact, global consequences and have massive media coverage. Black swan incidents are identified by responsible managers but the effort to foresee them is not fundable. Therefore they are usually identified as a potential risk but the unpredictability of their manifestation is widely accepted. They differ greatly from low spectrum risk based on a low frequency, massive impact and consequences, unpredictability and the lack of opportunity in crisis mitigation measures. Response to a black swan incident and recovery from it, is possible for companies with governmental support and massive financial expenses. Companies have no chance of limiting the probability of there being an occurrence.

Bostrom (2012) defines existential risks as incidents with an outcome that *"[…] threatens the premature extinction of Earth-originating intelligent life or the permanent and drastic destruction of its potential for desirable future development".* Existential risks and their consequences are identified. The likelihood of natural existential risks; like asteroid impacts, the eruption of super-volcanoes and so on is tremendously small and scientist are able to monitor those threats. The occurrence of anthropogenic existential risks; existential threats that are generated by humans (e.g. nuclear war); are more likely but the probability is still low. They differ from low spectrum risk and black swans, in such a way that there frequency is extremely low and not the survival of business is in the centre of attention, but the survival of mankind. Although the identification is theoretically possible for firms, influencing the probability of occurrence, direct impacts and consequences is beyond their control.

High spectrum risks are identifiable if the know how exists to ensure this. Alternatively from low spectrum risks the identification of high spectrum threats and preparation of the mitigation measures requires a lot of time, expert knowledge and financial assets. Those incidents have massive impact on business and generate greater complex

consequences. The main dissimilarity resides in the fact that those consequences have the potential to be "company killers". Unlike black swans, man-made high spectrum risks can target a specific company without influencing markets or the environment.

Another difference is that companies can manage the identification, preparation, response and recovery on their own. As they are able to do it in cases of low spectrum risk. What black swans and existential risks share with high spectrum risks are the characteristics of greater complex incidents. Of the low spectrum risks they diverge in that they have massive consequences that are only manageable with specialised crisis management personnel. The amount of work that needs to be applied in order to accomplish the requirements of greater complex man-made incidents is massive. Companies supported by crisis management solutions have the possibility to mitigate the likelihood of manifestation of high spectrum risks.

Accordingly, the nature of risks that cause greater complex consequences differs from usually identified threats in risk assessment, as the amount of work, which must be applied for the identification, preparation, response and recovery of threats that are manageable for companies without governmental support is significantly higher, and the probability of occurrence can be controlled. It was defined by the author as follows:

The probability of occurrence for a potential incident (risk) is directly proportional to the chances a potential target for individuals conducting (opportunity) man-made incidents against companies presents to execute their plans successfully, their will and motivation (intent) to realise those plans. In addition to their skills and their logistical background (capability) to perform those acts. It should be noted, that the number describing the opportunities conduct an attack successful cannot be nil.

$$risk \sim intent$$
$$risk \sim capability$$
$$risk \sim opportunity$$

This coherence leads to the assumption that the risk probability is equivalent to the product of opportunity times capability times intent. Thus it follows that the lower the resulting figure, the smaller the probability of risk occurrence. Based on the assumption that there is always an opportunity the figure for risk probability cannot be zero.

$$\text{risk probability} = \text{opportunity} \cdot \text{capability} \cdot \text{intent}$$

(Towers Watson, 2012)

Capability and intent are fixed; the only influential factor for Multinational Enterprises (MNE) is the opportunity. The opportunity is directly proportional to external factors, which must be estimated, and inversely proportional to the measures of risk estimation.

$$opportunity = external \cdot \frac{1}{risk\ mitigation}$$

Risk mitigation is comprised of the identification of security gaps and threats (*identification*) as well as preparation and implementation of countermeasures, response and recovery plans (*measures*).

$$risk\ mitigation = identification + measures$$

Risk probability and opportunity outline that risk mitigation is inverse proportional to the probability of the risk itself:

$$risk \sim risk\ mitigation^{-1}$$

As a result arises that the higher the applied target-oriented crisis management resources are, the greater the ability to manage opportunity risk, impacts and consequences is.

To sum it up, risks, which consist of probability and consequences, can have operational initial impacts or long lasting, strategic consequential effects.

