Project Dissertation

Psychological Contract in Hostile Workplace Environment

Submitted By:

Shivam Arora

2K14/MBA/69

Under the Guidance of:

Ms. Meha Joshi

Assistant Professor

DELHI SCHOOL OF MANAGEMENT
Delhi Technological University
Bawana Road Delhi 110042

Jan – May 2016

Certificate from the Institute

This is to certify that the Project Report titled **Psychological Contract in Hostile Workplace Environment** is a bonafide work carried out by Mr. Shivam Arora of MBA 2014-16 and submitted to Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42, in partial fulfilment of the requirement for the award of the Degree of Masters of Business Administration.

Signature of Guide

Signature of Head (DSM)

Place:

Seal of Head

Date:

Declaration

I, Shivam Arora, student of MBA 2014-16 of Delhi School of Management, Dehi Technological University, Bawana Road, Delhi-42, declare that Project Dissertation Report on **Psychological Contract in Hostile Workplace Environment** submitted in partial fulfillment of Degree of Masters of Business Administration is the original work conducted by me.

The information and data given in the report is authentic to the best of my knowledge.

This Report is not being submitted to any other University for award of any other Degree, Diploma and Fellowship.

Shivam Arora

Place:

Date:

Acknowledgement

This is matter of great joy to extend my gratitude to those people who helped me in completion of my dissertation project.

I am highly obliged to Ms. Meha Joshi (Delhi School of Management) for guiding me throughout the process of analyzing and preparing this final work on my dissertation.

My special thanks to Prof P.K. Suri (Head of Department, Delhi School of Management), for creating conducive environment in the institute, which boosted my morale and proved to be my driving force for not only performing well in academics but also for the completion of my project.

Shivam Arora

Executive Summary

Today almost every part of the world is living under a dreadful threat of terrorism. The way terrorists have come out in open to attack general masses in Paris, Mumbai and so many other places, and have been successful in creating the bloodshed, has developed an inevitable fear amongst the people.

But sitting back at home and waiting for a day when the globe would be free of any such ill happenings would be no less than sheer day dreaming. So anyhow one needs to step out in order to earn his/her bread and butter.

Any sort of intrusion in various employment zones (such as SEZs or technology parks) of metropolitan cities, where countless people exist, move and operate for their living, would mean tremendous risk to thousands of innocent lives.

Therefore one thing is for sure that all these hostilities and disturbances in our external environment have led to the emergence of certain workplace security related expectations from both employees' and employer's side.

Few factors which are critical to maintain workplace security have been identified and respondents have been asked to rank those factors.

Table of Contents

Title Page	Page i
Certificate from Institute	Page ii
Declaration	Page iii
Acknowledgement	Page iv
Executive Summary	Page v
Table of Contents	Page vi-vii
List of Figures	Page viii
1. Introduction	Page 1-16
1.1 Introduction of the Project	Page 1-15
1.2 Objective of the Study	Page 16
1.3 Scope of the Study	Page 16
2. Literature Review	Page 17-25
3. Research Methodology	Page 26-27
3.1 Data Sources	Page 26
3.2 Research Model	Page 26
3.3 Work flow of the Study	Page 27
3.4 Sampling	Page 27
3.4.1 Sample size	Page 27
3.4.2 Sample Method	Page 27
4. Data Analysis	Page 28-31
4.1 Tools used for analysis	Page 28
4.1.1 Instrument	Page 28

4.1.2 Method Page 28

4.2 Conclusions and Findings Page 28-30

4.3 Limitations and Future Scope of the Study Page 31

5. References Page 32-33

6. Adherence Sheet Page 34

7. Annexure Page 35-42

7.1 Questionnaire Page 35-42

List of Figures

Figure 1: The Hostility Behavioral Spectrum Page 3

Figure 2: Ranking of 162 Countries based on Global Terrorism Index Page 4

Figure 3: Countries with highest number of deaths by terrorism, percentage of Global Deaths for 2013 Page 4

Figure 4: Terrorist incidents in India Page 5

Figure 5: Targets of Terrorism 2000-2013 Page 5

Figure 6: Risk Management Cycle Page 7

Figure 7: Research Model Page 26

Figure 8: Work flow of the Study Page 27

1 Introduction

1.1 Introduction of the Project

Psychological contract refers to the expectations which employee and employer have from each other and what they owe to each other. As work changes, so does the nature of the relationships between employees and employers. In the new work context, the informal, "psychological contract" between workers and employers - what each expects of the other - focuses on competency development, continuous training, and work/life balance. In contrast, the old psychological contract was all about job security and steady advancement within the firm. As already discussed, few workers expect, or desire, lifelong employment in a single firm. As job security declines, many management scientists see clouds on the horizon, including:

- Corporate indifference - Shoshana Zuboff and James Maxmin, in The Support Economy, describe a new individualism among U.S. workers. These new individuals are invested in "psychological self-determination." They desire participation, expression, identity, and quality of life—all values which are espoused by organizations, but largely ignored in practice as organizations continue to focus on reducing fixed labor costs.
- Reduced loyalty and commitment - With little expectation for advancement, workers feel less committed to organizational goals and more committed to their own learning and development. The knowledge and technological skills that employees bring with them to the workplace are transportable and are not lost when a new job is taken.
- Increased time burdens - Years of downsizing and outsourcing have produced what Lesie Perlow calls a "time famine"- the feeling of having too much to do and too little time to do it. In order to keep up with workloads, many workers are spending longer hours at work, according to reports by the Bureau of Labor Statistics and the Center for Workforce Development.
- Flexible work arrangements do not keep up with employee preferences - The Work Trends 2000 report found that 74% of workers were not allowed flexible hours and work arrangements (such as telecommuting). Those with flex hours have limited freedom regarding when and where to work. The vast majority of

workers have to commit to a specific day to work at home or a specific day to take off if they work four10-hour days.

The term, "hostile work environment," is not a psychiatric or psychological construct, but a legal term that derives from Title VII Civil Rights United States laws prohibiting discrimination in the form of discrimination of all types, including sexual and other harassment. The law does not attempt to define what specific behaviours are to be labelled hostile, but, rather, allows the trier-of-fact to make such determinations after the fact, based upon the particulars of the individual case. While the law attempts to define the legal dimensions of harassment and a hostile work environment, psychiatry explores the behavioural and psychological dimensions that the law does not address. It has been difficult for medical researchers and behavioural scientists to study this concept using traditional scientific methods, because there are no objective and universally accepted behaviours that define hostile work environment. What is considered hostile in one workplace may not be considered hostile in another, because of cultural differences, the nature of the job, etc. Absent precise behavioural definitions, the current universe of knowledge about this phenomenon remains empirical, with the behaviours embraced by the term, hostile work environment involving individual perception and contextual factors broadly encompassed under the heading of inappropriate aggression and hostility. Because of the individual variations among the different workplaces and types of workers, and management need to understand certain fundamental concepts about human aggression, in general, and hostility, in particular. These concepts will assist them in assessing and responding appropriately to non-violent hostile work situations such as harassment and bullying. Hostile human behaviour exists along a spectrum (see figure 1). As can be seen in figure 1, on the one end of this spectrum are violent behaviours, such as homicide, terrorism, and rape. On the other end are more ambiguous and less severe forms of hostility, including verbal and sexual harassment, shunning, intimidation, physical bullying, and threats. Between these extremes are problems such as stalking and non-homicide related domestic violence.

The term "terrorism" means premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents, usually intended to influence an audience.

The term "international terrorism" means terrorism involving citizens or the territory of more than one country.

