Barbarian Syndrome: The Failure of Enterprise Risk Management in Outsourcing and Offshoring

Andrew Mournehis
MBus, GradCertMComm

Exhibited at: Gods, Myths and Mortals: Greek Treasures across the Millennia, Hellenic Museum Victoria, 6 Jun 2015

This thesis is in partial fulfilment of the requirements of the degree of:
Doctor of Information Technology – Charles Sturt University

March 2016

Protected by Copyright
# Table of Contents

Certificate of Authorship.......................................................................................... vii
Acknowledgments....................................................................................................... viii
List of Abbreviations ................................................................................................. ix
Definitions................................................................................................................... x
New terms................................................................................................................... xi
Abstract...................................................................................................................... xii

1. Introduction............................................................................................................. 1
   1.1 Research Questions .......................................................................................... 3
   1.2 Research Objectives ....................................................................................... 4
   1.3 Research Scope ............................................................................................... 5
   1.4 Significance of the Research .......................................................................... 5
   1.5 Chapter Overview ......................................................................................... 6

2. Literature Review .................................................................................................. 8
   2.1 Introduction to the Literature ........................................................................ 8
   2.2 Risk Management and Outsourcing ............................................................. 9
   2.3 Third-World Problems for First-World Countries ....................................... 16
   2.4 The Barbarians ............................................................................................. 17
   2.5 History Repeating ......................................................................................... 18

3. Research Methodology ......................................................................................... 21
   3.1 Research Question Design ............................................................................ 21
   3.2 Research Framework ..................................................................................... 22
      3.2.1 Research Approach ............................................................................... 22
      3.2.2 Case Study Research ............................................................................ 23
   3.3 Data Collection ............................................................................................... 24
      3.3.1 Data-Collection Procedure ................................................................... 24
      3.3.2 Survey Design ....................................................................................... 25
      3.3.3 Survey Instrument ............................................................................... 26
   3.4 Research Sampling Method ........................................................................... 27
   3.5 Research Sample Spread .............................................................................. 28
   3.6 Statistical Analysis ......................................................................................... 28
   3.7 Ethical Considerations .................................................................................. 29
   3.8 Data Quality and Control ............................................................................. 30
3.9 Long-term Research Benefits .................................................. 31
3.10 Research Project Phases ....................................................... 32

4. Research .................................................................................... 33
4.1 Research Coverage and Size Analysis ...................................... 33
4.2 Enterprise Risk Management ................................................. 37
4.3 The Risk Strategy Paradigm .................................................... 43
4.4 The Strategy of Outsourcing ................................................... 45

5. Outsourcing and Offshoring ....................................................... 49
5.1 Offshoring ............................................................................... 49
5.2 Outsourcing and Offshoring Risk ............................................. 51
5.3 Maintaining Organisational Control ....................................... 54
5.4 Offshore Trust ......................................................................... 56
5.5 Australia’s Top 5 Offshoring Destinations ............................... 57
5.6 Outsourcing Locations ............................................................. 62
  5.6.1 India ................................................................................... 62
  5.6.2 China ................................................................................. 63
  5.6.3 Brazil ................................................................................ 64
  5.6.4 United States of America ................................................ 65
  5.6.5 Philippines ....................................................................... 65
  5.6.6 Malaysia .......................................................................... 66
  5.6.7 Singapore ......................................................................... 67
  5.6.8 Argentina .......................................................................... 67
  5.6.9 Ireland .............................................................................. 67
  5.6.10 Israel ............................................................................... 68
5.7 Natural Disasters and Business Continuity .............................. 68
5.8 Social Unrest, Political Stability and Business Continuity .......... 70
5.9 Criminal Activity ...................................................................... 71
5.10 Health Care .......................................................................... 72
5.11 Economic Stability ................................................................. 73
5.12 Terrorism – The New Threat to IT Operations ....................... 74
5.13 Adjustments to ERM Practices ............................................. 76
5.14 Location Assessment Tool ................................................... 78
  5.14.1 Location Assessment – Cost ........................................... 81
  5.14.2 Location Assessment – Economy ................................... 81
## Table of Figures

<table>
<thead>
<tr>
<th>Table/Figure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 3.1 – Potential Ethical Issues</td>
</tr>
<tr>
<td>Figure 4.1 – Research Participant Roles by Industry</td>
</tr>
<tr>
<td>Figure 4.2 – Research Participant Percentage by Industry</td>
</tr>
<tr>
<td>Figure 4.3 – Research Participants by Location</td>
</tr>
<tr>
<td>Figure 4.4 – Research Participants by Employer Size</td>
</tr>
<tr>
<td>Figure 4.5 – Organisations That Outsource by Size</td>
</tr>
<tr>
<td>Figure 4.6 – Research Participant Spread by Methodology</td>
</tr>
<tr>
<td>Figure 4.7 – Action to Mitigate Risk</td>
</tr>
<tr>
<td>Figure 4.8 – Organisation’s Risk Tolerance</td>
</tr>
<tr>
<td>Figure 4.9 – Organisations Currently Utilising an Outsourcer</td>
</tr>
<tr>
<td>Figure 4.10 – Outsourced Services Currently Utilised</td>
</tr>
<tr>
<td>Figure 5.1 – Countries Outsourced to from Australia</td>
</tr>
<tr>
<td>Figure 5.2 – Offshoring Concerns of Participants</td>
</tr>
<tr>
<td>Figure 5.3 – Prefer Outsourcing to Local Firms</td>
</tr>
<tr>
<td>Figure 5.4 – More Required to Mitigate Risk</td>
</tr>
<tr>
<td>Figure 5.5 – Top 5 Offshoring Destinations</td>
</tr>
<tr>
<td>Figure 5.6 – Top 5 High Tolerance to Risk</td>
</tr>
<tr>
<td>Figure 5.7 – Top 5 Prefer Outsourcing Locally</td>
</tr>
<tr>
<td>Figure 5.8 – Top 5 Implementing Measures to Protect IP</td>
</tr>
<tr>
<td>Figure 5.9 – Top 5 More Required to Mitigate Risk</td>
</tr>
<tr>
<td>Figure 5.10 – Natural Disaster Risk Indicators</td>
</tr>
<tr>
<td>Figure 5.11 – Social and Political Stability Risk Indicators</td>
</tr>
<tr>
<td>Figure 5.12 – Crime Risk Indicators</td>
</tr>
<tr>
<td>Figure 5.13 – Health Care and Medical Risk Indicators</td>
</tr>
<tr>
<td>Figure 5.14 – Economic Stability Risk Indicators</td>
</tr>
<tr>
<td>Figure 5.15 – Terrorism Risk Indicators</td>
</tr>
<tr>
<td>Figure 5.16 – Adjustments to ERM Practices When Outsourcing</td>
</tr>
<tr>
<td>Figure 5.17 – Offshore Strategic Pillars</td>
</tr>
<tr>
<td>Figure 5.18 – Risk Matrix Customisable Scoring System</td>
</tr>
<tr>
<td>Figure 5.19 – The Four Fluctuations</td>
</tr>
<tr>
<td>Figure 5.20 – Evaluation Cycle</td>
</tr>
<tr>
<td>Figure 6.1 – Becoming Dependant on an Outsourcing Firm</td>
</tr>
<tr>
<td>Figure 6.2 – Concerned Outsourcer is Absorbing IP</td>
</tr>
<tr>
<td>Figure 6.3 – Establishing Measures to Protect Against Loss of IP</td>
</tr>
<tr>
<td>Figure 6.4 Competitive Mitosis Lifecycle</td>
</tr>
<tr>
<td>Figure 6.5 – Competitive Mitosis Stage 1</td>
</tr>
<tr>
<td>Figure 6.6 – Competitive Mitosis Stage 2</td>
</tr>
<tr>
<td>Figure 6.7 – Competitive Mitosis Stage 3</td>
</tr>
<tr>
<td>Figure 7.1 – Supply Chain Detriment</td>
</tr>
<tr>
<td>Figure 8.1 – Barbarian Syndrome Traits</td>
</tr>
<tr>
<td>Figure 11.1 – Location Assessment Form</td>
</tr>
</tbody>
</table>
Certificate of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgment is made in the thesis. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged. I agree that this thesis be accessible for the purpose of study and research in accordance with the normal conditions established by the Executive Director, Library Services or nominee, for the care, loan and reproduction of theses.

Andrew Mournehis

Dated: 25th March 2016
Acknowledgments

A large number of people have contributed to this research project. Although they may not realise it, over one hundred experienced IT professionals built the foundation of the study by providing an insight into the thoughts of professionals working in the industry, in addition to providing insight into the practices across enterprises based in Australia and New Zealand.

The works of Gibbon (1826), Bevan (1927) and Bryce (1871) with detailed accounts of what transpired in Ancient Rome and Ancient Greece provided insight into some of the oldest, most successful and complex civilisations of ancient times. An insight into the thoughts of Machiavelli would not have been possible without the work of Pocock (1976). Moreover, while there have been many authors linking business strategy to ancient ideas, the work of McAlpine (2000) provides thoughts that are particularly groundbreaking, drawing a link between Machiavellian theories and organisational practices of today. McAlpine’s work was instrumental in providing a modern business context to historical ideas.

Prof Junbin Gao, Dr Peter White and Dr Zahid Islam provided guidance and leadership that contributed to a successful research project. And Dr Tanveer Zia tasked the Chief Researcher, Andrew Mournehis, with expanding the research project to involve a reflection on past events where unmanaged risk when outsourcing impacted an enterprise. Who would have thought that outsourcing – which seems such a modern concept – could date back to 300 BC?
List of Abbreviations

ANZ – Australian and New Zealand

BPO – Business process outsourcing

CEO – Chief Executive Officer

CIO – Chief Information Officer

COBIT – Control Objectives for Information and Related Technologies

COSO – Committee of Sponsoring Organisations

CRO – Chief Risk Officer

ERM – Enterprise risk management

IaaS – Infrastructure as a service

ICT – Information & communications technology

IP – Intellectual property

ISACA – previously known as the Information Systems Audit and Control Association

IT – Information technology

ITO – Information technology outsourcing

KPI – Key performance indicator

ROA – Return on assets

SaaS – Software as a service

WTO – World Trade Organisation
Definitions

Barbarian – The term given by the Ancient Greeks to foreigners, namely anyone not of Greek or Roman origin.

Enterprise risk management or ERM “is the process of identifying major risks that confront an organisation, forecasting the significance of those risks in business processes, addressing risks in a systematic and coordinated plan, implementing the plan, and holding key individuals responsible for managing critical risks within the scope of their responsibilities” (Hampton, 2014, p20).

Intellectual property – Information and intangible capital that relates to knowledge.

Mercenaries – Privately funded soldiers.