## 3.2 Initial impacts, consequential effects and total economic impact

Mining companies and their supportive industry, mainly logistics, have to conduct business where commodities are available – often located in hostile, harsh or remote environment. Non-profit organisations, like the UN, are involved in widespread humanitarian business; from medical aid to infrastructure renewal, and are focused on hostile environments locations. Governmental organisations emulate the nongovernmental deeds

with another purpose - political influence (Sandschneider, 2010). All of these organizations have in common that they need infrastructure to run their business. Even if infrastructure is not very well developed in hostile environments markets, companies do not refuse to conduct business there. Quite the reverse, they are interested in improving the production, transport, medical, technological, education and communication infrastructure (Salvatore, 2010). In the context of the industry those assets are more expensive to install, maintain and protect. Physical threats are ubiquitous in dangerous countries and are able to destroy lines of communication, transport routes and production facilities. As an example, the initial damage on infrastructure the Indian Hotel Company Ltd., owner of the Taj Mahal Palace, suffered during the Mumbai attacks was $37 million (Thakur, 2010).

The most fatal infrastructural loss is the annihilation of data. Wallace and Vebber (2011, p. 315) describe the importance of data and the fatal consequences of data loss.

All initial effects on infrastructure hold the ability in themselves that they can lead to business interruption and if rapid recovery is not possible to a complete shutdown (Coss, Newsome, Wong, 2012).

Initial property damage or loss can occur through man-made violent incidents. Rendeiro (2013) specifies that up to 40% of the complications for work travellers involve crime and terrorism threats and that this number is significant higher in hostile environments. People are most affected by those incidents and the effects could be long-lasting. They could be physically or mentally injured during an incident. Companies have to face the threat that expatriates or local workers are injured or killed. In 2008, a single specialised company, International SOS, had to conduct approximately 18.000 medical evacuations around the globe, according to Druckman (2009). The convalescence of physically injured personnel may take a long time but the recovery of mentally injured employees takes more time.

Far worse is the death of personnel, not only from an interpersonal perspective, but also from an economic point of view. For a certain period of time organizations lose workforce, experience and know-how. The loss of experience has prolonged serious impacts. Mazarella (2005) argues that *"A lack of expatriates filling overseas assignments may create "an isolationist orientation…",* which creates *"[…] a drag on an company's international operations and global strategic decision-making process…".* Wallace and Vebber (2011, p. 143) complement that *"[…] people all have a stake in the company's survival".* All initial effects on personnel hold the ability in themselves that they can disturb or interrupt the business processes significantly negative.

Alternative outcomes caused by potential threats include companies not being able to meet contracts anymore or the market is destroyed. The possible negative impacts, as mentioned in the previous section, have direct influence on the market share and potentially prolong the business interruption. In some cases, even the threat is enough to impact on companies. Between 1997 and 2007 Chiquita, fearing business interruption, paid $1.7 million to AUC, a Columbian terror group.

All initial impacts, which are defined by proximity and concurrency, lead to business interruption and only quick mitigation adjustment lowers it. Coss, Newsome and Wong (2012) prove that *"25 percent of businesses do not reopen following a major disaster".*

With the onset of an incident the first indirect consequences can occur. Their emergence and influence are closely linked to the initial impacts. Consequential effects, in contrast to initial impacts, are long-lasting and far-reaching (Towers Watson, 2013).

An organization's obligation to shield its personnel from risk is the "Duty of Care". Concerning human threats in hostile environments, these risks are linked to security, safety, health and travel. Regarding risk mitigation, the measures to protect property and personnel have to be designed in a way that the impairment of the public or third parties can be excluded. If a company is not capable or willing to do so and this has been proven in the aftermath, the company will face liability claims by employees and third parties (Reindeiro, 2012). As an example, after paying $25 million fine for being guilty to similar criminal charges, Chiquita had to face a mass lawsuit filed by more than 100 lawyers on behalf of family members of over 4.000 victims of the paramilitaries of AUC and FARC. Larson (2012) clarifies that lawyers who filed the suit declared that Chiquita has to be heavily punished because

they transferred large sums to terrorist organisations that is responsible for the death of thousands of people. They stated that the liabilities should be devastating. A decision of the New York Court of Appeals (2008) clarifies in the matter of World Trade Center bombing 1993 the division of responsibility and declared that companies who fail to implement suitable security measure are with 68% responsible for the damage that occurred. Besides an enormous financial loss, liabilities can have more consequences – reputational damage and damage to the brand.

Brand and reputation are not the same. They are linked to each other and it is important that managers responsible for crisis management have to take into consideration that both could be afflicted by incidents happening in hostile environments. Reference?

Ettenson and Knowles (2008) define brand as a *"[…]'customercentric' concept that focuses on what a product, service or company has promised to its customers and what that commitment means to them".* Incidents in hostile environments have the potential to damage a brand's name and following the product offered by the company is not sold anymore. For example, Blackwater, an American PMSC mainly working in Iraq and Afghanistan, offered their services and advertised that those products are based on International Humanitarian Law. After some major incidents that proved that the company was not working with regard to the 1949 Geneva Convention some of their clients cancelled the contracts (Abriska, 2007). At that point the brand name was compromised. The direct brand damage caused by poor service turned into reputational damage. Later on the company had to rename twice to get back to business (Reddy, 2011).