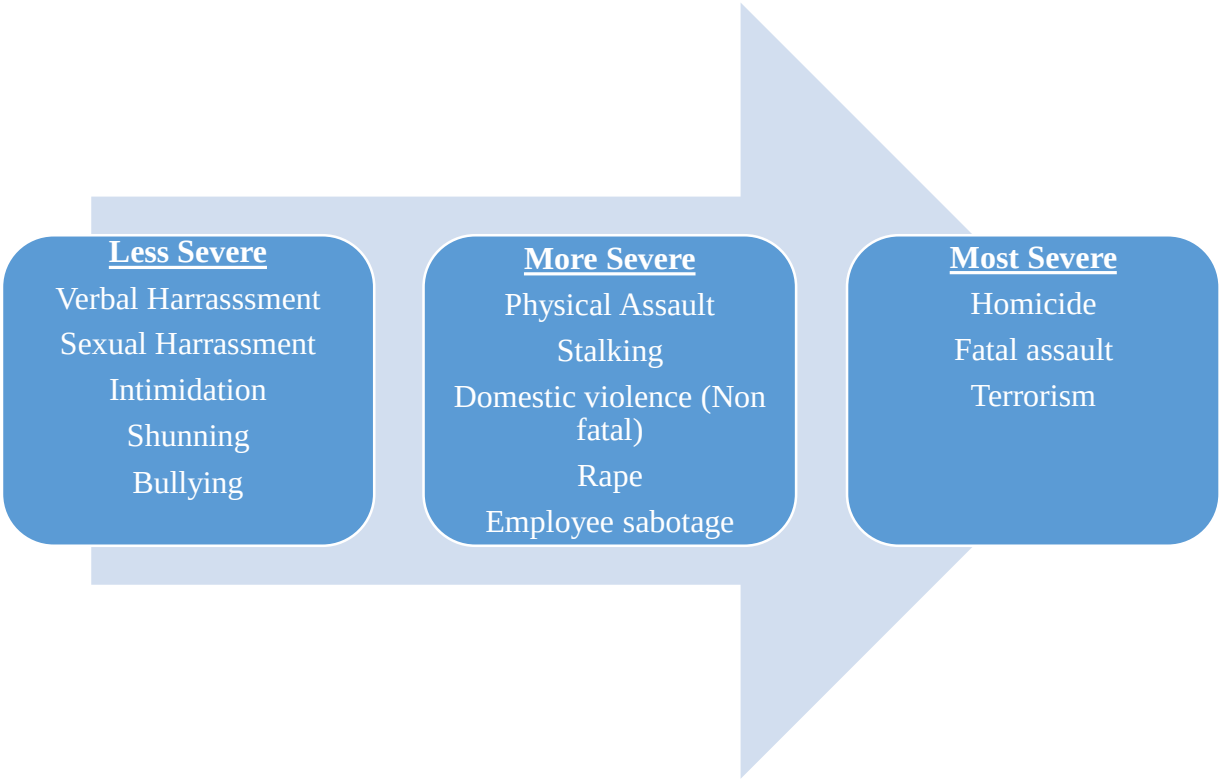

Figure 1: The Hostility Behavioural Spectrum

Source: Psychological aspects of the hostile workplace: Harassment and Bullying Barbara Long, M.D., Ph.D. (In Wilkinson, Carol and Peek-Asa, Corinne. Clin Occup Environ Med 3(2003) 803-820)

Terrorism is important aspect of risk exposure that is relevant to international HRM, particularly in the current political climate since the tragic events in New York on September 11, 2001. Most major multinationals must now consider political risk and terrorism when planning international meetings and assignments and it is estimated that they spend 1-2 per cent of their revenues on protection against terrorism. Terrorism has also clearly had an effect on the way in which employees assess potential international assignment locations. The HR department may also need to devise emergency evacuation procedures for highly volatile assignment locations.

Thus one thing can be said with no doubt that all these hostilities and disturbances in our external environment have led to the emergence of certain workplace security related expectations from both employees' and employer's side.

RANK	COUNTRY	SCORE
1	Iraq	10
2	Afghanistan	9.39
3	Pakistan	9.37
4	Nigeria	8.58
5	Syria	8.12
6	India	7.86
7	Somalia	7.41
8	Yemen	7.31
9	Philippines	7.29
10	Thailand	7.19
11	Russia	6.76
12	Kenya	6.58
13	Egypt	6.5
14	Lebanon	6.4
15	Libya	6.25
16	Colombia	6.24
17	Turkey	5.98
18	Democratic Republic of the Congo	5.9
19	Sudan	5.77
20	South Sudan	5.6
21	Algeria	5.52

Figure 2: Ranking of 162 Countries based on Global Terrorism Index

Source: Global Terrorism Index 2014 (Institute of Economics and Peace)

Figure 3: Countries with highest number of deaths by terrorism, percentage of Global Deaths for 2013

Source: Global Terrorism Index 2014 (Institute of Economics and Peace)

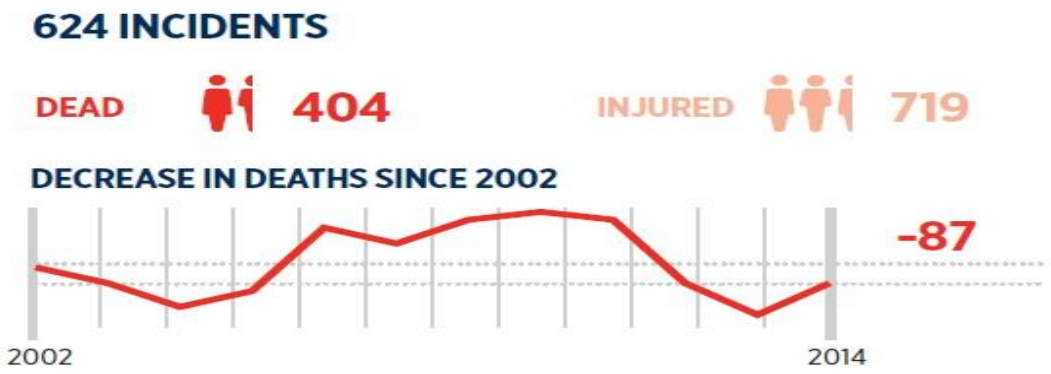

Figure 4: Terrorist incidents in India

Source: Global Terrorism Index 2014 (Institute of Economics and Peace)

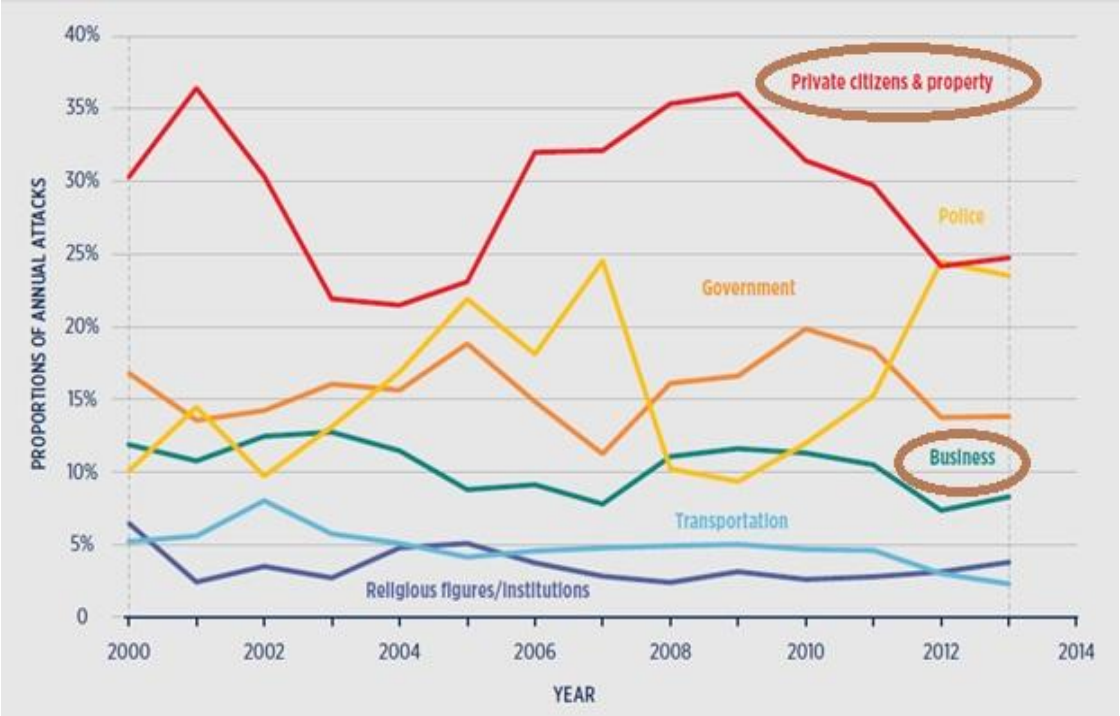

Figure 5: Targets of Terrorism 2000-2013

Source: Global Terrorism Index 2014 (Institute of Economics and Peace)

The importance of security planning

Terrorism is not just about physical attack. It might take the form of attacks on vital information or communication systems, causing disruption and economic damage. Some attacks are easier to carry out if the terrorist is assisted either directly or indirectly by an 'insider', or by someone with specialist knowledge or access. Terrorism also includes threats or hoaxes designed to frighten and intimidate.