Mitigation – Implementing measures, controls or treatments to lessen the impact or reduce the likelihood of risk (or both) with the overall objective of obtaining greater control over, and limiting exposure to, an uncertain or unpredictable outcome.

Offshoring – An activity, whereby an organisation outsources services to a location based in another nation.

Outsourcer – A firm that provides either offshore or onshore-outsourced services including technology (i.e. cloud computing) or human resources.

Risk – For the purposes of this study, risk is defined as the likelihood of an uncertain event where the outcome is unknown but could have a negative impact on an enterprise, its people or its operations.

Risk appetite or tolerance – The amount of risk that an enterprise is comfortable operating with and the degree to which the enterprise is willing to have threats persist unaddressed.
New terms

Barbarian syndrome – an affliction whereby an enterprise, in outsourcing parts of its business to an outsourcing firm, unwittingly introduces a threat that could lead to the demise of the enterprise.

Competitive mitosis – an affliction whereby intellectual property can be absorbed by an outsourcing firm from an enterprise leading to detrimental impacts on the organisation’s ability to maintain a competitive advantage.

Four fluctuations – four key outsourcing conditions that must be considered throughout an outsourcing engagement: benefits, climate and conditions, costs and pricing, and performance and quality.

Location Assessment Tool – a tool to help an organisation determine the most appropriate offshore location based on the enterprise’s risk appetite.

Offshore strategic pillars –15 strategic components that uphold a successful offshoring venture.

Supply-chain detriment – an enterprise outsources a service or business function to an outsourcing firm that then, in turn, subcontracts part or all of the work to another entity, introducing additional risk with even less visibility.
Abstract

Enterprise risk management (ERM) is the process of managing and controlling risks – that is, the unknown events that could endanger an enterprise and its operations. How ERM is being used in practice to reduce an organisation’s exposure to the risks associated with outsourcing and offshoring remains largely undocumented. In analysing the current information technology (IT) sector to understand how ERM is being applied, this research has identified key gaps in the mitigation of outsourcing risk in the Australian IT industry as well as potential impacts that could plague any enterprise worldwide. The study revealed a number of new concepts in the management of offshoring and outsourcing risk. Supply-chain detriment is a new concept identified through this research, whereby an enterprise outsources a service or business function to an outsourcing firm that then, in turn, subcontracts part or all of the work to another entity. In this scenario, the outsourcer is effectively outsourcing to another party, introducing additional risk with even less visibility. The research also identifies what it calls the *four fluctuations* – that is, four key outsourcing conditions that must be considered throughout an outsourcing engagement – and has developed a tool, called the *Location Assessment Tool*, to help an organisation determine the most appropriate offshore location based on the enterprise’s risk appetite. Two potentially destructive afflictions that can significantly impact on an enterprise when outsourcing were identified. These are *competitive mitosis*, whereby intellectual property can be absorbed by an outsourcing firm from an enterprise leading to detrimental impacts on the organisation’s ability to maintain a competitive advantage, and *barbarian syndrome*, an affliction whereby the enterprise places itself at immense risk by outsourcing the wrong business function, crippling the enterprise and opening up the potential for its prosperity to be undermined.
1. Introduction

Outsourcing (or offshoring when international) involves the subcontracting out of a product, service or people to another entity. Put simply, outsourcing involves the “contracting with a vendor, who is outside of the organisation, to develop and manage IT services” (Turban & Volonino, 2011, G-9). Outsourcing is not a new phenomenon; it has been used as a resourcing method since the earliest of times. In recent years, according to McIvor (2005, p1):

The drive for greater efficiencies and cost reductions has forced many organisations to increasingly specialise in a limited number of key areas. This has led organisations to outsource activities traditionally carried out in-house.

The main motivation behind outsourcing is to obtain benefits from the experience of other organisations whilst reducing costs, thus improving bottom lines. Outsourcing allows organisations to gain access to new technologies, achieve technological improvements more easily, draw on specialist skills available from experts and increase their agility in responding to business demands (Turban & Volonino, 2011, p382). Through outsourcing, organisations are not limited to their internal competency, and have the potential to expand their capabilities quickly, easily and at a lower cost than building the capability internally.

Although outsourcing can provide many benefits, it can potentially come with a large number of inherent risks that actually threaten the prosperity of an organisation. Risk is defined as “the probability and magnitude of a loss, disaster, or other undesirable event” (Hubbard, 2009, p8). These undesirable or unforeseen events can challenge organisations, placing their enterprise in jeopardy. When outsourcing, there is a potential risk of hidden costs, which are difficult to budget for, as well as the:

... risk of loss of intellectual property, the risk of loss of competency and the ‘lock-in’ phenomenon where the contractual obligations impose limitations on
both the buyer and the supplier in seeking alternative means to perform the outsourced task. (Tho, 2005, p105).

The management of risk is not only key to an organisation understanding the risks associated with outsourcing ventures or outsourced operations, but also vital in allowing the enterprise to control and limit the potential impact that these risks can have on the enterprise itself.

According to Sparrow (2003, p5):

IT outsourcing has grown at a phenomenal rate over the past decade in the UK, North America and Australia. The trend towards outsourcing has also increased elsewhere in Western Europe, and in South America and parts of South-East Asia including Japan.

As the industry grows it becomes more and more likely that an organisation will consider outsourcing as an option for their enterprise. Sparrow (2003, p5) notes that:

Growth is particularly strongly linked to periods of economic downturn when IT outsourcing is seen as a way to contain costs. Companies try to lower IT spending and convert unpredictable costs into fixed costs.

Leveraging outsourcing firms offshore allows an organisation to take advantage of the economic benefits associated with utilising developing nations. Carmel and Tjia (2005, p74) explain:

Offshoring is about sourcing mostly from developing and emerging countries, which have historically been more volatile, less stable, less predictable, and less transparent. When offshoring, companies are exposed to increased risks of war, terrorism, rioting, uprising, confiscation, expropriation, and currency crises.

When outsourcing offshore, the regions often selected for their financial appeal often come along with these location-based risks. These location risks have been well documented in the literature and have been covered at length in the literature review.
and subsequent sections of this thesis, yet it seems little is understood about how organisations actually protect themselves when entering into outsourcing ventures offshore.

Risk management forms the core of an organisation’s safeguard against threat. Risk management involves:

… the identification, assessment, and prioritisation of risks followed by the coordinated and economical application of resources to minimise, monitor, and control the probability and/or impact of unfortunate events. (Hubbard, 2009, p10).

Therefore it is paramount that a successful enterprise puts in place measures to manage the new and evolving risks inherent in outsourcing. As establishing an outsourcing arrangement can introduce the exposure of new risks to an enterprise, organisations should be applying risk-management techniques to protect their organisation. Through the literature review, this study exposed a gap in the literature – namely, that the policies and practices real organisations are implementing to manage the risk of outsourcing remain largely undocumented, until now.

This research involved surveying senior IT professionals in order to capture and analyse the impacts they believe outsourcing has on their organisation’s ability to safely manage its risk. The research also identified the potential areas within which the risk may increase when outsourcing offshore and gauged how effectively Australian enterprises are addressing these risks in practice. The research also identifies examples of when these risks have had dire consequences both historically and today.

1.1 Research Questions

The main research question that served as the key driver behind this research project was as follows:

*What are the impacts of outsourcing on enterprise risk-management practices in the technology sector?*
The following sub-questions also assisted in providing context to the main research question:

*Are organisations adjusting their risk-management practices when offshoring?*

*Have organisations looking to outsource realised the potential for third-world threats to impact their business?*

*Are organisations utilising an outsourcing firm concerned with the loss of their intellectual property?*

*What risks associated with outsourcing are organisations currently considering?*

*Of the concerns raised by authors, which risks are of genuine concern to enterprises in practice?*

### 1.2 Research Objectives

The objective of the research was to determine what impact outsourcing initiatives have on enterprise risk management (ERM) practices. Through the sub-questions, the research aimed at determining whether risk-management practices are adjusted to compensate for the increased exposure to risk. This includes, when firms outsource offshore and inherit location-based and often third-world risks, whether firms put in place adjustments to protect themselves from the loss of intellectual property; and what risks are actually considered in practice and how these compare to the many concerns raised in the literature. In doing so, this research project was able to expose gaps in the risk-management and outsourcing literature and the practices in place in Australian enterprises.

As detailed in the literature review, Siepmann (2013) and Lynch (2008) paint an extremely grim picture for organisations considering outsourcing. They identify a large number of risks associated with the outsourcing of business functions to other entities, particularly when the outsourcing process ends up being offshore. The literature review identified a substantial number of risks associated with outsourcing that are often not considered by organisations. By exposing these risks that are not being addressed in practice, this research was able to develop a tool that an organisation can use to assess
and mitigate the risks associated with an offshore-outsourcing program. Finally, by understanding what risk-management measures organisations currently have for reducing their exposure to risk when outsourcing, this research was able to gauge the overall threat that these risks place on the technology industry in Australia.

1.3 Research Scope
The scope of the research is as follows:

- Research was limited to the technology industry and did not cover the utilisation of outsourcing models for other sectors (for instance, agriculture, manufacturing).

- The research provided coverage for all forms of outsourcing in the technology industry, including products and services (for instance, cloud computing, IaaS, SaaS et cetera), as well as managed services and the outsourcing of human resources to other regions (offshore) for specific business functions such as software development, albeit through outsourcing providers or by the organisation itself.

- Contributions were only requested from experienced IT professionals.

1.4 Significance of the Research
The research undertaken is of importance to the IT industry as it bridges the gap between theory and practice. Through the research, the risks highlighted by authors were compared with the actual risks of concern to those organisations outsourcing or seeking to outsource. Many scholars have highlighted their perceived risks associated with outsourcing, yet, until this research, few studies have described how the ERM practices of organisations have been adjusted to safeguard the enterprise against these risks. It is possible that risk management is not more prominent in the literature reviewed because it is difficult to demonstrate how severe the impact of not mitigating these risks could be. By identifying similarities between events in history and the unmitigated actions of enterprises today, this research will make it evident just how
similar today’s problems actually are. By considering the examples from historical texts, organisations will be able to simplify the risk and adopt a strategy to combat the threat without being distracted by the complexity of today’s business world. Considering that the number of organisations outsourcing and offshoring continues to increase as industry grows, this research plays a key role in opening the minds of IT professionals to realise their organisation’s exposure to risk prior to continuing too far down the outsourcing path and potentially reaching a point of no return.

1.5 Chapter Overview

Chapter 1 has provided an introduction to the research problem, detailing the research objectives, research questions, scope and significance of the research conducted.

Chapter 2 examines the literature, identifying the risks highlighted by authors and the gaps in the literature with regard to what is actually being done in practice to mitigate these risks. Frameworks and standards for managing risk are identified, as well as the potential consequences of not adopting risk-management practices, with examples of outsourcing in modern and historical times.