Barnett, Jermier and Lafferty (2006) define reputation as *"'Observers' collective judgments of a corporation based on assessments of the financial, social, and environmental impacts attributed to the corporation over time".* Ettenson and Knowles (2008) complement that reputation *"…is a "'companycentric' concept that focuses on the credibility and respect that an organization has among broad constituencies, including employees, investors, regulators, journalists and local communities – as well as customers".* Every incident threatens the reputation of a company but this threat becomes a peril when an individual or enterprise is deemed to be responsible for the negative consequence (Coombs, 2010). By implication, this means that there is no threat to the reputation, if no one accuses a company to be responsible. In the nature of the types of threats in hostile environments is the foundation for public interest. Especially in mass media attention, if incidents are not well managed and communicated with the stakeholders, this leads to huge reputational damage (Coombs, 2007). The value impact of harmful reputation events is immense. In the Chiquita case the corporate value dropped 3.7 percent after the lawsuit became public (Larson, 2012). There is the possibility that the damage causes a direct reputational damage on a company, even in the wake of an event, the reputation repair and renewal efforts reach far beyond the end of an incident. Both devour large amounts of funds as well as time (Coombs, 2010).

As defined by the author initial impacts and consequential effects have a total economic impact on a company. This impact indicates if a company is able to recover and continue business. The total economic impact consists of the total direct impacts and the total consequential effects.

The impact analysis shows that initial impacts cause financial losses. These losses are defined as total direct impacts (TDI). Every incident leads to a target specific impact (TSI). How serious the impact is depends on its physical structure, the vulnerable assets, the importance for the business continuity and the implemented risk mitigation measures. Furthermore the TSI correlates with mitigation adjustment during a crisis. The mitigation adjustment has the potential to lower a negative outcome significantly. Therefore the TSI is determinative for the possible loss of contracts or market. Target specific involves the environment, the infrastructure and human resources. Based on the intensity of the incident the TSI affects facilities and data negatively and direct remediation is necessary. The TSI's potency on infrastructure has influence on the business interruption. Similar happens in the area of HR. The TSI may include a loss of life or injury of employees. This leads to a permanent or temporary loss of work force, experience and knowhow. Companies have to mitigate the TSI with temporary or lasting replacements to shorten the length of BI. TSI on the environment requires containment even if a company is not the cause. All TSI have direct influence on the potential loss of markets/ contracts and cause massive costs. The

BI is affected by the costs of the TSI, interacts with the loss of markets/ contracts and the mitigation adjustment. The height of the TDI thus results from the addition of BI and mitigation adjustment.

Another cost factor is illustrated by the effect analysis. The target specific impacts have influence on the regulatory action, response & recovery and the consequential effects. Regulatory actions and the necessary response/ recovery measures are directly influencing the consequential effects. As mentioned above, consequential effects are damaging to brand, to reputation and the formation of liabilities. The damage to reputation and to brand requires suitable crisis communication to lower the effects on the ability to operate. Caused liabilities originate mostly in the TSI and the mitigation adjustment. Lawsuits filed by employees, the public or third party can cause massive fines. All consequential effects, regulatory actions, crisis response and recovery measures affect the ability to operate, which can change a company's value. The heights of the TCE consequently result from the accumulation of the ability to operate and the change in value.

## 4. DETAILED EMPIRICAL RESULTS

Business in emerging markets offers new opportunities for MNE's. It is in the nature of the sensitive issue crisis management that companies do not talk openly about their approach and share their information with every person and risk that information being used by their competitors. Within the crisis management industry former military personnel with a high sense for operational and information security are involved in running the business. Especially PMSC's, where the mass media tends to focus a lot of attention, are very careful about giving away information. The same is applicable for private intelligence companies, where the success of their work is based on the possession of information and unique assessments. Consequently it was unlikely to get data without contacts in the Crisis Management industry and their clients.

In order to solve the above mentioned challenges a multilateral approach, consisting of quantitative surveys and qualitative interviews with experts, has been developed. For the quantitative part two surveys were developed with different target groups. The first survey was focused on MNE's with business in hostile environments states. Out of the top 3.000 companies around the world the author supported by Towers Watson Crisis Management and the Towers Watson Marketing selected the audience for that survey. For the *"Crisis Management Consultancy Survey"* several companies were selected that signed the *"International Code of Conduct for Private Security Service Providers"* (ICoC, 2013). In order to separate the interpretation of successful risk mitigation measures of the top 20 market leading companies from small crisis management companies based on their revenue; the author analysed those results separately and interviewed experts.