There are three strong business reasons why an organisation should plan to deter such acts, or at least to minimise their impact. They are:

I. **Legal obligations**

In the event of an incident, plans are likely to come under scrutiny. Health and safety at work regulations put the responsibility on the owner or occupier of the premises to provide a duty of care for staff and visitors. Although the police and other agencies can offer advice, it is up to the owner or occupier to seek out and act upon that advice. In any subsequent inquiries or court proceedings, organization would need to show that it took the relevant legislation into account.

II. **Business continuity**

Ensure that the business is able to cope with an incident or attack and return to normality as soon as possible. This is particularly important for smaller businesses that may not have the resources to withstand even a few days without trading.

III. **Loss of reputation.**

In addition, organisation must make sure that it has adequate insurance to cover terrorist threats after consultation with insurance company or broker. There is limited value in safeguarding the business premises in isolation. Neighbours' plans and those of the emergency services should also be taken into account, particularly if office is in a multi-occupancy building.

Managing Risks

If one thinks that the organisation might be affected by a terrorist attack, appropriate protective security measures should be applied. Some institutions may be more at risk

than others, especially if they have a higher public profile, but other factors can also play a part, such as the location of the business.

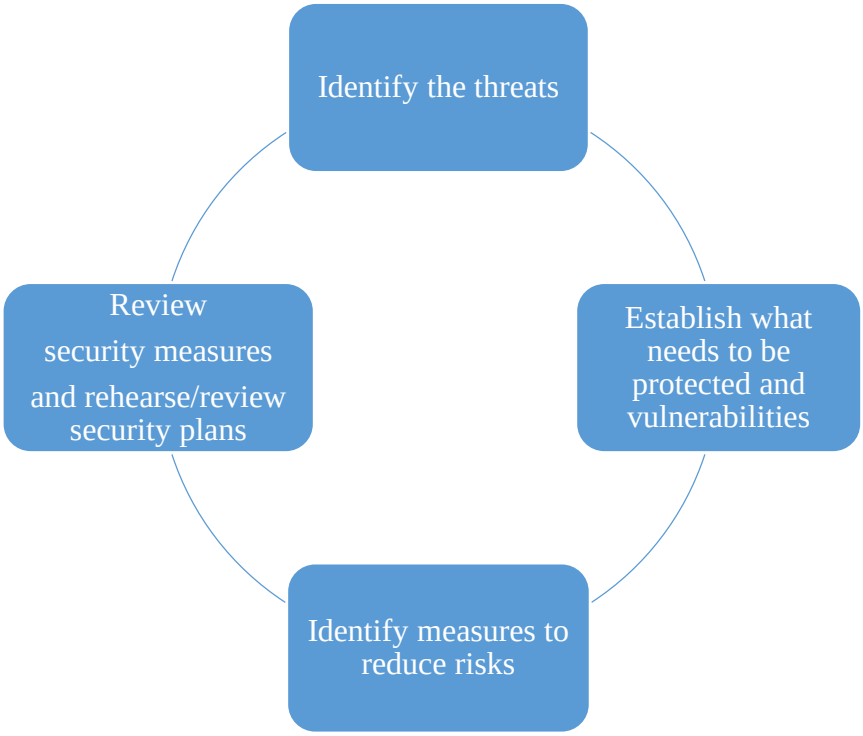

Figure 6: Risk Management Cycle

Step-1: Identify the threats

Following questions should be asked:

• What can be learnt from the Government and media about the current security climate and recent terrorist activities?

• Is there anything about the organisation, building or staff that might attract terrorist attack?

• Is there an association with high-profile individuals or organisations which might be terrorist targets?

• Could collateral damage occur from an attack on a high-risk neighbour?

• Is there anything terrorists might want to further their aims, e.g. materials, plans, technical expertise or access to other premises that might be targets?

Step-2: Establish what needs to be protected and vulnerabilities

Priorities for protection should fall under the following categories:

• People (staff, visitors, contractors, customers)

• Physical assets (buildings, contents, equipment, plans and sensitive materials)

• Information (electronic and paper data)

• Processes (supply chains, critical procedures).

Organization knows what is important to it and its business. It probably already has plans in place for dealing with fire and crime, procedures for assessing the integrity of those it employ, protection from IT viruses and hackers, and measures to secure parts of the premises. Review the plans on a regular basis and if organization thinks it is at greater risk of attack – perhaps because of the nature of its business or the location of the premises – then consider what others could find out about its vulnerabilities, such as:

• Information about organization that is publicly available, e.g. on the internet or in public documents.

• Anything that identifies installations or services vital to the continuation of the business.

• Any prestige targets that may be attractive to terrorists, regardless of whether their loss would result in business collapse.

As with Step 1, it is also to be considered whether there is an aspect of business or activities that terrorists might want to exploit to aid their work. If there are, how stringent are checks on the people company recruit? Is the staff security conscious?

Step-3: Identify the measures to reduce risk

An integrated approach to security is essential. This involves thinking physical security, information security and personnel security (i.e. good recruitment and employment practices). There is little point investing in costly physical security measures if they can be easily undermined by a disaffected member of staff or by a lax recruitment process. Many of the security precautions typically used to deter criminals are also effective against terrorists. So before investing in additional security measures, it should be review what organization already have in place. If there is need to introduce additional security measures, those should be made more cost-effective by careful planning wherever possible. Introduce new equipment or procedures in

conjunction with building work. In multi-occupancy buildings, shopping centres, high streets or business parks, try to agree communal security arrangements. Even if neighbours are not concerned about terrorist attacks, they will be concerned about general crime – and organization's security measures will help protect against crime as well as terrorism.

Step-4: Review security measures and rehearse/review security plans

Regular reviews and rehearsals of security plans should be conducted. This will help to ensure that they remain workable and up to date. One should be aware of the need to modify them to take account of any changes in your business. For instance, new building work, changes to personnel or revised health and safety procedures could have an impact on business plans. It should be ensured that staff understand and accept the need for security measures. Security should be seen as a common responsibility and not just something for security professionals. Make it easy for staff to raise concerns or report observations.

Physical Security

Having conducted the risk assessment, it is needed to decide which physical security measures to adopt. In most cases they will range from basic good housekeeping (keeping communal areas clean and tidy) through CCTV, intruder alarms, lighting and computer security, to specialist solutions such as mail scanning equipment. Specialist solutions, in particular, should be based on a thorough assessment – not least because one might otherwise invest in equipment that is ineffective, unnecessary and expensive.

Contact the Counter Terrorism Security Adviser through the local police force at the start of the process. As well as advising on physical security, they can direct one to professional bodies that regulate and oversee reputable suppliers. A reputable supplier can make a professional assessment of requirements and recommend suitable products. Through the professional bodies, one can compare different providers. Before buying any security product, one should make clear clear about what it is designed to achieve and what guarantees and after-sales service can be expected.

Protective Security Measures that can be considered:

I. Basic housekeeping

Basic good housekeeping reduces the opportunity for planting suspect packages and helps deal with false alarms and hoaxes. One can reduce the number of places where devices may be left by:

• Keeping public and communal areas – exits, entrances, reception areas, stairs, halls, lavatories, washrooms – clean and tidy.

• Keeping the furniture in such areas to a minimum – ensuring that there is little opportunity to hide devices.

• Locking unoccupied offices, rooms and store cupboards.

• Ensuring that everything has a place and that items are returned to that place.

• Considering the removal of litter bins or replacing them with clear bags.

• Putting plastic seals on maintenance hatches.

• Keeping external areas as clean and tidy as possible.

• Pruning all vegetation and trees, especially near entrances, to assist in surveillance and preventing concealment of packages.

II. Security awareness

The vigilance of the staff (including cleaning and maintenance staff) is key to one's protective measures. They will know their own offices or work areas and should be encouraged to look out for unusual behaviour or items out of place. They must have the confidence to report any suspicions, knowing that reports will be taken seriously even if they turn out to be false alarms. Staff must also know who to report to and their contact details. Training is therefore particularly important. Staff should be briefed to look out for packets, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places.

III. Access routes

An efficient reception area is essential to controlling access, with side and rear entrances denied to all but authorised people. Access points should be kept to minimum and it should be made sure that the boundary between public and private areas of building is secure and clearly signed. One should invest in good quality access

controls such as magnetic swipe identification cards or proximity cards which are readable from a short distance.

IV. Security passes

If a staff pass system is in place, one should insist that staff wear their passes at all times and that their issuing is strictly controlled and regularly reviewed. Visitors should be escorted and should wear clearly marked temporary passes, which must be returned on leaving. Anyone not displaying security passes should either be challenged or reported immediately to security or management. Consider introducing a pass system there is not one already in place.