Chapter 3 describes the research methodology and approach, including data-collection processes, sample methods and the sample spread. It also describes the project phases, data-analysis techniques, ethics, quality control and long-term benefits of the research undertaken.

Chapter 4 details the research coverage by describing the types of organisations analysed as part of the research project and their current outsourcing practices. Context for the research is provided and where the research fits into the general risk-management topic is explained.

Chapter 5 discusses the location of outsourcers as a source of risk, identifying the countries outsourced to by Australian firms and the risk these countries pose. The risks that are of genuine concern and the measures that Australian enterprises are putting in
place to mitigate these risks is discussed. Finally, a tool for enterprises to conduct a thorough location assessment prior to outsourcing offshore is presented.

Chapter 6 discusses the outsourcing firm itself as a source of risk, covering impacts to intellectual property (IP), the potential for an enterprise to become dependent on its outsourcing firm and how this impacted ancient empires. The link between intellectual property loss and competitive advantage is established, leading to competitive mitosis, a new concept describing the damage to competitive advantage as a result of the loss of IP. Guidance for how enterprises can identify and mitigate competitive mitosis is provided.

Chapter 7 further expands on the risks associated with outsourcing and their consequences by introducing supply-chain detriment, a new concept that highlights the influence that the supply chain can have on increasing risk levels and reducing visibility and control, thereby exacerbating the risks highlighted in previous chapters and increasing the likelihood that competitive mitosis will occur. Guidance for how enterprises can identify and mitigate supply-chain detriment is provided in this chapter.

Chapter 8 describes barbarian syndrome, a new concept that brings together the self-inflicted accumulation of unmitigated risks covered in previous chapters, including dependency on outsourcing firms and loss of IP through competitive mitosis. This is worsened by supply-chain detriment, which can threaten the prosperity of an enterprise. This chapter describes how an enterprise can identify barbarian syndrome, summarises strategies available to mitigate the condition and provides a modern example.

Chapter 9 expands on the findings to provide a prediction on where the outsourcing industry is going, as this pertains to the potential for future research and may influence risk-mitigation activities employed by enterprises to combat the risks highlighted throughout the thesis.

Chapter 10 recaps the research conducted, summarises the findings throughout the thesis, draws conclusions and describes the potential for future research.
2. Literature Review

2.1 Introduction to the Literature

This research involved a study of IT professionals with the intention of gauging current outsourcing, offshoring and ERM practices. As literature on these topics was reviewed and concatenated, the researcher was led back in time to Ancient Greece and Rome. Although there are only a few reliable source documents, the overwhelming preponderance of information indicated that outsourcing, particularly of military forces and tax collection, was prevalent in antiquity. This outsourcing continued into the Middle Ages and into more modern times. Potgieter and Liebenberg (2012, p127) note that in the 18th century Prussia “relied heavily on foreign mercenaries in order to lessen the impact on its own labour and economy”. The rediscovery of evidence from the ancient past demonstrates that risk management and outsourcing are actually much older problems than once thought.

There are trends that indicate many organisations may not be entirely satisfied with their decisions to outsource. According to Cox (2007, p255):

> Companies that embraced outsourcing early were not always happy with the results. This was predominately because their objectives and reasons for outsourcing were often ill thought-out or reactive.

ERM best practices allow an enterprise to incorporate risk-management rigor into their decision to outsource, minimising the potential for failure. Yet in the early days of outsourcing, many companies took a “piecemeal approach to their sourcing decisions”:

> Business units outsourced on their own back, without considering the wider business. Management took decisions based on local requirements, often division by division. (Cox, 2007, p255)

ERM can assist in preventing such a piecemeal approach by providing a mechanism for an enterprise to manage its risks holistically. Investing time to incorporate such major decisions into the organisation’s ERM framework will aid the firm in ensuring the
outsourcing engagement is the right decision in the first place. Yet it appears this may not be the case in practice with many organisations having cancelled their outsourcing engagements. For example, “Schrodes cancelled its outsourcing deal, and JPMorgan Chase also cancelled its IBM outsourcing contract” (Cox, 2007, p255). Considering organisations establish outsourcing engagements for the primary purpose of cost reduction, the cost associated with establishing and then breaking the partnership with an outsourcing firm should be managed with ERM practices in mind.

2.2 Risk Management and Outsourcing
Outsourcing presents a logical choice when an enterprise simply does not have a particular expertise, and has no appetite for investing time and effort into developing this expertise (Noe et al., 2010, p205). Whilst outsourcing can be beneficial to an organisation’s bottom line, there are dangers in pursuing an outsourcing model, dangers that have plagued civilizations since ancient times. Utilising outsourcing models for military purposes has been particularly common.

Private military forces are as old as warfare itself. The ancient Chinese, Greek, and Roman armies employed large numbers of mercenaries, and mercenaries comprised about half of William the Conqueror’s army in the eleventh century. During the fourteenth century, Italian city-states contracted private military forces, known as condottieri, to protect themselves—an early acknowledgement that hiring mercenaries can often prove more cost-effective than maintaining standing armies. (Shearer, 1998, p69)

The organisations of today also utilise outsourcing as a cost-effective way of maintaining a larger workforce; therefore one should expect that the enterprises of today could be just as susceptible to the risks of outsourcing as their ancient counterparts.

Bolman and Deal, arguably two of the most influential authors on organisational change, highlight the dilemma of the modern enterprise brought about by global competition, turbulence and rapid change. They ask: “Is it better to be lean and mean
or to invest in people?” (Bolman & Deal, 2008, p137). Yet, for those that opt for “lean and mean” there are few strategies available for organisations to consider if downsizing their workforce. It’s no wonder so many organisations of today are pursuing outsourcing models. As with most phenomena captivating the technology industry, there are copious studies available on the topic of outsourcing, yet this one facet of outsourcing remains largely unaddressed. ERM is core to the successful management of any enterprise; therefore one would expect that any organisational element that has potential to impact greatly on ERM practices should be given serious consideration by all organisations and covered fastidiously by authors in all outsourcing literature. Yet the vast majority of the literature appears to focus primarily on the benefits of outsourcing, with the associated risks receiving considerably less coverage.

The world of outsourcing is experiencing rapid growth, with more and more organisations adopting outsourcing models in a variety of different applications. Siepmann (2013, p7) underscores that, due to competition, margins are paper-thin, which has resulted in outsourcing companies earning their profit through volume. This essentially means that the more outsourcing engagements an outsourcer has, the more profit they earn. Adopting this model creates a challenge for security and privacy, which results in outsourcers managing compliance through Service-level Agreements and not risk management. Siepmann’s views are potentially groundbreaking in that they raise the concern that the competition in the outsourcing industry is placing pressure on outsourcers, which impedes risk management. Adopting an outsourced service can be considered as extending an organisation’s operations, because the outsourced function serves as an extension of the organisation’s capability and vulnerability. For this reason, when organisations adopt an outsourced service they in effect extend the enterprise’s exposure to risk. But do the organisations that are adopting these new outsourced services understand that they are extending their business to an industry based on a model that, by its nature, according to Siepmann, impedes risk management?

Siepmann continues to expose the flaws in the fundamental principles of outsourcing. Outsourcing can involve the adopting of a cloud or multi-tenant service, the
engagement of another organisation to provide a managed service or, in its simplest form, purely outsourcing a workforce. Regardless of the underlying service and technology, outsourcing by its nature involves the extension of business operations from one entity to another, so as to take advantage of financial benefits. As the key objective of outsourcing is to lower costs, most outsourcing engagements involve the farming out of people or services to cheaper parts of the globe. However, Siepmann stresses the potential for these economically more attractive parts of the globe to increase exposure to risk:

You would not put your operation at risk by putting it in an area that is prone to hurricanes, earthquakes, or other natural disasters. Unfortunately, some of the top outsourcing countries are known for some of the biggest disasters in history. From a continuity of operations perspective, this is a critical risk area. (Siepmann, 2013, p8)

It is clear that outsourcing any aspect of an enterprise to a region that has greater threat could increase exposure to risk; yet unfortunately few studies describe how this changes ERM practices.

According to Hampton (2014, p17):

Enterprise risk management or ERM emerged in the late 1980s as an extension of hazard risk management. It argues that an organisation should manage enterprise risks in a single, comprehensive program and coordinate ERM with hazard risk management, internal control processes, internal audit, and compliance.

An enterprise should utilise ERM to predict and manage its risks; however, some outcomes are not predictable. Hubbard (2009, p147) points out that:

There exist extraordinary events that no model could have predicted. The events of September 11, 2001, the unexpected rise of Google, major stock market crashes, and various engineering disasters, are cited as evidence for this point.
The fact that some risks are not predictable should not discourage an enterprise from adopting ERM best practices, as there remain many decisions that can benefit from leveraging risk-management practices. For instance, Taiwan is prone to earthquakes; therefore, any decision to outsource to this nation should have some sort of mitigation or contingency in place.

The 1999 Taiwan earthquake caused shortages both in dynamic random access memory (DRAM) and microprocessors that affected many firms, including Dell and Apple. In response, Apple chose to ship pre-ordered computers with a less powerful chip without lowering prices, which led to many complaints and order cancellations. (Gurnani & Mehrotra, 2012, p37)

Could Apple have been more prepared considering Taiwan's history of earthquake activity? Could having mitigations in place have prevented Apple customers from cancelling orders, which resulted in loss of market share?

Likewise, Thailand is prone to floods; yet many enterprises outsource operations there.

The 2011 flood in Thailand created major global supply chain disruptions in the automotive industry (due to a shortage of parts) and the computer industry (due to a shortage of hard disks). The World Bank estimated 1.5 trillion baht (US$50 billion) in economic damages and losses due to the 2011 flood in Thailand. (Soyka, Palevich & Leon, 2013, p1201)

ERM practices can assist an organisation in managing such threats, not only to minimise the likelihood and impact, but to feed into business decision-making to reduce exposure altogether. As the historian Santayana said, “those who cannot learn from the past are condemned to repeat it” (McCormick, 2009, p173).

Natural disasters are not the only threats that an organisation can be exposed to in outsourcing parts of its business. The geographical location also may raise considerations for medical care. Most of the outsourcing of software development is to China, India and Russia (Carmel & Tjia, 2005, p79). Yet the quality of medical care in
India can vary considerably depending on the area (Siepmann, 2013, p13) and this can lead to varying levels of enterprise risk. The region that a business outsources to should influence the ERM practices of the organisation. If an organisation is to manage its risk successfully, careful consideration must be given to the location of the outsourcing organisation in order to ensure the level of risk is aligned with both the risk appetite of the organisation and its risk-management practices.