The background of the author with working experience in hostile environments supported the interviews. The promise that all company specific information would remain confidential but the all over results will be shared should serve as an incentive for their participation.

The outset for the surveys was the identified lack of existing data about companies dealing with man-made incidents in hostile environments stated during the literature review. The works of the Fund for Peace (2009), the OECD (2011a), the WEF (2012) and the Economist Intelligence Unit (2006) offered basic data and raised questions concerning business and risks in hostile environments states.

The multilateral approach, consisting of quantitative surveys and positivist qualitative interviews with experts offered the possibility to crosscheck the results of the questionnaire. Nevertheless, it must be mentioned that this approach and the separation between market leading crisis management companies and small companies may raise the difficulty that there is a mismatch between the statistical results and the results of the small interview group. In addition, the interviews offered the chance to discuss questions and get more insight. Nevertheless, this split approach, even if there was the potential danger to spoil statistical data, offered the best opportunities to underpin the developed crisis management approach for companies operating in hostile environments.

After the literature review two questionnaires were developed. One question set was developed for companies with business in hostile environments. It had the purpose to demonstrate the expectations

and approaches of MNE's concerning business in hostile environments, the potential risk, the impact and consequences and their approach to mitigate these risks. The second questionnaire clarified the crisis management industry's perception about business in danger zones. The questionnaires focused on man-made risks.

There are four different topics: Questions about risk, impacts and consequences, hostile environments hotspots and future development and finally about mitigation approaches and solutions. The category of questions also varied. Questions were asked as multiple choice questions, as rating scale questions and questions that required written answers.

Firstly the surveys consist of attribute questions. These offered insight about demographic and "personal" characteristics of companies. Secondly behavioural questions were asked. These demonstrated the companies and approach. It must be noted that those questions are describing a specific action and that the perception of respondents about understanding the questions or the reality could be based on wishful thinking. Finally the surveys asked questions about personal opinions, personal conviction and attitude. It must be noted that there is no right or wrong in response to this question. Besides that, answering of surveys are binding forces that are needed elsewhere for business issues.
The sample group can be divided into different sectors. All participants are from the commercial sector. The questioned companies came out of the extractive industry, supply chain, producing industry, services industry, PMSC, private intelligence and risk management companies.

Most of the questioned organizations conducting business in hostile environments are situated in industrial nations like the USA, Japan, UK and Germany. The employees involved in crisis management are mainly located in the UK. More than 60% have up to 20.000 employees working around the world. One quarter of all asked organisations have more than 20.000 personnel and thus have the duty of care for a large number of people.

The majority of the surveyed companies offering crisis management solutions are situated in UK. The personnel working in crisis management are deployed all around the globe. The largest part of the companies are relatively small enterprises with few employees. Only 27% have more than 100 employees. This is primarily due to the fact that few staff are available and most companies are focusing on a small and specialised range of products. More than 40% of the companies surveyed asked have only little experience in hostile environments. This is offset by 44% companies with more than 20 years experience. This experience includes support for clients due to natural disaster, industrial disaster, political unrest, war, civil war, terrorist incidents, security incidents and threats. The majority of experience, more than 67%, has been gained while dealing with man-made incidents.

## 4.1 Results – organizational view and approach

FDI is still interesting for many organizations. About 40% of all respondents stated that they experienced an increase in their investment.

90% of the organizations state that they are involved in business in emerging markets, but an awareness of the dangers in emerging markets only exists for 30% of all organizations notwithstanding that most of them had to face dangers.

39% of all respondents stated that FDI became more dangerous in the last couple of years. Furthermore the majority had to conduct evacuations for various reasons and in particular due to man-made threats. It therefore must be assumed that only these organizations identify the need for suitable crisis management. At that point it is remarkable that approximately 70% of all asked organizations state that they operated 15 years or longer in hostile environments.

An in-house crisis management scheme is used by 61% of all organizations. Despite the fact that the asked personnel are involved in crisis management, 31% do not know if there is an in-house crisis management team. A notable fact is that 53% of the organizations have only a few people available to conduct crisis management. Even worse is that 8% do not have personnel who are involved in crisis management and 39% do not know if there is more staff involved in the crisis

management plan. This proves that crisis management is not a primary focus of organizations and awareness for the need for a detailed crisis management plan does not exist. A working crisis management is not possible with so few people - the large amount of work, the complexity of suitable planning processes and the requirements of fitting response measures are not achievable.