V. Screening

The random screening of hand baggage is a significant deterrent and organization have the right to refuse entry to anyone who does not allow to search their possessions. However, body searches may be carried out only with the agreement of the person being searched. Routine searching and patrolling of premises represents another level of screening covering both internal and external areas. Keep the patrols regular, but not too predictable.

VI. Traffic and parking controls

If one believes that office might be at risk from a vehicle bomb, the basic principle is to keep all vehicles at a safe distance. Those requiring essential access should be identified in advance and checked before being allowed through. If possible, one should ensure that they have proper access control, careful landscaping, traffic-calming measures and robust, well-lit barriers or bollards. Ideally, non-essential vehicles should be kept at least 30 metres from building.

VII. Doors and windows

Good quality doors and windows are essential to ensure a building's security. External doors should be strong, well-lit and have good quality locks. Alarms can be considered as well. Doors that are not often used should also have internal bolts. All accessible windows should have good quality key-operated locks. Many casualties in urban terrorist attacks are from flying glass, especially in modern buildings, and glazing protection is an important casualty reduction measure. Extensive research has been

carried out on the effects of blast on glass. There are technologies that minimise shattering and casualties, as well as the costs of re-occupation. Anti-shatter film, which holds fragmented pieces of glass together, offers a relatively cheap and rapid improvement to existing glazing. If new windows has to be installed, laminated glass can be considered, but before undertaking any improvements seek specialist advice through police Counter Terrorism Security Adviser.

VIII. Integrated security systems

Intruder alarms, CCTV and lighting are commonly used to deter crime, detect offenders and delay their actions. All these systems must be integrated so that they work together in an effective and co-ordinated manner. Intrusion detection technology can play an important role in an integrated security system; it is as much a deterrent as a means of protection. Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations, but only if the images are good enough to identify what happened and be used in court. External lighting provides an obvious means of deterrence as well as detection, but impact of additional lighting on neighbours should be taken into account. If it is carefully designed and used, external lighting will help security staff and improve the capabilities of CCTV systems.

Managing staff securely

Besides ensuring physical and data security of an organization, it is also crucial to guard the employee's and visitor's activities in the premises.

I. Detailed and exhaustive verification of employee, employee's reference and all related documents:

Some external threats, whether from criminals, terrorists or competitors seeking a business advantage, may rely upon the co-operation of an insider. This could be an employee or any contract or agency staff (e.g. cleaner, caterer, security guard) who has authorised access to office premises. If an employee, he or she may already be working, or may be someone newly joined who has infiltrated organisation specifically in order to seek information or exploit the access that the job might provide. Much of the following advice simply reflects good basic recruitment and employment practice. During the recruitment process one should ask each candidate to:

• Confirm their full name, date of birth and address with a supporting official document such as a photo driving licence or passport. Other useful identifying documents are credit card with statements, birth certificate, cheque book and bank card with signature and bank statements (account documentation from any financial institution is particularly useful as they will usually have made their own identity checks before opening an account). Ask to see recent utility bills confirming the given address. Do not accept as proof of identity any duplicate or photocopied documents, an international driving licence, or a birth certificate issued more than six weeks after birth.

• Give evidence of academic or professional qualifications. Take up any references from schools, colleges, universities and previous employers (again, insist on originals) and check with the originators that they are genuine.

• Give full details of previous employers (name, address and date) covering at least the past three years.

• Give details of any unspent convictions, or NOC/Affidavit from police authorities certifying that no civil/criminal prosecution is pending. Remember, however, that a conviction – spent or unspent – need not be a bar to employment.

Having obtained this information, check it: the increasing availability of reasonably good quality false documentation on the internet has made establishing identity more of a problem than it used to be. Look out for any obvious gaps and inconsistencies in the applicant's employment or residential history. All this will take time, so if one need the candidate to start work quickly, or if an offer of employment is made, then make the satisfactory completion of the checks a condition of employment. In all cases, remind applicants that supplying false information or failing to disclose relevant information could be grounds for dismissal and could amount to a criminal offence, candidate should be made sign such a declaration.

II. Shredding, incineration of important and sensitive documents

Companies and individuals sometimes need to dispose of sensitive information. Some of the material that businesses routinely throw away could be of use to a wide variety of groups including business competitors, identity thieves, criminals and terrorists. The types of information vary from staff names and addresses, telephone numbers, product information, customer details, technical specifications and chemical and biological data. Terrorist groups are known to have shown interest in this area.

The principal means of destroying sensitive waste are:

i. Shredding

A cross-cutting shredder should be used so that no two adjacent characters are legible. This produces a shred size of 15mm x 4mm assuming a text font size of 12.

ii. Incineration

Incineration is probably the most effective way of destroying sensitive waste, including disks and other forms of magnetic and optical media, provided a suitable incinerator is used (check with local authority).

Open fires are not reliable as material is not always destroyed and legible papers can be distributed by the updraft.

Electronic attack

Since the entire organizational data-related transactions are carried out through electronic medium, so data security becomes very critical, in order to protect organizations from any electronic attack.

Electronic attack could:

• Allow the attacker to remove sensitive information.

• Allow the attacker to gain access to computer system and do whatever the system owner can do. This could include modifying data, perhaps subtly so that it is not immediately apparent, or installing hardware or software devices to relay information back to the attacker. Such attacks against internet-connected systems are extremely common.

As soon as one entrust his/her information or business processes to a computer system, they are at risk. Electronic attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet.

The typical methods of electronic attack are:

i. Hacking

This is an attempt at unauthorised access, almost always with malicious or criminal intent. Sophisticated, well-concealed attacks by foreign intelligence services seeking information have been aimed at government systems but high-tech industries might also be targets.

ii. Malicious software

The techniques and effects of malicious software (e.g. viruses, worms, trojans) are as variable as they are widely known. The use of e-mail, systems that interconnect, external contractors and remote access (e.g. for home working) allows virus infections to spread ever more widely and rapidly.

iii. Malicious modification of hardware

Computer hardware can be modified so as to mount or permit an electronic attack. This is normally done at the point of manufacture or supply prior to installation, though it could also be done during maintenance visits. The purpose of such modifications would be to allow a subsequent attack to be made, possibly by remote activation.

As with other security measures, one should conduct a risk assessment to establish whether organization might be at particular risk from an electronic attack. System security professionals can provide detailed advice.

Protective Security Measures that can be considered:

• Acquire IT systems from reputable manufacturers and suppliers,

• Ensure that software is regularly updated. Suppliers are continually fixing security vulnerabilities in their software. These fixes or patches are available from their websites – consider checking for patches and updates at least weekly.

• Ensure that all internet-connected computers are equipped with anti-virus software and are protected by a firewall.

• Back up the information, preferably keeping a secure copy in another location.

• Assess the reliability of those who maintain, operate and guard systems.

• Consider encryption packages for material which needs to be protected, particularly if taken off-site – but seek expert advice first.

• Take basic security precautions to prevent software or other sensitive information falling into the wrong hands. Encourage security awareness among staff, training them not to leave sensitive material lying around and to operate a clear desk policy (i.e. desks to be cleared of all work material at the end of each working session).

• Make sure the staff are aware that users can be tricked into revealing information which can be used to gain access to a system, such as user names and passwords.

• Investing in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material.

• Where possible, lock down or disable disk drives, USB ports and wireless connections.

• Ensure computer access is protected by securely controlled, individual passwords or by biometrics and passwords.

1.2 Objective of the Study

The objective of this dissertation is to review and synthesize the literature of psychological contract in order to provide a comprehensive framework for psychological contract in hostile workplace environment. The report provides an inclusive review of antecedents and outcomes of psychological contract. The work aimed to determine the factors associated with Psychological contract in hostile workplace environment and assessing their impact on the expectations of employee and employer. The report begins with the overview of the Psychological contracts. Literature on complexities and challenges associated with Psychological contract as a construct is subsequently reviewed. The method as well as an overview of the findings of the review is presented. The dissertation concludes with way forward and implications for research scholars and practitioners.

1.3 Scope of the Study

In order to ensure organizational security in hostile environments, risk management activities, ranging from identifying potential risks to a formal risk management cycle, need to be put in place. With the changing work environment and increasing hostility, so does the nature of the relationships between employees and employers. The study is conducted to know various factors impacting the expectations of employee and employer in hostile workplace environment. By looking it one can adopt measure to ensure safety, security and harmony at the work place by identifying the potential threats which in-turn will enhance the organizational performance and productivity.