There are many frameworks and standards that can be utilised by an organisation for risk management, such as Six Sigma:

Like operational risk management, Six Sigma is not new. The discipline is an outgrowth of quality management programs that have gone before it. (Hoffman, 2002, p65)

Although Six Sigma was originally a quality improvement framework, it is still utilised as a framework for managing risk today. Hoffman (2002, p65) explains that “The term Six Sigma refers to its primary objective: striving for virtual perfection in meeting customer requirements”. It involves the adopting of processes to improve quality and minimise waste, both of which cannot be achieved without consideration for the management of risk. The RIMS Risk Maturity Model for ERM is a methodology based upon assessment of seven key factors:

A ‘maturity level’ score is determined for each factor, with the overall ERM level of maturity being signified by the weakest attribute. (Young & Coleman, 2010, p183)

The seven key factors are culture, process, risk appetite, root-cause analysis, risk identification, and assessment, performance management, and business resiliency and sustainability (Young & Coleman, 2010, p183). The COSO framework (Committee of Sponsoring Organisations of the Treadway Commission) was developed out of a “need for a widely-accepted risk management framework” following a loss of public confidence due to the tremendous losses resulting from high-profile events such as the Enron scandal and the September 11 attacks in 2001 (Young & Coleman, 2010, p178).
The COSO framework seeks to establish a common language for risk and definition as well as providing guidance and direction to evaluate risk by focusing on ERM philosophy and risk appetite, and by developing a portfolio view of risk (Young & Coleman, 2010, p178). Further detail on these methodologies and their adoption by Australian organisations in practice is covered in a subsequent section titled “Enterprise Risk Management”.

Ho and Atkins (2009, p35) suggest that outsourcing can lead to improved risk management. They advise that: “outsourcing allows companies to exploit the resources and expertise of specialists, thus resulting in better risk management compared to internal handling”. They go on to address some of the more business-related risks of outsourcing, suggesting that there is potential for an organisation to lose competencies by transferring human resources and internal expertise to an outsourcer. They also highlight the potential for an enterprise to develop dependence on external service providers. Therefore as organisations outsource skills and services to external organisations to reduce costs and improve their organisation, they may actually be introducing new threats that must be addressed through their ERM practices.

When organisations utilise outsourced technologies such as cloud services, they expose their organisation to potential risks that can eventuate from the outsourcing provider. For example:

Target announced that a trusted third-party heating and air-conditioning contractor was responsible for the biggest data breach in its history. In this insider incident, 40 million customer credit and debit card numbers were breached, along with 70 million records containing names, addresses, email addresses and phone numbers of Target shoppers. This breach is still under federal investigation, and Target is now dealing with lawsuits put forward by affected banks and credit unions. (Preimesberger, 2014)

Harvard Business Review reported that this breach “tarnished the company’s reputation, caused its profits to plunge, and cost its CEO and CIO their jobs” (Upton & Creese,
Many authors have also described anonymous examples of such breaches occurring. Claycomb and Nicoll (2012) give this example:

The insider was employed as a system administrator at a data-mining firm contracted by a victim organization to process customer information. Though unnecessary for the job function, the insider had access to servers and data owned by the victim organization. An unprotected file containing encrypted password information was found on one of these servers. The insider brute-force attacked over 300 passwords, accessed data belonging to dozens of the victim organization’s customers, and downloaded millions of personal records. Fortunately, the information was never sold or released by the insider prior to arrest.

It’s likely that many such breaches actually go unreported, as many firms may prefer not to publicise their breach, while others may not even be aware that a security breach has occurred.

Ho and Atkins (2009, p35), in addition to Lynch (2008, p44), emphasise the potential impact that outsourcing can have on quality. Although there is potential for quality reduction when subcontracting any component of a business to a cheaper source, exactly how organisations address the threat of quality degradation in their ERM practices remains largely undocumented with the exception of these few scholars. It would be prudent to suggest that any risk-averse organisation using an outsourcing model would have some modifications to their risk-management practices to ensure quality-related risk is monitored and addressed. Whether real enterprises currently identify quality as a major risk associated with outsourcing and offshoring forms a key part of this research.
2.3 Third-World Problems for First-World Countries

Lynch (2008, p43) states that:

... unfortunately, advanced risk management practices are too often not a prerequisite in the decision to offshore or outsource labour. The reason for this is clear; companies operating in emerging economies often lack the experience, time, capital, and resources to effectively manage risk.

Lynch also seeks to identify the most critical risks associated with an enterprise outsourcing. These critical risks include a lack of adequate public records to allow effective worker background checks on employees, language interpretation issues, inadequate public infrastructure, quality issues, as well as regulatory and legal issues related to foreign data access (Lynch, 2008, p44). So, with all this potential to threaten the continuity of a business, why are organisations continuing to pursue outsourcing options?

Linstead, Fulop and Lilley (2004) put the rise in outsourcing of business operations to countries like India for routine and repetitive tasks down to significantly lower labour costs, overheads and regulations than many Western countries. They suggest that this is because these business functions can be so easily handled remotely via the Internet (Linstead, Fulop & Lilley, 2004, p773). Turban and Volonino (2011) are also concerned about the risks associated with outsourcing. They suggest that the outsourcing trend may be much more widespread when it comes to IT services and they advise that: “about one-third of Fortune 500 companies outsource software development to companies in India” (Turban & Volonino, 2011, p382). Due to their success and potential, one would expect Fortune 500 companies to be at the forefront of ERM; yet what they perceive as threats and the practices they have adopted to mitigate these risks evade the literature.

In outsourcing to countries like India, third-world issues such as rabies and tuberculosis can be just as significant a threat to the organisation’s prosperity as the risk of natural disasters such as cyclones. These are risks that may not have threatened
a first-world organisation prior to moving business functions offshore. Worse yet, the risk of other socioeconomic and political factors such as crime and terrorism demand careful consideration in developing an organisation’s risk-management plan. Outsourcing a component of a business cannot be considered outsourcing the problem because when a function is outsourced to another entity, the exposure to risk is now managed by someone else. When an enterprise outsources it effectively inherits new risks, relinquishing control of these threats, which results in it being more difficult for the organisation to identify, monitor, manage and mitigate offshore risk. It is imperative that organisations consider their risk-management practices when outsourcing, as out of sight should not be out of mind.

2.4 The Barbarians
In his text titled *At Your Own Risk*, Lynch describes six business mega-changes that have significantly altered organisations’ risk profiles. These changes have spurred economic and social benefits, but Lynch warns they also pose a considerable long-term risk (Lynch, 2008, p35). One of these risk mega-changes that is responsible for changing an organisation’s risk profile is outsourcing and offshoring labour. He advises that the outsourcing to offshore locations such as India, China and the former Soviet Union in order to take advantage of a less expensive labour pool and favourable tax structures has actually doubled the world supply of workers from 1.5 billion to 3 billion people (Lynch, 2008, p42). Nonetheless this is not the first time in history a demand for outsourcing has seen a labour pool experience such rapid expansion – this was also the case with the barbarians.

The term *barbarian* was first used by the Ancient Greeks to describe anyone that did not have Greek ancestry. As the Ancient Greeks were moulding modern civilization, they considered these people to be uncivilised, in comparison to Greek standards. But the Ancient Greeks also recognised these outsiders for their potential as a pool of prospective resources. In the ancient world, the number of barbarians grew to be numerous and were utilised by ancient empires as mercenaries to supplement their
existing armies. Griffith (1935) recounts the evident reasons for the rapid growth of barbarian mercenaries. That is, barbarian nations were more numerous, easier to recruit and, most importantly, cheaper soldiers to fund (Griffith, 1935, p79). This bears a striking similarity to the pools of outsourcing resources available today, which are vast in comparison to local resources and, most notably, considerably cheaper.

2.5 History Repeating

Compared with onshore outsourcing, evidence suggests that offshore outsourcing can provide a firm with greater cost saving and higher performance whilst exposing a firm to greater risk of losing control of processes and information (Wilkinson & Kannan, 2013, p127). If the driver to outsource is cost and an enterprise pursuing an outsourcing arrangement places their organisation at greater risk, then how much danger is an organisation placed in as a result of outsourcing? Furthermore, how much of an impact can offshoring have on a firm? Although offshore service providers can often leverage lower costs than onshore providers and thus generate greater savings, the distance between the onshore party and its offshore partner makes the management of the outsourced activity inherently difficult (Wilkinson & Kannan, 2013, p127). If the organisation is now at increased risk and, by virtue of outsourcing a reduction in control established, the increase in risk and the lack of ability to address it is likely to be a recipe for disaster.

Resourcing for military purposes was not the only function outsourced by ancient empires. Rather than harvesting their own, the Ancient Greeks preferred to import their cotton from Persia (Townsend, 2005, p4). Much as modern enterprises do today, the Greeks would also strategically outsource to different nations based on their particular requirements and cost factors. They found that “it was cheaper to transport grain by sea from Egypt and Africa than overland from southern Italy” (Adkins & Adkins, 2004, p195). This suggests that economic reasons also played a part in formulating outsourcing strategies in ancient times.
In addition to their regular army, under the Ptolemaic dynasty, the Egyptians employed Greek, Macedonian and other mercenary troops on a large scale. Mercenary troops were recruited through businessmen acting as brokers fulfilling a business requirement (Bevan, 1927, p.168). Ancient Greeks also outsourced work to temporary contractors based on demand for projects. Fine (1985, p.431) provides details on how such projects were responsible for generating a demand for temporary labour:

From the middle of the fifth century, Athens, under the leadership of Pericles, was engaged in a large building program, a project which, as Plutarch emphasizes, gave employment to a wide variety of craftsmen and labourers. Athenians, whose passion for independence abhorred the condition of being permanently under the restraint of another, worked intermittently on many of these enterprises as contractors, artisans and labourers.

With the high demand for resourcing and the desire to reduce costs, could the outsourcers in antiquity have been conscious of the risks associated with outsourcing? In the late Middle Ages, the Italian historian, politician and philosopher Niccolo Machiavelli was clearly conscious of the relationship between risk and reward when he stated: “never was anything great achieved without danger” (Seka, 2014, p.35). If outsourcing is not a new phenomenon, is there more to learn from our distant past on the dangers of outsourcing? And, most importantly, could the risks inherent from outsourcing cause a company of today to unravel like a former ancient empire?
Exhibited at: Gods, Myths and Mortals: Greek Treasures Across The Millennia, Hellenic Museum Victoria, 6 June 2015
3. Research Methodology

3.1 Research Question Design

The proposed research was aimed at addressing a gap currently in the literature concerning organisational risk-management practices when outsourcing. The primary focus was on extracting detail on the practices currently in place in organisations that apply an outsourcing model. The intention was to identify the ERM practices so as to further improve the knowledge surrounding outsourcing in the technology industry. As the outsourcing of people and services is experiencing significant growth, organisations in first-world countries such as Australia will be more and more likely to consider outsourcing to developing countries such as India, China and African nations, either through directly offshoring resource pools or through outsourcing providers, as a means of lowering the costs of doing business. Greater information on how organisations in practice are managing the risks associated with outsourcing is vital to business success as first-world organisations continue to outsource to other parts of the globe, in most cases first-world organisations inheriting third-world risks.