Nearly 40% ignore the necessity of crisis management solutions and do not have relationships with external vendors. The majority of organizations are aware that there is a need for crisis management solutions and solve this problem by hiring external crisis management companies. Of these 40% 38% have no idea, if there are external solutions and about 30% do not know who has the lead during a crisis. In most of the organizations crisis management is performed as a secondary task. This is evidence of the ignorance of the company's internal crisis management solutions if they exist; a lack of liaison, information flow and crisis preparedness. Hereby the majority of companies cede the control of crisis management to external vendors and therefore have no guarantee that managing their crisis management is top priority.

Risk assessment is perceived as important by most of the organizations. A risk assessment is done by 70% for all business travel and expatriate deployments, of whom 39% use the help of external vendors. 7% are only conducting risk assessments, if they are involved in business in higher risk locations. It is noteworthy that ¼ of the organizations have no knowledge about risk assessment.

Even though the majority of responders have no suitable risk analysis system, they only trust a little international and governmental organization with great experience in foreign engagement. Furthermore it is remarkable that about 30% assess crisis management providers, security companies and specific intelligence as not really trustworthy. This is even more surprising because a large part does not have own risk analysis options available. The remaining organizations place their trust in the abilities of those companies. Questionably enough, 62% of the responders have confidence in relation to information about hostile environments in an information network with competitors. This leads to the conjecture that anticipation is not done properly by ¼ of all organizations and the crisis management teams are not suitable.

Although the view on the level of peril in emerging markets is contrary to popular belief, the threats felt most dangerous are indeed perceived as hostile. Man-made threats are of special concern for organizations. As the greatest threat the respondents perceive terrorism, followed by kidnapping, bribery and corruption. This view is based on the organizations ranking of their greatest distresses. Physical integrity of employees is for all organizations a question of importance, but organizations identify mass media attention and damage to brand and reputation as the most devastating perils.

Most of the responders believe that they are capable of managing any of the risks in hostile environments and are able to protect facilities, people, data, brand, reputation and the environment. Despite the fact that approximately 40% have no autarkic crisis management system implemented, no personnel available and depend on external advisors, the surveyed believed that the protection is relatively easy. These statements do not correlate with the data about the most dangerous and concerning issues concerning exposures. Nevertheless, the data also confirms that people, brand and reputation are perceived as the most vulnerable corporate goods.

In order to mitigate the risks companies use different types of training, information and methods. Employees are trained with country specific information by 62% of all organizations asked. Online trainings are only used by a minority. Pre-travel safety training is offered by 39%. Special hostile environments awareness training is only implemented in about ¼ of all organizations, in which this corresponds to 75% of all companies that perceive the regions in which they invest in emerging markets as hostile environments. 30% conduct information security training, which shows that data protection is important for these companies. Only 15% use the chance to offer training in hostile environments after the arrival of expatriates or work-travellers. The non-utilization of the resources and methods presented above contradicts the assumption of many responders that the protection of personnel, brand name, reputation and assets are no great challenge. Furthermore, it controverts the information that people are at the centre of

concerns and offers insight that corporate social responsibility is not really in the focus.

Furthermore, the analysis of the data shows that there are also lacks in the organizations' crisis management approach. Most of the companies conduct in-house monitoring, what could be rated as good, if not testified the previous information that resourcefulness is not given. Additionally, third party risk information subscription is a mitigation method most organizations take advantage of. Again, the question arises, what the benefit is, when 40% of the respondents indicated that there is a lack of trust with external consultants.

In terms of duty of care, 50% of all respondents contradict their statements. They indicated that the welfare of employees is the biggest concern. However, only half of them use close protection teams or armed guards, a crisis management measure that mitigates the risk by deterrence. Besides, vetting measures for employees are only implemented and expatriates are merely selected properly by 22% of asked organisations. The same applies for the protection of data and IT. Only 28% use enhanced IT and information security measures, which contradicts the stated importance of data. In addition to the relatively careless handling of personal and data, 61% of all organizations express confidence to deal with incidents without implemented crisis management plans or pre-prepared crisis communication plans. To sum it up, only 30% of all respondents experience a high return on mitigation investment. For most of the organizations the need and benefits of mitigation measures are not clear.

Asked about the hindrance of several factors on their organizations' ability to implement flexible crisis management and crisis response 62% stated that money is a major problem, followed by 54% who were concerned about reputational issues and 39% with compliance issues. The availability of experts, experience and knowledge was assessed as little hindrance, which is noteworthy.