2 Literature Review

Argyris (1960) coined the term "psychological work contract" emphasizing implicit relationship between leaders and subordinates from the lenses of leadership styles used by leaders. Schein (1965) extended the concept further and emphasized upon the relevance of Psychological contract for managing employee behaviours in organizations. Schein argued that employees and organizations have multiple expectations from each other that change continually. Thereafter, work on Psychological contract was limited and geared up with seminal work by Rousseau (1989). Rousseau (1995) defined Psychological contract as "individual beliefs, shaped by the organization, regarding terms of an exchange agreement between individuals and their organization". Psychological contract is important to researchers and practitioners alike due to its association with critical organizational outcomes.

Studies highlight that various individual and organizational factors play a critical role in influencing the Psychological contract of employees. The basic tenet of the papers reviewed is that individual and organizational level variables can change the Psychological contract and subsequently the work outcomes. The studies examining the link between individual variables and Psychological contract are limited. In most of the studies individual variables particularly age and gender are considered as control variable. Some studies do provide a detailed description of association of Psychological contract with gender and age. There are plethora of research examining the association between organizational variables and Psychological contract. Since, Psychological contract is perceptual and idiosyncratic employee might perceive the same Psychological contract differently. Psychological contract has emerged as a construct to deal with complex relationship between the employees and employers (Pate, 2006). The research in the area of Psychological contract has grown significantly due to its link with favourable organizational outcomes.

Psychological contract refers to the expectations which employee and employer have from each other and what they owe to each other. The traditional Psychological contract between the employee and employer is breaking. In a fiercely competitive environment employer is no longer obliged to provide lifelong job security, guaranteed pay increases, and assured career opportunities (Singh, 1998; Herriot et al., 1997). The

old Psychological contract is altered and both employee and employer are equally concerned about the new Psychological contract (Rousseau, 1995; Welch & Hood, 1992). The new Psychological contract has resulted in emergence of new factors and outcomes. A healthy employee-employer relationship has become fundamental aspect for survival of the organization. The examination of its factors is necessary in order to understand and predict the consequences of Psychological contract. There are various individual and organizational factors which influence Psychological contract. Therefore, there is need for comprehensive framework to understand the Psychological contract to take it to another level in the current era.

Workers who have gone through workplace threats and actual violence are likely to be more depressed and to report more anxiety and less job satisfaction (Driscoll, Worthington, & Hurrell, 1995). They are also more likely to suffer from decreased well-being (Schat & Kelloway, 2003) and to experience more health problems (Shakespeare-Finch, Smith, & Obst, 2002) than employees who have not been confronted with violence or aggression.

The psychological contract refers to an individual's beliefs about terms and conditions of a reciprocal exchange agreement between that person and his or her employer (Robinson,1996; Robinson & Rousseau, 1994; Rousseau, 1989; Rousseau & Tijoriwala, 1998). It specifies the contributions that employees believe they owe to their employer and the obligations and inducements they believe are owed in return (Robinson & Rousseau, 1994). Psychological contract breach is likely to result when employees perceive that they have made contributions as promised, yet the employer failed to reciprocate these contributions (Morrison & obinson, 1997; Robinson, Kraatz, & Rousseau, 1994). In the case of threats of violence, this may also hold for the violation of more explicit agreements, such as the "duty of care" (i.e., the requirement that everything reasonably be done to protect the health and safety of employees; Cartwright & Cooper, 1996). This can also be interpreted as inequity; inequity occurs when—in the perception of employees—the employer has failed to adequately fulfil promised obligations (Arnold, 1996; Coyle-Shapiro, 2002). The resulting output-input ratio may be perceived as unequal and employees will strive to restore this inequity by decreasing commitment and dedication.

Terrorism is the premeditated use or threat of use of violence by individuals or subnational groups to obtain a political or social objective through the intimidation of a large audience, beyond that of the immediate victim. Although the motives of terrorists may differ, their actions follow a standard pattern with terrorist incidents assuming a variety of forms: airplane hijackings, kidnappings, assassinations, threats, bombings, and suicide attacks. Terrorist attacks are intended to apply sufficient pressures to a government so that it grants political concessions. If a besieged government views the anticipated costs of future terrorist actions as
greater than the costs of conceding to terrorist demands, then a government will make some accommodation. Thus, a rational terrorist organization can, in principle, reach its goal quicker if it is able to augment the consequences of its campaign. These consequences can assume many forms including casualties, destroyed buildings, a heightened anxiety level, and myriad economic costs. Clearly, the attacks on September 11, 2001 (henceforth, 9/11) had significant costs that have been estimated to be in the range of $80 to $90 billion when subsequent economic losses in lost wages, workman's compensation, and reduced commerce are included (Kunreuther, Michel-Kerjan, and Porter, 2003).

Terrorism can be considered to be severely affecting the business environment, clearly posing a threat for internationally operating firms. However, it is not the only form of violent risk and danger though. While already having or currently developing prosperous and growing markets, many countries in the world are endangered by violent conflict, civil unrest, drug-related crime and other forms of crises. This is detrimental for business, especially for subsidiaries of foreign MNCs (Oh & Oetzel, 2011). In terms of foreign direct investment, Oh and Oetzel (2011) revealed that the presence of man-made disasters, such as terrorism, compared to natural disasters, significantly decreases the number of foreign subsidiaries. Besides responses to violent conflict and terrorism on subsidiary level, there are also negative outcomes on the individual level. For instance, Bader and Berg (2013) found that various terrorism-related pressures can cause stress, which eventually impedes expatriate work attitudes and performance. Reade and Lee (2012) showed that violent ethno-political conflict decreases organizational commitment in foreign-based firms, whereas such effects could not be detected for indigenous companies.

The psychological contract in employment refers to the system of beliefs that an individual and his or her employer hold regarding the terms of their exchange agreement (Rousseau, 1995). These beliefs are shaped by preemployment factors (e.g., values, motives), on-the-job experiences (e.g., socialization practices), and broader societal context (e.g., norms). Psychological contracts are characterized as "schemas shaped by multilevel factors" (Rousseau, 2001a, p. 525), which affect the creation of meaning around promises and commitments workers and employers make to each other, the interpretations of the scope of their obligations, and the degree of mutuality and reciprocity the parties manifest. Much of the value in creating psychological contracts lies in their capacity to reduce insecurities and anticipate future exchanges, helping both individuals and organizations to meet their needs (Rousseau, 1995; Shore & Tetrick, 1994). When workers and employers agree on the terms of the contract, their future exchanges develop into actions predictable by each party, facilitating planning, coordination, and effective performance (Rousseau, 1995). This agreement becomes manifest in the degree of mutuality and reciprocity between the parties to a psychological contract. In the context of psychological contract, mutuality describes the degree to which the two parties agree on their interpretations of promises and commitments each party has made and accepted (i.e., agreement on what each owes the other). Reciprocity refers to the degree of agreement about the reciprocal exchange, given that commitments or contributions made by one party obligate the other to provide an appropriate return. When an individual becomes employed at an organization, many paper contracts are signed where both the employee and the organization develop expectations of each other. What many employees do not realize is that they are also forming another contract that is not written on paper nor articulated. This contract is called a psychological contract. A psychological contract plays a vital role in how employees perceive their organizations as well as how they will perform.

Theories of organisational behaviour suggest that a psychological contract between an employee and an organisation will emerge and develop in virtually every employment relationship. Given that these psychological contracts consist of the expectations that employees, in particular, will have of their employing organisation (and its managers), it is evidently important that managers are at least aware of the existence of these contracts and recognise that employees have legitimate expectations relating to how they are treated at work. Psychological contracts are normally thought to be important

because their breach has been found to lead to serious consequences. Thus, it is vital that managers understand, manage and work to fulfil and sustain psychological contracts if these adverse consequences are to be avoided.

Barnard's (1938) theory of equilibrium posits that employees' continued participation depends upon adequate rewards from the organization. Here lies the idea of a reciprocal exchange underlying the employee-organization relationship. This was elaborated upon by March and Simon (1958) in their inducements-contributions model. They argued that employees are satisfied when there is a greater difference between the inducements offered by the organization and the contributions they need to give in return. From the organization's perspective, employee contributions need to be sufficient enough to generate inducements from the organization, which in turn need to be attractive enough to elicit employee contributions. The work of March and Simon (1958) is rarely acknowledged in the psychological contract literature (Conway & Briner, 2005) but the idea of a reciprocal exchange bears a remarkable resemblance to a core tenet of the psychological contract.