As part of the literature review, the research question was formulated as it became evident that little literature on organisational risk-management practices when outsourcing was available. It was obvious in the literature that the risks associated with outsourcing were many, but insight into the real world was necessary. This led to the development of the primary research question: What are the impacts of outsourcing on enterprise risk management practices in the technology sector? The research question was focussed primarily on discovery – that is, to understand the difference between the literature and applied practice. In addition, common themes in the literature were identified and interrogated as to their perceived significance to real businesses. Based on this, the sub-questions were formulated to provide further insight into organisational practices and further context to support the primary research question.

Although the literature review sought to conduct a critical assessment of the literature on offer, a systematic review was also used as a mechanism to “help to identify gaps in
knowledge” (Jesson, Matheson & Lacey, 2011, p15). As gaps were identified, the researcher used these gaps to formulate the research sub-questions – five distinct questions that would assist in gaining further context to the primary research question as well as building the foundation for the remainder of the study, which was validated through the case study method.

3.2 Research Framework

3.2.1 Research Approach

The research method selected was a mixed methods approach using a combination of qualitative and quantitative techniques. Creswell (2009, p203) explains the popularity of this method thus:

With the development and perceived legitimacy of both qualitative and quantitative research in the social and human sciences, mixed methods research, employing the combination of quantitative and qualitative approaches, has gained popularity. This popularity is because research methodology continues to evolve and develop, and mixed methods is another step forward, utilising the strengths of both qualitative and quantitative research.

The research primarily revolved around the study of people (IT professionals) and their risk-management practices. A survey was conducted as a way of obtaining insight into the practices of enterprises. The survey used a sample of the population to generalise attitudes and trends that could then be utilised throughout the research and associated case study. A cross-sectional survey was conducted which allowed for the collection of data in one stage and the survey was self-administered so as to reduce any likelihood of bias and allow for a large number of participants to be surveyed across multiple locations throughout Australia and New Zealand. The literature was utilised extensively in order to identify the key areas for survey questioning, as validating the theories and claims highlighted in the literature formed a significant part of the research project. The data collected from the survey was collated and analysed to provide statistical information for measuring organisational practices and then supplemented with
additional literature. As the survey statistical data were analysed, linkages between the typical risk-management literature, enterprise practices identified from the survey and additional literature from history were established through qualitative content analysis. Developing these linkages formed an important part of the research as they provided historical information to gain an insight into the potential impact of Australia’s organisational practices with regard to outsourcing.

3.2.2 Case Study Research

Gillham (2010, p3) argues that: “scientific evidence is, in a sense, manufactured. It is an outcome of the investigative methods used: it didn’t exist before”. In the final stage of this research, the case study method was applied because it:

… seeks a range of different kinds of evidence, evidence which is there in the case setting, and which has to be abstracted and collated to get the best possible answers to the research questions. (Gillham, 2010, p1)

Dubé and Paré (2003, p609) suggest that when using the case design approach, a single case could be selected if specific conditions needed to be met for the testing of the theory. Using the case study approach in this study allowed the primary findings of the research to be validated, and provided evidence that barbarian syndrome is more than just a theory; it actually exists in practice. Although the theories that constitute barbarian syndrome were devised using quantitative data from the surveys conducted and the analysis of literature on Ancient Rome, the case study was crucial to relating this theory back to enterprises in practice today and validating the concept. Dubé and Paré (2003, p624) advise that:

… in order to increase the reliability and internal validity of their findings, case study researchers must provide the external observer with sufficient relevant information so s/he can follow the derivation of any evidence from initial questions to ultimate conclusions and vice-versa.
This was achieved by relating the literature used for the case study back to the barbarian syndrome theory. The case study process commenced through the systematic review of literature available on defunct companies in order to determine if any demonstrated the traits described in the barbarian syndrome theory. The traits of barbarian syndrome described in detail in Chapter 8 formed the selection criteria for the case study, and the examples of defunct companies in the literature were assessed for the potential influence that outsourcing might have had on their demise. The review of the literature concluded with the selection of a case: Swissair.

The Swissair case study provided in section 8.11 Barbarian Syndrome – A Modern Example, was selected to demonstrate the theory in practice by mapping the literature on the case to the traits of barbarian syndrome. Dubé and Paré (2003, p625) stress the need for quotes to be presented so that an external observer can reach an independent judgement regarding the merits of the analysis. Primarily, two sources were used to conduct this case study on Swissair: *Greed and Corporate Failure* by Hamilton and Micklethwait (2006) and *Risk Management and Corporate Governance* published by the Organisation for Economic Co-operation and Development (OECD, 2014). These sources acted like a post-mortem of the now defunct company, putting the theory of barbarian syndrome to the test.

### 3.3 Data Collection

#### 3.3.1 Data-Collection Procedure

The survey, administered through Survey Monkey, was the primary instrument used to capture the required data. The comprehensive survey consisted of a questionnaire that had been formulated in a manner that ensured that all targeted outcomes were addressed, and all survey questions mapped back to, or provided additional context to, the research questions. The participants in the research were able to view the survey questions and submit their responses into the form using any web browser. The survey invitation was distributed to participants via email. The data-collection process commenced with approval from the Charles Sturt University’s Research Ethics
Committee. It took place over six months, with the response rate monitored to ensure the targeted number of respondents was achieved.

### 3.3.2 Survey Design

The Chief Investigator of this research study administered the surveys via the Survey Monkey tool. The survey method was selected to maintain consistent questioning across all participants. The survey was distributed and responses self-completed by research participants. The responses captured were collated and entered into a spreadsheet for statistical analysis, which took place once all survey responses were collated. The survey questionnaire was designed in a streamlined fashion to allow for easy execution of the research with the intention of minimising the amount of time and effort required by participants. As participants were experienced IT professionals, likely in high-profile senior roles, the intention was to minimise the total overhead of participation, which ensured that participants were not burdened by their involvement whilst encouraging the most number of participants to respond.

The aim of this study was to analyse the enterprise through the opinion of individuals. Therefore, the selection process was tailored to ensure that the participants were in the correct role within their respective organisation to accurately respond on behalf of their enterprise. The participants selected were primarily in senior management, architectural, business analysis, service delivery and project-management roles within the IT industry. The sample group was selected using homogeneous sampling. The method and process for selection has been provided in further detail in section 3.4 – Research Sampling Method.

The survey included all the questions required to capture the required data to answer the research questions. The questions included in the survey were selected on the basis that they would provide the most suitable data for formulating findings that would address the gaps in the literature. As the intention of the study was to leverage the data collected to guide the analysis, additional data were collected through the survey to provide further context to the results and assist in conducting the statistical analysis.
and correlation. For instance, survey participants were asked what countries they outsource to. Participants were also asked whether they were concerned about intellectual property theft when outsourcing. This information was then fed into the statistical analysis to determine if those that outsource to China, for instance, are more likely to have concerns about intellectual property theft. Further details on this analysis have been included in section 3.6 – Statistical Analysis.

### 3.3.3 Survey Instrument

Survey Monkey was chosen as the primary survey instrument because of its ease of use and easy access. Questions were short, clear and concise in order to minimise the effort required from the participants. Most responses involved the ticking of boxes and selecting the responses that applied to the individual’s organisation. This allowed for streamlined questioning and minimised the overall time required by the participants to partake in the research. Survey questions were formulated across the following areas:

- Participant’s job title
- General questions for company profiling including sector, employee size, geographical location and so forth
- Countries outsourced to
- Types of services outsourced, such as managed services, fixed deliverables, outsourced technology (e.g. IaaS, SaaS) or workforce labour
- Business risks that are of concern when outsourcing, such as natural disasters, economic stability, crime, terrorism and so forth
- Areas that firms should address such as ERM practices, dependency on outsourcing firms and mitigation strategies

The purpose of the survey was to capture data from organisations so as to determine their perceived threats in comparison to the threats detailed in the literature. This would allow the research to highlight the gap between the risks documented and the
mitigating actions taken in the real world. The survey was not intended to identify and address all the potential risks associated with outsourcing and offshoring, as the number of locations outsourced to is large and each location comes with its own potential risks and permutations of risk. The focus of this survey was on the practices (or lack of practices) adopted by enterprises to mitigate risks and not the individual risks themselves, as defined in the research questions and sub-questions.

3.4 Research Sampling Method

The sample group was selected using homogeneous sampling, a purposive sampling technique used to identify a sample group with similar traits. According to Baran and Jones (2016, p118):

> A homogenous sample is often chosen when the research question that is being addressed is specific to the characteristics of the particular group of interest, which is subsequently examined in detail.

The objective of this research was to capture and analyse the impacts of outsourcing on risk management for enterprises. In order to achieve this, the sample group was required to consist of senior, decision-making and influential personnel.

To form the sample group, two main criteria were required to be met for selection. Firstly, all participants were required to have worked in the IT industry in Australia or New Zealand. Secondly, all participants were required to be employed in senior roles, so as to ensure they were high enough within their organisation’s hierarchy to observe and understand the organisation’s risk-management practices, risk appetite, and stance towards IP risks. Whilst those taking part in the study did not have to be decision-makers, they did have to be senior enough within their respective companies to be familiar with the risk strategy and its implementation in practice.

Participants were selected from diverse backgrounds and were employed in organisations from various different sectors. Suitable candidates were profiled in order to assess suitability against the aforementioned selection criteria, and to ensure the
sample group consisted of a sufficient spread of traits to simulate the population as closely as possible. The initial targeted sample size for this research project comprised of one hundred (100) participants. As research participation was optional, participants were provided with an opportunity to opt-in to complete the survey. This resulted in some participants choosing to not partake in the research; nonetheless, the target was exceeded and the final number of respondents was one hundred and two (102) in total.

3.5 Research Sample Spread

The profiles of the selected research participants helped execute the inductive data analysis. The profiles have been outlined below:

- Industry – all participants are IT professionals
- Seniority – all participants are in senior, non-entry-level roles
- Experience – all participants have a number of years of experience in the industry
- Roles – participants are primarily in Architectural, Project Management, IT Management and Service Delivery roles

Greater information on the participants’ roles, as well as the size and sector of the organisations they were currently employed in, was obtained through the first section of the survey. These results have been detailed in Chapter 4.