A further remarkable aspect is the confidence of organizations in their own crisis management abilities. More than 50% assessed have confidence in their risk assessment, their risk mitigation measures, their crisis management and their crisis communication. This circumstance must be assessed as very threatening for the crisis survivability of those organizations, because the correct assessment of own abilities is the basis for all crisis management steps.

In summary it can be said that the organizational view on crisis management and the crisis management approach of most of the questioned organizations is not sufficient. It lacks a necessary crisis management mind-set, appropriate self-assessment of own skills, resourcefulness, personnel, knowledge, experience, networks and a holistic crisis management approach.

## 4.2. Results - The crisis management industry's view

The services offered include security risk analysis, physical security, maritime security, security consulting, training for people deploying in hostile environments, travel security training, 24/7 operations room, evacuation and repatriation, kidnap for ransom response and crisis management preparation. The majority of activity is focused on selling physical protection based on their own risk and vulnerability assessment. At this point it is remarkable that only 28% offer training for expatriates and 39% a 24/7 operations room. Nevertheless, the product range shows that across the market-leading companies diversity is needed in order to face multiple challenges in hostile environments.

As against the clients, 44% of the crisis management vendors assess anticipation as the most important step to handle a crisis, followed by prevention with the 2nd priority. Response is only for 17% the most important part of crisis management, in which recovery is excluded due to the fact that it is business continuity task. In total, prevention is of significant importance, primarily because it offers the best possibilities for revenue.

Contrary to their potential customers, crisis management consultants understand the countries where they conduct business in hostile environments. "Hostile environments" are, in this industry, an established concept. This mind-set is considered a precursor for suitable crisis management solutions.

The risks identified as threats for clients differ slightly from the perception of the customers. Terrorism is for 66% a serious threat on a par with violent crime, followed by regime change, vehicle accidents, bribery and corruption, kidnapping for

ransom and espionage. Disasters are also a threat but not in the focus of crisis management providers.

All of the crisis management industry's clients fear damage to brand and reputation. This is remarkable due to the fact that few customers have crisis management and crisis communication plans implemented. The next important worry is the health of people stated by 95% of all respondents. Media attention is also perceived as an imminent threat, followed by arising liabilities caused by not existing crisis management solutions.

The protection of all assets and personal is in some categories judged as very difficult. In total the protection of people is assessed as the most challenging. This is due to the fact that the protection is not guaranteed by introducing technical system, physical protection or processes but must be supplemented by intra- and interpersonal training, awareness training and the setup of a suitable mind-set.

### 4.3 Coherence between crisis management providers and clients

There is nearly no coherence between the perceptions of the crisis management industry and potential clients operating in hostile environments. This begins with the understanding of hostile environments risk exposure. Crisis Management companies assess dangerous countries as hostile environments and do everything in order to identify and mitigate the risks. Clients have a different understanding. Emerging markets are perceived as a new economic opportunity and the dangers are often underestimated. Consequently, within the security buyer community the mind-set, which is fundamental for holistic and flexible crisis management, is as robust or effective as it should be. 74% of the crisis management industry assesses the evolution of risks in hostile environments as steadily rising but only 39% of the potential customers are of the same opinion. Conversely, with the assessment of the return on investment, clients identify a stronger growth opportunity. The risks recognized as threats for customers diverge to some extent from the opinion of the clienteles.

Terrorism is for 66% a severe threat followed by violent crime, trailed by regime change, vehicle accidents, bribery and corruption, kidnapping for ransom and espionage. The protection of all assets and personnel is in some categories judged as very difficult. In total the protection of people is assessed as the most challenging.

To sum it up, it can be said that clients and the crisis management industry have recognized the need for a suitable crisis management solution.

## 5. CONCLUSIONS

Crisis management must not only consist of reaction possibilities on possible risks but should adequately provide a complete solution. There will never be a single manual that provides action plans for every single crisis (Regester, Larkin, 2005, p. 199). A holistic, flexible and modular crisis management approach allows companies to anticipate risks early, and mitigate them with suitable in-house solutions. Due to the fact that this approach is not, in the short term, the lowest-priced, organizations should focus on the implementation of affordable modular elements. The most important thing is that organizations recognize the need for crisis management. This includes solutions for a suitable crisis management team and the definition of standard operating procedures during the crisis management cycle. All desired solution and requirements are at best in-house solutions if this is financially possible for companies. Organizations should recognize the benefits of the concept allowing them to lay the foundations and work their way from the low cost large benefit to the more expensive marginal enhancements. Some steps must necessarily be realized through external networking.