Argyris (1960) viewed the psychological contract as an implicit understanding between a group of employees and their foreman, and argued that the relationship could develop in such a way that employees would exchange higher productivity and lower grievances in return for acceptable wages and job security (Taylor & Tekleab, 2004). Argyris (1960) believed that employees would perform at a higher level if the organization did not interfere too much with the employee group's norms and in return employees would respect the right of the organization to evolve. The defining characteristics of this first explicit conceptualization of the psychological contract viewed it as an exchange of tangible, specific and primarily economic resources agreed by the two parties that permitted the fulfillment of each party's needs.

Subsequently, Levinson et al. (1962) introduced a more elaborate conceptualization of the psychological contract that was heavily influenced by the work of Menninger (1958). Menninger (1958) suggested that in addition to tangible resources, contractual relationships also involve the exchange of intangibles. Furthermore, the exchange between the two parties needs to provide mutual satisfaction in order for the relationship to continue (Roehling, 1996). Levinson et al. (1962) based their definition of the psychological contract on the data they gathered in interviewing 874 employees who spoke of expectations that seemed to have an obligatory quality. They defined the psychological contract as comprising mutual expectations between an employee and

the employer. These expectations may arise from unconscious motives and thus each party may not be aware of the own expectations yet alone the expectations of the other party.

The findings of Levinson et al's (1962) study highlighted the role of reciprocity and the effect of anticipated satisfaction of expectations. Specifically, the emphasis on the fulfillment of needs created a relationship in which employees would try and fulfill the needs of the organization *if* the organization fulfilled the needs of employees. Thus, the employee and organization held strong expectations of each other and it was the anticipation of meeting those expectations that motivated the two parties to continue in that relationship. Taylor and Tekleab (2004) note that the work of Levinson et al. (1962) contributed in the following ways: the two parties in the contract are the individual employee and the organization represented by individual managers; the psychological contract covers complex issues – some expectations are widely shared, others are more individualized and the specificity of expectations may range from highly specific to very general; the psychological contract is subject to change as the parties negotiate changes in expectations that may arise from changes in circumstances or a more complete understanding of the contributions of the other party.

Although Schein's (1965) definition shares some similarities with Levinson et al (1962), he placed considerable emphasis on the matching of expectations between the employee and organization. The matching of expectations and their fulfilment is crucial to attaining positive outcomes such as job satisfaction, commitment and performance. Consistent with this, Schein (1965) by implication highlighted the importance of understanding both the employee's as well as the employer's perspective. Schein went further than previous researchers in discussing how organizations might express the organization's psychological contract through its culture.

In the late 1980s, Denise Rousseau (1989) described the psychological contract construct as underdeveloped and misunderstood. As a result, she attempted to provide clarity to the construct. A revitalized interest in psychological contracts at the time was also being credited to new people-focused management practices and an economy that was facing increased international competition (Anderson & Schalk, 1998; Cullinane & Dundon, 2006). In response, Rousseau offered a refined conceptualization of the psychological contract, indicating what it was and was not (Anderson & Schalk, 1998;

Conway & Briner, 2009; DelCampo, 2007). First, she emphasized that the psychological contract was a subjective perception held by one individual (Rousseau 1989, 1995). As noted earlier, there was inconsistency up to this point as to whether the psychological contract was an individual- or group-level phenomenon. Rousseau viewed the psychological contract as beliefs and perceptions about the relationship, as each employer and employee viewed it.

Secondly, Rousseau (1989) defined the psychological contract as promissory in nature. She also distinguished this promissory nature of psychological contracts from expectations and obligations. She argued that although psychological contracts do entail expectations, not all expectations are contractual (Robinson & Rousseau, 1994; Rousseau & Tijoriwala, 1998). For example, a new employee may expect to receive a pay raise after one year of work because this occurred at his/her last job. However, because this expectation was not contractually implied by the current employer, it is not part of the psychological contract (Robinson, 1996). Similarly, obligations do not necessarily possess the same contractual commitment as promises (Roehling, 2008; Rousseau, 1989). For example, an employee may believe that his/her employer is obligated to provide flexible work hours because the practice is common in his/her particular industry. However, if the employer did not implicitly or explicitly make that promise to the employee directly, Rousseau argued that the obligation is not part of that particular psychological contract.

Conway and Briner (2005, 2009) reported that promises should be the preferred conceptualization of psychological contracts, compared to expectations and obligations, because of the strong contractual nature and precise elements of promises. Cassar and Briner (2009) noted however, that the binding connotation in the term promises is only applicable in North American cultures, and may convey less of a commitment orientation in other cultures. After conducting interviews of Maltese workers, Cassar and Briner concluded that the term obligation represented a more binding relationship between the employer and employee, compared to promises.

In a study on expatriate social networks, Bader and Schuster (2015) empirically showed that the prevalence of terrorism per se does not directly decrease the individual's psychological well-being; however, positive effects of a big social network are even more important when a country's terrorism threat is high. All these impacts are burdensome to business and their employees and can create bigger

problems if the organization, in particular HRM, is not dealing with them appropriately.

Terrorism can impose costs on a targeted country through a number of avenues. Terrorist incidents have economic consequences by diverting foreign direct investment, destroying infrastructure, redirecting public investment funds to security, or limiting trade. If a developing country loses enough FDI, which is an important source of savings, then it may also experience reduced economic growth. Just as capital may take flight from a country plagued by a civil war (see Collier et al., 2003), a sufficiently intense terrorist campaign may greatly reduce capital inflows (Enders and Sandler, 1996). Terrorism, like civil conflicts, may cause spill-over costs among neighbouring countries as a terrorist campaign in a neighbour dissuades capital inflows, or a regional multiplier causes lost economic activity in the terrorism-ridden country to resonate throughout the region. In some instances, terrorism may impact specific industries as 9/11 did on airlines and tourism (Drakos, 2004; Ito and Lee, 2004). Another cost is the expensive security measures that must be instituted following large attacks – e.g., the massive homeland security outlays since 9/11 (Enders and Sandler, 2006, Chapter 10). Terrorism also raises the costs of doing business in terms of higher insurance premiums, expensive security precautions, and larger salaries to at-risk employees. The size and the diversity of an economy have much to do with the ability of a country to withstand terrorist attacks without showing significant economic effects. Yemen's shipping industry suffered greatly after the terrorist attacks on the USS Cole and the Limburg diverted half of Yemen's port activities to competitive facilities in Djibouti and Oman due to a 300% increase in insurance premiums (US Department of State Fact Sheet, 2002). In a more diversified and developed economy, such losses may have a temporary influence as resources are reallocated to other sectors or better security measures are deployed to allay concerns. Moreover, developed economies have better monetary and fiscal capabilities to limit macroeconomic impacts of terrorist attacks than small developing countries. Thus, we should anticipate that developed countries are more likely to display sector-specific reactions to terrorism attacks, while developing countries are apt to exhibit some macroeconomic consequences to a particularly vicious attack or a sustained terror campaign.

The National Counterterrorism Center (2012) reports more than 10,000 attacks just in the year

2011, killing or injuring almost 45,000 people in 70 countries. Despite the relatively low likelihood for an individual of actually becoming a direct victim of an attack, compared to, for instance, being killed in a car accident, indirect effects prevail. Reade and Lee (2012) found that operating in a terrorism-endangered area has a tremendous negative effect on the organizational commitment of the workforce. More concretely, Bader and Berg (2013) analysed the impact of terrorism on expatriates, finding that expatriates who experience stress from terrorism perform worse than those who are not affected by this. Global relocation involves many changes and stressful challenges. For instance, learning a new language, adapting to different cultural norms, and establishing a new social network are some of the possibly associated challenges (Caligiuri, Hyland, Bross, et al., 1998; Selmer, 2001). In terrorism-endangered countries, these challenges are multiplied by safety concerns (Bhanugopan & Fish, 2008; Wagner & Westaby, 2009). For example, Bader and Berg (2013) found evidence that terrorism-induced stress lowers an expatriate's work attitudes, increases his or her disaffection with host country nationals (HCNs), and eventually impedes his or her performance. If the expatriate's family members are accompanying him or her on the assignment, they are also exposed to these dangers (Shimoni, Ronen, & Roziner, 2005). However, even if the spouse stays in the home country, there is potential for disputes about the safety situation, since mutual concern and regular contact is assumed to be given in the nuclear family. Thus, it is promising to incorporate the role of spouses and family members when investigating performance consequences for expatriates.