3.6 Statistical Analysis

The data-collection process involved capturing information through the survey for offline analysis. At the completion of the data collection, responses were collated for the data-analysis process to be executed. The analysis of data was completed using Microsoft Excel. The research questions and objectives were mapped back to the survey question results to quickly and easily identify solutions to the gaps in the current literature. Detailed analysis was undertaken to calculate the metrics that formulate the findings, as the aim of the research was to identify opinions and trends in the industry.
as well as any linkages, patterns and commonalities between traits of the different organisations studied.

Conducting the survey via email brought to this research a level of validation of results that helped identify trends without bias. The answers to survey questions were captured and submitted by the participants through the self-administered survey, thereby minimising the likelihood of misinterpretation of responses. This allowed the researcher to easily and unbiasedly develop the outputs required to present and communicate the findings of the research, in addition to ensuring that the research achieved its purpose – namely, to improve industry knowledge on ERM when outsourcing.

The results of the statistical analysis have been detailed in chapters 4 and 5, where the measurements of how significant the risks are have been provided using quantitative data from the survey results. The statistical analysis also assisted in the correlation of results and the influences that various factors may have on the findings. For instance, the survey was able to ascertain how many participants believed their organisation had a high tolerance for risk. Using statistical analysis the research was then able to conclude, for example, that those that outsource to China are more likely to have a high tolerance for risk in comparison to those that outsource to Malaysia. This analysis formed a critical element in understanding the multiple dimensions of the issues raised in this research as well as guiding the investigation, which led to the discovery of the new theories detailed in chapters 6, 7 and 8.

3.7 Ethical Considerations
Some of the potential ethical issues identified are outlined in Table 3.1 below. Controls were implemented to ensure that the risk of ethical issues had limited impact on the research project. Ethical issues were addressed as part of the planning phase and controls and mitigations were implemented throughout the course of the research project. All potential ethical issues were addressed as part of the Charles Sturt University ethics application and approval process.
Table 3.1 – Potential Ethical Issues

<table>
<thead>
<tr>
<th>Potential Issue</th>
<th>Potential Impact</th>
<th>Control and Mitigation</th>
</tr>
</thead>
</table>
| Effort of participants          | Participants may have concerns regarding the amount of time involved in partaking in the research project. | 1) Ensured that all questioning was short and concise.  
2) Ensured that all participants understood that they could opt-out of the research at any time. |
| Identity of the research participants | Research participants may have concerns about being named in the thesis and/or having their responses published. | 1) The information sheet accompanying the survey questionnaire reiterated that participation in this research was optional and that anonymity was maintained at all times.  
2) All participants’ names were omitted from the survey data collected and the findings detailed in this thesis. |
| Intellectual property           | Individuals or organisations may make claims of intellectual property ownership for any output of the research conducted due to their contribution. | 1) The information sheet accompanying the survey advised all participants that the aim of the thesis was to publish overall trends, not the responses of individuals.  
2) Any potential contributions to the research other than through responses to the survey questionnaire were not permitted. |
| Investigation bias              | The investigation could be influenced by bias when using techniques that require interpretation of responses (e.g. interviews). | 1) The survey approach was utilised to provide transparency in the process of analysing data and formulating findings.  
2) All participants were required to complete the exact same survey with the same questions responded to by all participants, ensuring consistent questioning. |

3.8 Data Quality and Control

As quality of data was critical to the formulation of sound findings, controls were implemented to ensure high standards were maintained. The controls established throughout this research project are as follows:

**Data Relevancy** — Data were obtained directly from the source, alleviating the requirement for any unnecessary extraction, translation and loading of the data prior to analysis. The data collected were exported from the survey database only once, diminishing the potential for errors. The survey was also administered through a self-service function, limiting the potential for inaccurate data caused by manual data entry.
Data Not Skewed — Although the research was centred on outsourcing and offshoring, those selected to take part in the study were selected regardless of whether their enterprise had adopted an outsourcing model. This ensured that the data collected were not skewed towards those that outsource. Some participants (22%) advised they did not currently outsource, and data collected from these individuals provided insight into their organisation’s size, risk appetite, risk methodologies and frameworks.

Data Accuracy — The vast majority of questioning administered throughout the survey was multiple choice and tick-box selection to prevent any requirement to interpret results. The data collected were reviewed for accuracy by inspecting the responses of those that took part in the study for inconsistencies. All responses were found to be consistent and there was no evidence of erroneous or inconsistent answers to questions.

Data Validity — To ensure the data collected were valid, all questioning was linked back to the literature, gaps identified and the research questions to provide the researcher with traceability of data back to the requirements and objectives of the study.

3.9 Long-term Research Benefits

It was envisaged that organisations would benefit long term from the findings of this research project. The findings will assist organisations by improving their knowledge and understanding of how the risks of outsourcing can affect an organisation. This will pave the way for organisations to learn from the risks realised by the other organisations before them, allowing the industry to grow and further develop. Further development of the industry will be possible now that the perceived risks associated with pursuing an outsourcing engagement have been captured, shared and understood. This allows an organisation to consider these risks in their decision to adopt an outsourcing model. Through the findings of this research, the impact discovery can be completed to determine how significant and widespread the overlooking of ERM practices when outsourcing in the technology sector actually is. This research project
may be responsible for producing the first documented ERM analysis of organisations in practice, which will be paramount to organisations understanding and mitigating the business risks associated with outsourcing based on shared knowledge. The findings identified through this research project could be utilised in the future to develop frameworks, standards and guidelines for outsourcing in the technology industry.

3.10 Research Project Phases
The research project was completed through the establishment of the following phases:

- planning
- data collection
- data analysis
- thesis development
- review and closure.

The planning phase sought to develop the foundation for the research, with the initial identification of potential research participants as well as ratification of the university’s ethics application. The data-collection phase involved the execution of the research, commencing with the data collection via the execution of the survey. The data-analysis phase was responsible for identifying, capturing and finalising the research findings for the preparation of, and input into, thesis development. The thesis-development phase was followed by the review-and-closure phase, which involved submission of the thesis for multiple reviews as well as completion of any subsequent activities.
4. Research

4.1 Research Coverage and Size Analysis

The research completed involved the contribution of 102 research participants. As indicated in Figure 4.1 the research was limited to the participation of senior IT professionals. The sample group established included participants across roles consisting of thirty (30) per cent Project Management, twenty-three (23) per cent IT Architecture and forty-six (46) per cent IT Management or Service Delivery.

![Research Participant Roles by Industry](image)

Figure 4.1 – Research Participant Roles by Industry

Figure 4.2 highlights the spread of research participants across industry sectors. In total, fifty-one (51) per cent of participants indicated that they were currently employed in the telecommunications, technology and electronics industry; Twenty-one (21) per cent indicated that their current employer was in the finance and insurance industry; and fewer than nine (9) per cent indicated that they were currently employed in the government and education industry. The construction industry was represented by just under five (5) per cent of participants with real estate and business support
providing four (4) and three (3) per cent respectively. The utilities, energy and extraction industry, as well as the food, beverages and entertainment industry, were indicated by two (2) per cent of participants as their currently employed industry, with retail, health care, airlines and defence industries being represented by one (1) per cent of participants each.

The research conducted specifically targeted IT professionals that reside in Australia and New Zealand to ensure that the current trends in offshoring from the ANZ region were identified. Figure 4.3 portrays the participant spread across locations. A large majority of participants that took place in this research study were located in Sydney, Australia, with over seventy-five (75) per cent of participants currently residing in Sydney. This is likely due to the research requiring experienced IT professionals and Sydney being the primary employer for IT professionals in Australia. Almost thirteen (13) per cent of participants currently reside in Melbourne, almost six (6) per cent in Brisbane and two (2) per cent indicated that they currently reside in the ACT. Almost three (3) per cent of research participants indicated that they currently reside in Auckland, New Zealand. The organisations currently employing the research
participants were also measured in terms of their overall number of employees. Figure 4.4 illustrates that almost fifty-seven (57) per cent of research participants are currently employed in organisations of greater than 5,000 employees. The percentage of participants currently employed by an organisation with between 1,000 and 4,999 employees is fourteen (14) per cent. This indicates that the vast majority of the spread, seventy-one (71) per cent in total, consisted of organisations with greater than 1,000 employees. Twenty-two (22) per cent of participants are currently employed in organisations with more than 100 and fewer than 1,000 employees.

The size of the enterprises represented in this research was captured due to its critical importance in contributing to the overall objectives. Carmel and Tjia (2005, p49), among others, have stressed the importance of the size of the organisation in determining the level of acceptable risk and the degree to which mitigation should take place:

There are differences between large and small firms regarding offshore risks. Strictly speaking, for a large firm, the risk is the mathematical expected value, namely the product of the likelihood and the severity. However, for small firms,
some risks, such as IP risk, can be so severe as to lead to the company’s downfall.

If smaller firms are more susceptible to the impact of risks, the size of an organisation must form a critical part of any sound risk analysis. Carmel and Tija go on to question whether such risks are actually worth the cost savings obtained through offshoring.

![Figure 4.4 – Research Participants by Employer Size](image)

The findings illustrate that the size of an organisation bears a direct relationship to whether it will utilise an outsourcing model. The numbers of participants that outsource are shown in Figure 4.5 below. Based on these data, it has been determined that eighty-nine (89) per cent of participants employed in organisations with greater than 5,000 employees utilise an outsourcing arrangement. Conversely, only sixty-one (61) per cent of participants that are currently employed in an organisation with less than 5,000 employees indicated that they currently outsource. These findings provide justification to the claims of multiple authors that the size of an organisation can have a bearing on its potential to consider offshoring.

Two of the important differences between offshoring and traditional onshore IS outsourcing ... are the importance of the firm size and return on assets in determining the decision to offshore. Larger firms generally have deeper pockets
in terms of greater amount of resources (hence more risk-taking ability), and firms with a higher ROA generally have a better ability to manage risks. (Srivastava, Teo & Mohapatra, 2009, p121)

Figure 4.5 – Organisations That Outsource by Size

4.2 Enterprise Risk Management

Risk management is crucial to the success of any institution and therefore it is no wonder that risk management formed a critical part of the success of the Persians.

The rise of the Persian Empire was based on the acquisition and improvement of territory and ideas from other cultures. The early Achaemenid monarchs were conscious of the risks of opposition to their rule, but had access to huge resources from their military empire to be comfortable in managing any risk. (Slatyer, 2012, p79)

It seems like an eternity since the ancient Persians roamed the world, but even then the importance of managing risk was understood. Just as the Persians were drawing on their resources to aid in their management of risk, the organisations of today should seek to do the same. Adopting an effective risk-management methodology is critical to the success of an enterprise. As pointed out by Borek et al. (2014, p55):

37
Organisations that have adopted risk management methodologies are better placed to ensure that operations are successful and the potential damage from risk is reduced.