As in reality, however most organizations do not have the possibilities to finance all best practice solutions, alternative resolutions are also considered. All recommendations depend on the ALARP (As low as reasonably practicable) principle. This creates interpersonal relationships; networks consisting of people involved in crisis management and ensure that the companies' view of crisis management is shared. The overall goal should always be that the approach is implemented in its entirety

Even if greater complex incidents are in the area of responsibility of the crisis management team, here, a rounded approach is described that considers all responsible levels, their structure and tasks as well

as other necessities. The requirements, recommended behaviours and objectives to be achieved are divided into the phases: basics, anticipation, preparation and response.

Fundamental to the approach is a change in the understanding of crisis management. Crisis management is no longer defined as event approach, where everything is focused on incident response. The event approach is limited to purely tactical or operational activities (Jaques, 2010, p. 10). The event approach understands every single crisis as an event, which starts with a trigger incident, followed by response and solved during recovery. This approach is not proactive but purely reactive, which leads to inflexible and phlegmatic crisis management. The below mentioned solution is based on contemporary scientific developments, where crisis management is understood as a perpetual process on a strategic level. Pauchant and Mitroff (1992, p. 11) provide a suitable demarcation to the event approach when they state, that *"crisis management is not the same as crash management […] Obviously this is important, but it is only one part of total crisis management effort. Here we focus not only on crash management – what to do in the heat of a crisis – but also on why crises happen in the first place and what can be done to prevent them".*

The absolute focus is on anticipation and prevention of crisis, so that the response is like a "reflex". No surprises, plan for the best, prepare for the worst– this is the guideline of suitable crisis management.

## 6. ABOUT THE AUTHOR

Daniel Mueller studied history at the University of the Bundeswehr, Hamburg and International Business Management and Leadership at the Professional School of Business and Technology, Kempten. During this time, he served as an Human Intelligence officer and interrogator within the German Special Operation Forces. Afterwards Daniel Mueller worked in Great Britain and Germany as a Crisis Management Consultant, and supported companies across all industries to anticipate and prepare for risks to which they are exposed – including physical risks, terrorism, travel security, kidnap for ransom, extortion, reputational damage and political risk. Currently, he is working for McDonald's Deutschland Inc. as Senior Manager Security.

## 7. REFERENCES

Abriska, J. (2007). *Blackwater; mercenaries and international law.* Retrieved 06-19-2013 from http://fride.org/publication/254/blackwater:-mercenaries-and-international-law

Barnett, M.L., Jermier, J.M., Lafferty, B.A. (2006). Corporate reputation: The definitional landscape. *Corporate Reputation Review*. 26-38.

Bostrom, N. (2012). *Existential risk prevention as global priority.* Retrieved 06-19-2013 from http://www.existential-risk.org/concept.pdf

Coombs, W.T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10, (2). 163-176.

Coombs, W.T. (2010). *Parameters for crisis communication.* Retrieved 06-19-2013 from http://media.johnwiley.com.au/product_data/excerpt/13/14051944/1405194413.pdf

Coss, A.L., Newsome, C.W., Wong, J. (2012) *Accounting for the critical variable in emergency response - people.* Retrieved 06-19-2013 from http://www.securitymagazine.com/articles/83115-accounting-for-the-critical-variable-in-emergency-response---people

Denning, S. (2012). *What killed Michael Porter's Monitor Group? The one force that really matters.* Retrieved 06-19-2013 from http://www.forbes.com/sites/stevedenning/2012/11/20/what-killed-michael-porters-monitor-group-the-one-force-that-really-matters/

Druckman, M. (2009). Keeping your globally mobile employees healthy, safe and secure. *Global Business and Organizational Excellence*. 29, (1). 41-49.

Economist Intelligence Unit (2006). *Operating risk in emerging markets.* Retrieved 06-19-2013 from http://graphics.eiu.com/files/ad_pdfs/eiu_Operating_Risk_wp.pdf

Ettenson, R., Knowles, J. (2008). *Don't confuse reputation with brand.* Retrieved 06-19-2013 from http://sloanreview.mit.edu/article/dont-confuse-reputation-with-brand/

Frey, B. S. (2007). Terrorism and business. *Economics Working Paper*, 329. 1-21.

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

Fund for Peace (FFP) (2009). *The Fund for Peace country analysis indicators and their measures.* Retrieved 06-19-2013 from http://www.fundforpeace.org/global/library/cr-10-97-ca-conflictassessmentindicators-1105c.pdf

Fund for Peace (FFP) (2013). *The Failed State Index 2012.* Retrieved 06-19-2013 from http://ffp.statesindex.org/rankings-2012-sortable

IEP (2012). *Global Terrorism Index 2012.* Retrieved 06-19-2013 from http://reliefweb.int/sites/reliefweb.int/files/resources/2012-Global-Terrorism-Index-Report.pdf

Jaques, T. (2010). Reshaping crisis management: the challenge for organizational design. *Organizational Development Journal*, 28, (1). 9-17.