A study by Beatty, Ewing and Sharp (2003) also showed that HR risk was associated with higher organisational risk. The very nature of global HR poses several risks, like political instability, fraud, terrorism, regulations, health and safety, human rights abuses and intellectual property issues (Garratt, 2003).

3 Research Methodology

There are three types of research methodologies, they are:

1. Explorative
2. Descriptive
3. Experimental

Descriptive methodology is used in the present study.

3.1 Data Sources

Primary Data:

Primary data was collected from the respondents by administering a structured questionnaire.

Secondary Data:

Apart from Primary data. The secondary data is being collected through existing Research Papers, Journals, Academic Reports, Internet, and Text books, used for this study.

3.2 Research Model

Figure 7: Research Model

3.3 Work flow of the Study

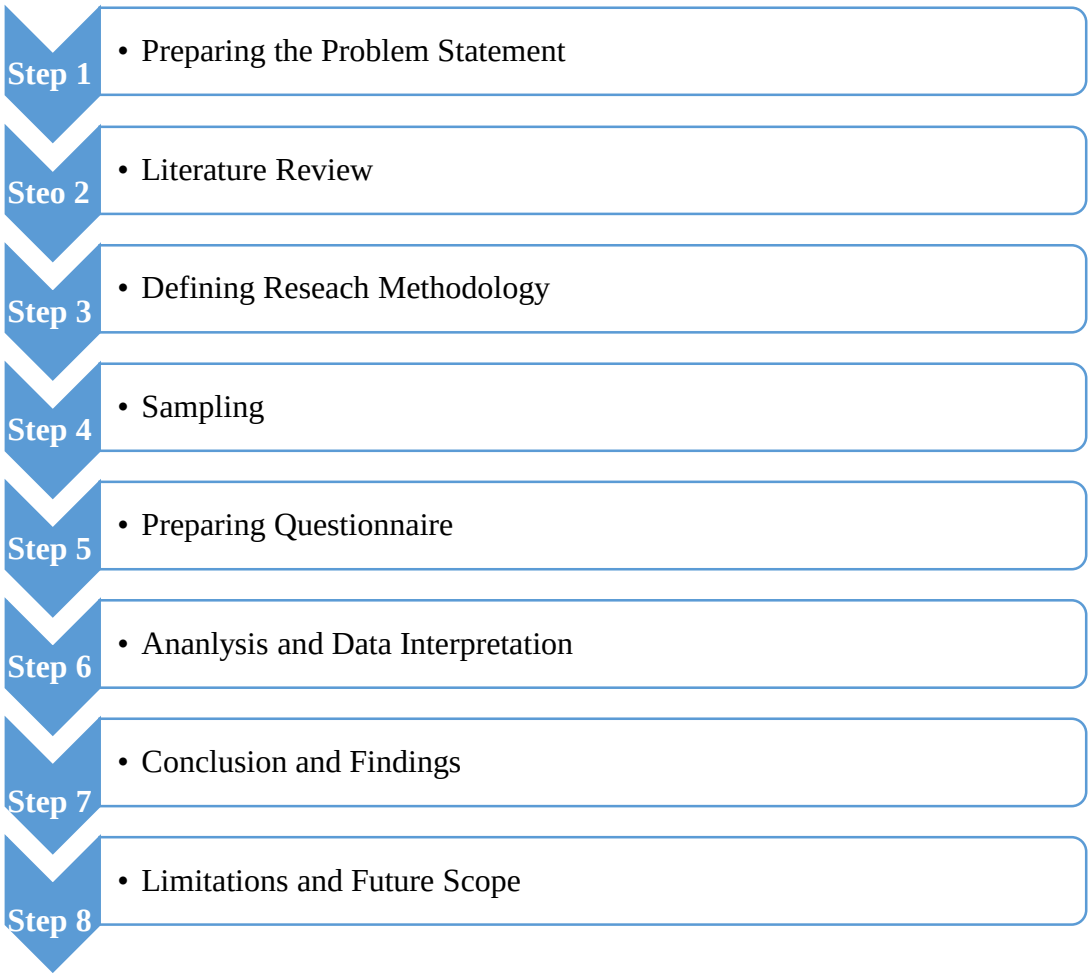

Figure 8: Work flow of the Study

3.4 Sampling

3.4.1 Sample Size:

Out of the total 107 respondents - 80 are currently students, 20 are current employees working in different firms and 7 are employers of different firms.

3.4.2 Sample Method:

The research was made by the survey in accordance to the convenience of the respondents. So the sample type is convenience sampling.

4 Data Analysis

4.1 Tools used for analysis

4.1.1 Instrument

A structured Questionnaire is used and the type of questionnaire is target questions. For analysis Microsoft Excel has been used.

4.1.2 Method

The research was conducted by using contact methods through Questionnaire. The information was collected from the assorted sample containing students, employees and employers.

4.2 Conclusions and Findings

Following are key findings of this study:

I. Out of all the independent variables, Workplace Security is majorly dependent upon “Managing Risk”.

II. Based on the analysis of individual independent variables, following can be deduced:
   a. From first independent variable Managing Risks, “Address issues like identification of threat” is the most important factor.
   b. From second independent variable Security Co-ordination, “Generating a security plan” is the most critical factor.
   c. From third independent variable Physical Security, “Security passes for employees (with electronic or biometric verification)” is the most vital factor.
   d. From fourth independent variable Managing Staff Securely, “Detailed and exhaustive verification of employee, employee’s reference and all related documents” primarily affects this factor.

e. From fifth independent factor Electronic attack, “Protection against hackers, malicious software and malicious modification of hardware” plays the key role in protection against Electronic attack.
f. From sixth and last independent factor Religion, “Some informal talks or comments on certain religious norms” makes an individual most uncomfortable at work.

III. Based on gender, following can be inferred:

a. Out of all independent variables, Workplace Security is majorly dependent upon “Managing Risk”, irrespective of the gender.
b. From first independent variable Managing Risks, “Address issues like identification of threat” is the most important factor, for females.
c. From first independent variable Managing Risks, “Identify Company’s vulnerability and what is to be protected” is the most important factor, for males.
d. From second independent variable Security Co-ordination, “Generating a security plan’ is the most critical factor, irrespective of the gender.
e. From third independent variable Physical Security, “Passes for visitors after submitting their government approved identification card with photograph on entry” is the most vital factor, for females.
f. From third independent variable Physical Security, “Security passes for employees (with electronic or biometric verification)” is the most vital factor, for males.
g. From fourth independent variable Managing Staff Securely, “Detailed and exhaustive verification of employee, employee’s reference and all related documents” primarily affects this factor, irrespective of the gender.
h. From fifth independent factor Electronic attack, “Data back-up at another secure location” plays the key role in protection against Electronic attack, for females.
i. From fifth independent factor Electronic attack, “Protection against hackers, malicious software and malicious modification of hardware” plays the key role in protection against Electronic attack, for females.

j. From sixth and last independent factor Religion, “Some informal talks or comments on certain religious norms” makes an individual most uncomfortable at work, for females.
k. From sixth and last independent factor Religion, “People exhibiting their religious beliefs at workplace” makes an individual most uncomfortable at work, for males.

IV. Based on number of years of experience following can be implied:
a. For respondents with $0 \leq 2$ experience, the most critical variable out of all the six independent variables is “Managing Risks”.
b. For respondents with $2 \leq 3$ experience, the most critical variable out of all the six independent variables is “Security Co-ordination”.
c. For respondents with $3 \leq 4$ experience, experience, the most critical variable out of all the six independent variables is “Security Co-ordination”.
d. For respondents with > 4 experience, the most critical variable out of all the six independent variables is “Electronic attack”.

V. From employer’s perspective following can be implied:
a. Out of all independent variables, Workplace Security is majorly dependent upon “Security Co-ordination”.
b. From first independent variable Managing Risks, “Identify measures to reduce risk” is the most important factor.
c. From second independent variable Security Co-ordination, “Conducting regular review of security procedures” is the most critical factor.
d. From third independent variable Physical Security, “Integrated security systems - intruder alarms, CCTV cameras and adequate lighting” is the most vital factor.
e. From fourth independent variable Managing Staff Securely, “Watching for unusual behavior at/around the premises” primarily affects this factor.

f. From fifth independent factor Electronic attack, "Data back-up at another secure location" plays the key role in protection against Electronic attack.
g. From sixth and last independent factor Religion, "People exhibiting their religious beliefs at workplace make me uncomfortable" makes an individual most uncomfortable at work.