It is evident, however, that in practice this is not the case. As portrayed in Figure 4.6, this research has exposed a serious deficiency in the risk-management practices of Australian organisations, with the most recent risk-management methodologies appearing to be experiencing extremely low uptake, based on the survey of Australian IT professionals.

When asked which methodology their employer utilises for risk management, over forty (40) per cent of participants advised that their organisation utilises an internal methodology or framework, rather than one of the generally available and published industry-standard methodologies. Even more alarmingly, over thirty-eight (38) per cent of participants indicated that they were unaware of exactly which methodology their enterprise has adopted, suggesting that these professionals do not play an integral role in understanding and influencing the organisation’s day-to-day risk-management function. According to Borek et al. (2014, p55), “Risk management should be integrated in day-to-day operations and become part of the culture, with everyone in the organisation being responsible for managing risk in their sphere of work”. However, the findings indicate that this is not the case. If risk management were integrated into day-to-day operations and everyone in the organisation was responsible for managing risk, the organisation’s senior employees would have an understanding of which methodology (at a high level) was in place. This suggests two possible causes: 1) the organisation has not made sufficient investment in training its senior employees on how to effectively manage risk, or 2) the organisation does not utilise a risk-management framework at all. These findings indicate a trend within Australian corporations that is concerning. A large portion of enterprises utilise their own internal framework over published methodologies and a significant portion does not actually know what methodology their enterprise is currently using. Based on this, it is possible that up to eighty (80) per cent of Australian enterprises may not be utilising leading,
published, industry-proven, risk-management methodologies to assist their enterprise is governing risk-management practices.

Of the published methodologies, Six Sigma and Lean Six Sigma have received the greatest uptake according to the research. The Six Sigma methodology was originally developed in the 1980s by Motorola for the improvement of product quality (Breyfogle (2003, p5). It went through a number of iterations as it progressed throughout the 1990s with its adoption by global corporations such as General Electric (GE). With over seven (7) per cent of enterprises utilising Six Sigma and over ten (10) per cent utilising Lean Six Sigma, these methodologies appear to be applied in practice more than any other published methodology. Of the newer methodologies, the Risk Maturity Model (RMM) has been adopted by just under three (3) per cent of participants’ organisations. Young & Coleman (2010, p183) advise how this model is used to embed risk-management practices within an organisation:

The Risk Maturity Model for Enterprise Risk Management, developed by the US-based Risk and Insurance Management Society Inc. (RIMS), seeks to determine the extent to which enterprise risk management is embedded within the organisation and is leading to enhanced performance.

Yet such a promising methodology has only been adopted by three (3) per cent of the sample group. The ERM framework produced in 2004 by COSO, which provides internal control methods and risk-management functions (Hopkin, 2014, p62), appears to have also been substantially overlooked over internal custom frameworks and the more archaic Sigma methodology. Research participants were also provided an opportunity to manually add a methodology that was not available in the provided list; however, no participants chose to do so.

The research indicates that many of the risk-management frameworks that have been proposed by COSO and ISACA have failed to be adopted widely by Australian enterprises. As the ISACA’s Risk IT framework complements ISACA’s comprehensive IT governance framework COBIT (Roebuck, 2012, p53), one would have expected that
some enterprises seeking to mitigate risk in their IT estates would have adopted the methodology. Roebuck (2012, p53) advises that Risk IT provide a framework with practices to identify, govern and manage risk in IT environments; therefore, greater adoption should have been witnessed in this study. Overall, the question why Australian organisations would place their operations at risk by focussing on the use of older methodologies and internal frameworks over the new, cutting-edge and IT-focussed methodologies remains unclear.

As mentioned in the preceding section, outsourcing itself is not a new phenomenon. The literature indicates that by the second century BC, rather than toiling itself, Rome would import large quantities of grain from provinces in Sicily and Sardinia, and then later on from Egypt and North Africa (Adkins & Adkins, 2004, p195). Regardless of the motives, this suggests that Rome was actually outsourcing the cultivation of crops to other nations and regions, similar to the way in which we outsource services to offshore locations today. This grain was then subsidised by political leaders and distributed to the people to insure against starvation (Adkins & Adkins, 2004, p195). It is possible that this process may have been an early form of outsourcing and could be regarded as a form of risk management. Outsourcing the growing and cultivation of
grain to other regions helped Rome’s leaders to prevent starvation, mitigating the risk that starvation posed to the empire. With such evidence for the use of outsourcing and risk management in ancient times, one would expect that the enterprises of today would have considerably more investment in the management of risk and the adoption of the most current and effective risk-management methodologies. The findings from the data collected reveal the current trends of risk management in practice. Figure 4.7 depicts the action that organisations take to mitigate risk. Over seventy-two (72) per cent of participants demonstrated that their organisation always takes action to mitigate risk when required. Twenty-five (25) per cent of respondents indicated that their current employer takes action to mitigate risks on some occasions, suggesting that some risks remain un-mitigated. Disturbingly, two (2) per cent of respondents advised that their employer does not take action to mitigate risk at all, which could be placing their organisations in serious danger.

Enterprises can have vastly different risk appetites/tolerances. Some have a low tolerance for risk, mitigating all potential risks where possible; others may have a high tolerance and generally accept larger levels of risk. Figure 4.8 outlines the tolerance for risk depicted in the organisations studied. This has revealed that a large majority,
seventy-seven (77) per cent of participants indicated that their employer has a low appetite for risk. This essentially means that these enterprises prefer not to take large risks and will seek to minimise the probability and impact level wherever possible. In fact twenty-one (21) per cent of individuals that stated that their organisations have a low tolerance for risk also indicated that they do not actually outsource, suggesting that outsourcing requires an enterprise to have a reasonable appetite for taking on risks. On the other hand, over twenty-two (22) per cent of participants stated that their organisation has a high tolerance for risk. This ultimately means that these enterprises have an appetite for risk-taking and may make risky decisions or even allow some risks to remain un-mitigated. Could this lack of risk management be effectively placing an organisation at risk of being beaten by a rival competitor? 

Slatyer (2012, p80) describes how the first Persians (aka Achaemenids) would tour their empire to obtain visibility and exercise control over their vast administration. This is a clear illustration of how visibility and risk management contributed to the success of ancient empires. Touring allowed the Persians to monitor their large empire and mitigate risks as they arose. In later years, their dynasty declined and their failure in risk management allowed their rival, Alexander the Great, to conquer the Persian Empire.

![Figure 4.8 – Organisation’s Risk Tolerance](image-url)
4.3 The Risk Strategy Paradigm

There are four traditional risk-management methods that are key to managing risk within a business context. These are:

- **Avoidance** – Avoid the risk by changing the approach so as to completely bypass the risk. For instance, if there is a concern that a particular service is unstable, the risk may be avoided by selecting a completely different service.

- **Mitigation** – Implement a control or action to minimise the impact, reduce the likelihood of occurrence, or both. For instance, upgrading the service to reduce the likelihood of the risk occurring or reducing the amount of reliance on the service to lessen the impact on the business if it were to occur.

- **Acceptance** – Accept the fact that the risk exists and may occur, and purely monitor the risk for impact.

- **Transference** – Transfer the risk to another entity, thereby making it the responsibility of another party to manage. Using the service stability example, transference may be achieved through outsourcing the service to another entity to manage, or purchasing insurance to cover the potential impact of the risk.

Acceptance involves accepting the risk, and so it can be easily argued that this approach does not warrant an ERM framework; it is purely a reporting function that involves the organisation tracking and monitoring the risk to report on its occurrence. If the organisation opts to allow a risk to go untreated, it is clearly not a significant enough threat for the organisation to concern itself with implementing any treatment and such a scenario results in the organisation monitoring the risk at most. Avoidance is also commonly not a real option in the scenarios that organisational management deal with. If it were that easy to avoid the risk, an enterprise would not be in a position where it is genuinely at risk. Such a simple strategy could be employed long before there is a need for organisational governance, frameworks and collective strategy to combat the threat.
at an executive level. If the organisation is in a position where it can merely avoid the risk, was the organisation at real risk to begin with?

If an insurance policy is purchased as a method of transference, the organisation may be able to minimise the impact of the risk should it eventuate. Transferring the entire ownership of a risk to another party, however, may not always be the safest option. Can transferring a risk to another entity really reduce the impact on the organisation? It may no longer be responsible for managing the risk, but it will likely continue to feel the impact should the risk occur. Transferring risk involves outsourcing the risk to another entity for the purposes of sharing or completely offloading responsibility to another party. But with so many potential threats to an enterprise when outsourcing, is transferring risk really an option? Organisations need to determine for themselves whether they are willing to accept the heightened risk that is incurred as a result of transferring complete responsibility for risk management to an outsourcing firm when in fact there is serious potential to disrupt the business. Although outsourcing to another entity may appear to be the most suitable option on paper, allowing the outsourcer that is introducing the risk to also treat, manage and control the risk may not be the most effective option long term – because the only party with the organisation’s best interests at heart is the organisation itself.

Of these four mainstream approaches to risk management, the only technique that can be seen as genuinely improving an organisation’s risk level is mitigation. Through mitigation an enterprise can successfully minimise impact and likelihood of occurrence. Minimising the likelihood that a threat can eventuate and implementing measures to reduce the impact of the threat maximises the organisation’s defence, thereby safeguarding the enterprise against risk. It is for this reason that the primary focus of this research is on mitigation, the only strategy that can be considered genuinely useful in improving an organisation’s risk position.
4.4 The Strategy of Outsourcing

According to the survey, seventy-seven (77) per cent of organisations currently utilise an outsourced service, with twenty-two (22) per cent indicating that they do not currently outsource. Solli-Saether and Gottschalk (2010, p130) highlight the potential for outsourcing to cause problems if the risks are not managed:

Not all companies benefit from outsourcing, and the disadvantages of outsourcing can create serious problems for organisations if they are not well understood and managed.

Yet outsourcing and offshoring can take place through a multitude of different models and services. Although there is immense literature on the topic of outsourcing, very little delves into the types of outsourced services that are actually being used by Australian organisations.

Through this research, an attempt was made to understand the way in which Australian businesses utilise outsourced and offshore services in order to better understand how the risks that threaten an enterprise are making their way into our organisations. These findings are evident in Figure 4.10, which indicates that seventy-eight (78) per cent of
research participants whose organisations outsource advised that their organisation currently outsources services such as managed-service contracts (which deliver a particular outcome such as an entire function like an IT support contract) and fixed-service deliverables such as software development. Of the participants, six (6) per cent indicated that they are currently considering the adoption of an outsourced managed service. On the other hand, fifty-two (52) per cent of participants indicated that their employer is currently outsourcing technology such as cloud platform, SaaS, IaaS or similar technology; and eighteen (18) per cent of participants suggested that their employer was currently considering the adoption of an outsourced technology, indicating that technology as a service is the most likely type of outsourced solution currently under consideration, and therefore is the most likely type of outsourcing model to grow.