Jaques, T. (2007). Issue management and crisis management: An Integrated, non-linear, relational construct. *Public Relations Review*, 33, (2). 147-157.

Kennedy, C. (1988). Political risk management: A risk portfolio planning model. *Business Horizons*, 31, (6). 26-33.

Mazarella, J.J. (2005). *Terrorism and Multinational Corporations: International business deals with the costs of Geopolitical Conflict.* Retrieved 06-19-2013 from http://business.uni.edu/economics/Themes/mazzarella.pdf

Kobrin, S. J. (2005). The determinants of liberalization of FDI policy in developing countries: a cross-sectional analysis, 1992-2001. *Transnational Corporations*, 14, (1). 68-104.

Larson, E. (2010). *Chiquita settles investor suits over terror payments.* Retrieved 06-19-2013 from http://www.bloomberg.com/apps/news?pid=newsarchive&sid=ayT65YLVeJBs

New York Court of Appeals (2008). *No.217. In the matter of World Trade Center bombing.* Retrieved 06-19-2013 from http://www.courts.state.ny.us/CTAPPS/Decisions/2011/Sep11/217opn11.pdf

OECD (Ed.) (2013). *FDI in figures.* Retrieved 06-19-2013 from http://www.oecd.org/daf/inv/FDI%20in%20figures.pdf

OECD (Ed.) (2012a). *Fragile states 2013. Resource flows and trends in a shifting world.* Retrieved 06-19-2013 from http://www.oecd.org/dac/incaf/FragileStates2013.pdf

OECD (Ed.) (2011a). *Conflict and fragility. Managing risks in fragile and transnational contexts. The price of success?* Retrieved 06-19-2013 from http://www.oecd.org/development/incaf/48634348.pdf

Porter, M. E. (1979). *How competitive forces shape strategy.* Retrieved 06-19-2013 from http://prolog.univie.ac.at/teaching/LVAs/KFK-LM/WS07/Porter.pdf

Reddy, L. (2011). *Blackwater renames itself and wants to go back to Iraq.* Retrieved 06-19-2013 http://abcnews.go.com/Blotter/blackwater-renames/story?id=15140210

Red24 (Ed.) (2012). *Threat forecast 2013.* London: Red24.

Regester, M., Larkin, J. (2005). *Risk issues and crisis management: a casebook of best practice*. London: Kogan Page Limited.

Rendeiro, J.G. (2013). *Threat analysis and ratings for overseas security.* Retrieved 06-19-2013 from http://www.securitymagazine.com/articles/83892-threat-analysis-and-ratings-for-overseas-security

Salvatore, D. (2010). Globalisation, international competitiveness and growth: Advanced and emerging markets, large and small countries. *Journal of International Commerce*, Economics and Policy, 1, (1). 21-32.

Sandgrove, K. (2005). *The complete guide to business risk management.* Burlington: Gower Publishing Company.

Sandschneider, E. (2010). *Doing business in disputed regions. A proposal for a new focus on private sector support for state building.* Retrieved 06-19-2013 from https://dgap.org/de/article/getFullPDF/17757

Steinberg, G. (2005). *Das Netzwerk des islamistischen Terrorismus: Der Nahe und der Ferne Feind.* München: C.H. Beck.

Thakur, P. (2010). *Taj Opens Palace wing 2 years after Mumbai attacks.* Retrieved 06-19-2013 from http://www.bloomberg.com/news/2010-08-12/taj-mahal-reopens-century-old-palace-suites-two-years-after-mumbai-attack.html

Towers Watson (Ed.) (2012a). *Crisis Management – Consulting Standard Operating Procedures (SOPs).* London: Towers Watson.

Towers Watson (Ed.) (2012b). *Crisis Management Overview.* Retrieved 06-19-2013 from http://www.towerswatson.com/assets/pdf/8455/TW-2012-28915_Crisis_management_overview.pdf

Towers Watson (Ed.) 2013). *Crisis Management Overview and Sunstone™.* London: Towers Watson.

Tzu, S. (2010). *The art of war.* Campbell: FastPencil.

Wallace, M., Vebber, L. (2011). *The disaster recovery handbook. A step-by step plan to ensure business continuity and protect vital operations, facilities and assets.* New York: AMACOM.

WEF (Ed.) (2012). *Global Risks Report 2013.* Retrieved 06-19-2013 from http://reports.weforum.org/global-risks-2013/