4.3 Limitations and Future Scope of the Study

Since sample size of respondents primarily includes the students and employees and only a handful of employers are included, so primary research can be carried out with the optimum assorted group to get the more accurate result.

Further literature could be reviewed and some more variables can be added into this study.

Using some other tool like SPSS, statistical analysis of data is possible to find out the correlation between ranks of different variables. Relation between different independent variables can also be make out.

5 References

1) Li, J., & Dai, L. T. (2015). A Review of Psychological Contract. Psychology, 6, 1539-1544.http://Dx.Doi.Org/10.4236/Psych.2015.612150
2) Agarwal, P. (2014, 3 December). The Psychological Contract: A Review Model. [Weblog]. Retrieved 24 April 2016, From http://Www.Iimahd.Ernet.In/Assets/Snippets/Workingpaperpdf/12762980542104-12-03.Pdf
3) Bader, B, Berg, N & Holtbrugge, D. (2015). Expatriate Performance in Terrorism-Endangered Countries: The Role Of Family And Organizational Support. Elsevier Ltd, 849-860
4) Sandler, T & Enders, W. (2008). Economic Consequences of Terrorism in Developed and Developing Countries: An Overview. Retrieved 24 April, 2016, From http://Www.Utdallas.Edu/~Tms063000/Website/Econ_Consequences_Ms.Pdf
5) Long, B. (2003). Psychological Aspects of the Hostile Workplace: Harassment and Bullying. [Weblog]. Retrieved 24 April, 2016, From http://Barbaralongmdphd.Com/Hostileworkplace.Pdf
6) Mcinnis, Kate J., "Psychological Contracts in the Workplace: A Mixed Methods Design Project" (2012). Electronic Thesis and Dissertation Repository. Paper 383
7) Coyle-Shapiro, Jacqueline A-M. And Parzefall, M. (2008) Psychological Contracts. In: Cooper, Cary L. And Barling, Julian, (Eds.) the SAGE Handbook of Organizational Behavior. SAGE Publications, London, UK, Pp. 17-34
8) Protection against Terrorism. Security Service MI5. 272839/0306/D88 (Secured). Retrieved 24 April, 2016, From http://Www.Lancsresilience.Org.Uk/Documents/Bcm/Protecting_Against_Terrorism.Pdf
9) Global Terrorism Index Report (2014). Measuring and Understanding the Impact of Terrorism. Institute Of Economics and Peace. Retrieved 24 April, 2016, From http://Economicsandpeace.Org/Wp-Content/Uploads/2015/11/Global-Terrorism-Index-2015.Pdf
10) Herriot, P., Manning, W. E. G., & Kidd, J. M. (1997). The Content of the Psychological Contract. British Journal of Management, 8, 151-162. http://Dx.Doi.Org/10.1111/1467-8551.0047

11) Arnold, J. (1996). The Psychological Contract: A Concept In Need Of Closer Scrutiny. European Journal Of Work And Organizational Psychology, 5, 511-520
12) Morrison, E. W., & Robinson, S. L. (1997). When Employees Feel Betrayed: A Model of How Psychological Contract Violation. Develops. Academy of Management Review, 22, 226-256
13) Meyer, M., Roodt, G., & Robbins, M. (2011). Human resources risk management: Governing people risks for improved performance. SA Journal of Human Resource Management/SA Tydskrif vir Menslikehulpbronbestuur, 9(1), Art. #366, 12 pages. doi:10.4102/sajhrm.v9i1.366
14) Cullinane, N., & Dundon, T. (2006). The psychological contract: A critical review. International Journal of Management Reviews, 8, 113-129
15) Guzzo, R. A., Noonan, K. A., & Elron, E. (1994). Expatriate managers and the psychological contract. Journal of Applied Psychology, 79, 617-626

6 Adherence Sheet

Following timeline was adhered during this project dissertation:

Sr. No.	Phases	Expected date to finish the task	Actual date to finish the task
I	Proposal discussion	5th April 2016	31st March 2016
II	Data Collection and Analysis	12th April 2016	12th April 2016
III	First draft	19th April 2016	24th April 2016
IV	Final report submission	26th April 2016	29th April 2016

7 Annexure

7.1 Questionnaire

PART A: Demographics

Name* _____

Age* _____

Gender* _____

Total Years of _____ Experience*

PART B: Factors affecting Workplace Security

1. Managing Risks

In order to ensure organizational security in hostile environments, risk management activities, ranging from identifying potential risks to a formal risk management cycle, need to be put in place.*

Kindly rank the following items from 1 (Most critical) to 5 (Least critical). Note: You cannot give same rank to more than one item.

	1	2	3	4	5
Address issues like identification of threat	○	○	○	○	○
Identify companies vulnerability and what is to be protected	○	○	○	○	○
Identify measures to reduce risk	○	○	○	○	○
Incorporate risk management cycle	○	○	○	○	○
Review security	○	○	○	○	○

	1	2	3	4	5
measures and rehearse security plans					

2. Security Co-ordination

To stay uptight against any form of physical or electronic attack, an organization needs to draft and execute thorough security arrangements *

Kindly rank the following items from 1 (Most critical) to 6 (Least critical). Note: You cannot give same rank to more than one item.

	1	2	3	4	5	6
Generating a security plan						
Formulating contingency plan dealing with threat packages, possible evacuation, bomb threats and so on						
Arranging staff training and mock drills						
Conducting regular review of security procedures						
Presence of security coordinator or security executive						
Liaising with police and other emergency						

	1	2	3	4	5	6
services, and local authorities						

3. Physical Security

More than any form of loss, physical damage to property or human life, puts a huge question mark on the security measures of any organization or nation.*

Kindly rank the following items from 1 (Most critical) to 7 (Least critical). Note: You cannot give same rank to more than one item.

	1	2	3	4	5	6	7
Basic housekeeping such as locking unoccupied offices, rooms and cupboards, and taking care of surveillance							
Security passes for employees (with electronic or biometric verification)							
Passes for visitors after submitting their government approved identification card with photograph on entry							
Screening visitors and baggage (through metal							

	1	2	3	4	5	6	7
detectors and x-rays)							
Traffic and parking controls							
Doors and windows - bulletproof glass, alarm system							
Integrated security systems - intruder alarms, CCTV cameras and adequate lighting							

4. Managing Staff Securely

Besides ensuring physical and data security of an organization, it is also crucial to guard the employee's and visitor's activities in the premises.*

Kindly rank the following items from 1 (Most critical) to 5 (Least critical). Note: You cannot give same rank to more than one item.

	1	2	3	4	5
Detailed and exhaustive verification of employee, employee's reference and all related documents					
Shredding, incineration of important and sensitive documents					

	1	2	3	4	5
Watching for unusual behaviour at/around the premises					
Guarding against unexpected visitors					
Keeping a check on employees coming in usually early or staying late					

5. Electronic attack

Since the entire organizational data-related transactions are carried out through electronic medium, so data security becomes very critical, in order to protect organizations from any electronic attack.*

Kindly rank the following items from 1 (Most critical) to 5 (Least critical). Note: You cannot give same rank to more than one item.

	1	2	3	4	5
Protection against hackers, malicious software, malicious modification of hardware	○	○	○	○	○
Antivirus, firewall and encryption in place	○	○	○	○	○
Data back-up at another secure location	○	○	○	○	○
Granting access through password protection	○	○	○	○	○
No entrance and exit with disk drives/flash drives without proper authorization	○	○	○	○	○

6. Religion

Religion is often associated with terrorism.*

Kindly rank the following items on the basis of your comfort level with respect to given aspects, from 1 (Most uncomfortable) to 4 (Least uncomfortable). Note: You cannot give same rank to more than one item.

	1	2	3	4
Working with someone from a specific religious community makes me uncomfortable				
Working at a client location, situated in a religion-centric country, makes me uncomfortable				
People exhibiting their religious beliefs at workplace make me uncomfortable				
Some informal talks or comments on certain religious norms makes me uncomfortable				

PART C:

Individual Factor Comparison

We hope, by now you must have got a fair idea about the significance of previous mentioned factors.*

Kindly rank them in the order of their significance for workplace security, from 1 (Most critical) to 6 (Least critical). Note: You cannot give same rank to more than one item.

	1	2	3	4	5	6
Managing Risks	○	○	○	○	○	○
Security Co-ordination	○	○	○	○	○	○
Physical Security	○	○	○	○	○	○
Managing Staff Securely	○	○	○	○	○	○
Electronic Attack	○	○	○	○	○	○
Religion	○	○	○	○	○	○