![Outsourced Services Currently Utilised](image)

**Figure 4.10 – Outsourced Services Currently Utilised**

The most traditional type of outsourcing – human resources or workforce labour outsourcing – is utilised by sixty-five (65) per cent of the individuals that participated in the study, but only three (3) per cent of respondents from the remaining organisations advised that their organisation is currently considering the adoption of such a model. This indicates that fewer businesses are considering workforce labour outsourcing over other types of outsourcing models. Overall, the findings indicate that organisations are utilising the managed-services outsourcing model the most, and are
considering the outsourcing of technologies such as SaaS and IaaS over the traditional outsourcing of workforce labour. This provides an interesting thought from a risk-management perspective, as generally speaking workforce labour outsourcing carries the least risk. Outsourcing the workforce allows an enterprise to maintain control over the deliverables without relinquishing complete control to an outsourcer, as is demonstrated through the adoption of a service or technology offering. It is plausible from these data that there is a significant paradigm shift taking place across the industry, whereby many of the enterprises seeking to outsource are actively considering the outsourcing of labour rather than the traditional forms of technology and services outsourcing we have come to expect from the industry.

Alexander the Great, whilst making use of local resources, would often import food and water for his army from great distances (Engels, 1978, p2). Mercenary troops were strategically used to fill a shortage within an army. According to Griffith (1935, p78):

The whole purpose of a mercenary force was that it constituted the permanent and standing army which a rural population could not supply. (Griffith, 1935, p78)

Leveraging the benefits of other nations based on their skills is not a new concept. When there is a need to satisfy a particular requirement or generate a desired outcome we turn to offshore sources for a variety of reasons. However, the location that we seek to obtain the services from is often determined based on the requirement we are seeking to fulfil. Outsourcing requires strategy to obtain the best from each nation, and when particular skills and resources are required to deliver the outcome, we often turn to nations where they are available. In his text from 1927, Bevan highlighted that the use of strategy when outsourcing today was also the case during the Ptolemaic Dynasty, which ruled Egypt circa 300 BC:

For certain kinds of troops, expert in the use of a particular arm, required generally in the warfare of those days, the Ptolemies had regularly to resort to mercenary corps, recruited, in the first instance at any rate, from the peoples
after which they were called – Creten bowmen, Thracians with their large shields and straight double-edged swords (rhomphaiai), Gauls, tall fair-haired men of the North, with long narrow shields and swords of an extraordinary length, dreaded more than any other people as fighters but liable to danger their employer no less than his enemies. (Bevan, 1927, p168)

The Ptolemies employed foreign troops with specialist skills and traits to fulfil their particular need, much the same as we do today. We often see firms outsource specific functions (such as software development) to particular nations where those specialist skills are in abundance. Bevan also refers to the Gauls as being dreaded more than any other people as fighters but posing a danger to their employer as well, indicating that outsourcing posed risk in antiquity, much as the risks associated with outsourced and offshore resources today can impact an enterprise.
5. Outsourcing and Offshoring

5.1 Offshoring

Carmel and Tja (2005, p30) highlight the risk associated with outsourcing revenue-generating processes, such as contact centres, offshore:

Revenue can be lost if customers are frustrated with the offshore service provider. A widely published example is Dell, which decided in 2003 to redirect some customer service calls to helpdesks in the US, rather than to its call centre in Bangalore, India. Dell brought some activities back to the US when it found that several of its business customers complained that Indian technical support workers relied too heavily on scripted answers and could not handle complex computer problems.

If large, global conglomerates such as Dell are reconsidering the offshoring of critical, revenue-generating operations, this may suggest that other enterprises that have rushed into offshoring arrangements may need to revise their risk analysis. Carmel and Tja (2005, p46) advise that:

… once IT operations are in a country, most country risks are not controllable. The risk may be diversified, mitigated, or insured, but it cannot be controlled since in theory, no single country has the power, for example, to stop a war between India and Pakistan.

As it can be difficult to control and mitigate this risk once the engagement has commenced, analysis of risks is required with the commencement of the offshoring plan to ensure the strategy addresses the relevant risks:

Risk assessment needs to take place up-front, before going offshore, but also on an ongoing basis. Many firms conduct some type of country risk assessment before they enter a country. However, it is rare that firms continue to conduct regular assessments once they already have operations in-country. This is a mistake. Companies need to continually assess risks by collecting data from
experts, but particularly from people who are in-country on the ground. (Carmel & Tjia, 2005, p49)

This research has developed a tool, called the Location Assessment Tool, to help organisations conduct this risk assessment and provide further information on the evaluation cycle to ensure the risk assessment remains valid and current – see subsequent sections.

The evaluation of a country to determine the level of risk should form a critical part of any offshoring strategy. Carmel and Tjia (2005, p45) advise of some of the perceived risks that are associated with offshoring:

The consequences of country risk can be severe because they affect, among other things, business continuity – the ability of the firm to continue its core operations. When offshoring, companies are exposed to increased risks of war, terrorism, rioting, uprising, confiscation, expropriation, and currency crises. These are real risks. They do happen. We just do not know how to predict them, especially the big, shocking events.

It is evident from the research conducted that ANZ-based firms outsource to locations that are at risk of some of the threats detailed by Carmel and Tjia. Figure 5.1 below represents the nations the participants indicated that they actively offshore to. The links between these nations and the risks detailed by authors such as Camel and Tjia (2005) have been detailed in subsequent sections below.
5.2 Outsourcing and Offshoring Risk

The number of organisations transitioning services offshore continues to grow. Heath (2014) predicts that by 2016 major companies from the United States and Europe will have transitioned almost 1.1 million IT jobs offshore. Yet organisations can have different reservations when considering an offshore location to outsource to. Analysis of these concerns for ANZ enterprises formed a crucial part of the research conducted. As various authors have raised the risks associated with offshoring, a substantial focus was directed toward determining which risks are genuine concerns of real organisations currently outsourcing business functions. These concerns are detailed in Figure 5.2 below. Despite the obvious evidence that the majority of outsourced-to nations have a greater risk of natural disasters, only eleven (11) per cent of participants whose organisations outsource indicated that they were concerned about natural disasters. This suggests that the participants are either ill-informed regarding the environmental risk of their offshore locations, do not completely understand the probability of a disaster, or believe that the impact will be minimal. A slightly higher percentage, sixteen (16) per cent of participants also advised that they were concerned about the risk of

![Figure 5.1 – Countries Outsourced to from Australia](image-url)
economic instability. Based on the fact that the most cost-effective destinations for offshoring would be third-world or developing nations, this suggests a significant amount of unmitigated risk among ANZ enterprises. If these participants do not have concerns regarding the economic stability of the nation they are outsourcing to, their organisations may not be effectively managing the risk. Some countries such as Ireland, India and China have grown at a considerable rate in recent years and their ability to maintain the current economic climate long term may prove challenging for these nations.

![Offshoring Concerns of Participants](image)

**Figure 5.2 – Offshoring Concerns of Participants**

Healthcare quality and availability of offshore locations has been raised by a number of scholars as a risk to a successful offshoring engagement because it can have an enormous impact on resource health, productivity and life span—all factors that can seriously affect an organisation’s operations. The threat of infectious diseases and a nation’s ability to deal with an epidemic or large-scale medical crisis could have a crippling effect on the most successful of enterprises. Yet only six (6) per cent of individuals surveyed advised they were concerned about the availability or quality of medical care in outsourced-to countries. Likewise, only sixteen (16) per cent of respondents raised concerns about crime and its ability to endanger their offshoring
arrangement. With a number of developing nations currently being outsourced to by Australian firms, it is only logical that crime should be a much larger concern for these enterprises. Criminal activity does not only have a detrimental effect on individual resources; other crimes such as robbery and theft, corruption and embezzlement could cripple an organisation’s entire business operations. Considering Australia has a relatively low crime rate in comparison to the rest of the globe, outsourcing services to a destination with a higher crime rate should be a cause for concern.

An haphazard approach to threat management is also demonstrated in the responses from participants regarding terrorism and political stability, with only nineteen (19) per cent of individuals advising that they had concerns regarding political instability and the potential for social unrest in the nations that currently house their outsourced operations. With the increase in developing nations performing outsourced services, it would be reasonable to expect that Australian organisations would, at the very least, be more concerned about the threat. Similarly, Australia has an extremely low terror rate in comparison with the rest of the world, which means that other nations pose greater risk of terrorist attacks. Nonetheless, only one (1) per cent of those participants surveyed indicated concern about the threat that terror can pose to their offshore locations. Further analysis on social stability and terrorism as part of this research has been detailed in subsequent sections.

According to Srivastava, Teo & Mohapatra (2009, p121), “Risk-taking and managing ability emerge as major determinants for the offshoring decision”. An organisation’s ability to control and manage its operations should be at the forefront of its decision to outsource. Authors such as Ho and Atkins (2009, p35) and Lynch (2008, p44), however, have described many of the most outsourced-to locations as providing poor-quality outputs. Considering the most important driver behind an offshoring decision is the saving of costs, quality output should be a priority for mitigation. Of the participants surveyed in this study, eighty-three (83) per cent indicated a concern regarding the quality of output. The location selected should be assessed to ensure that the nation has a track record of providing the desired output quality prior to establishing the
venture. The concerns of participants emphasise that mitigating processes and activities should also be established to ensure that quality is managed, measured, reported on and controlled. The potential to control resource quality is a precursor to acceptable quality output; yet obtaining background checks can prove difficult in some countries. Twenty (20) per cent of participants advised they were concerned about the lack of public records available to perform thorough background checks, which essentially means that not only are eighty-three (83) per cent of people concerned about quality output but twenty (20) per cent have concerns that they may not be even able to select and recruit the most suitable resources to complete the work in the first place, presenting a serious compounded risk for ANZ enterprises.

5.3 Maintaining Organisational Control

In their text on Machiavelli, Skinner and Price (1988, p84) detail an interesting theory on willingly taking risk:

A man should never risk falling because he thinks it is likely that he will be rescued. This may not happen, but even if it does it will not make you secure; such a defence is weak and cowardly, because it is outside your control. Only those defences that are under your control and based on your own ability are effective, certain and lasting.

This thought-provoking theory, if translated within the context of today’s business environments, suggests that an enterprise that takes a known risk assuming that they will be protected from its impact demonstrates weakness and a lack of control. To be effective and stable an enterprise must be in control of its defences, taking action to mitigate threats and protect itself from hazards. Maintaining control in an enterprise is also critical to an organisation steering itself in the correct direction, in order to ensure it pursues and achieves its intended strategy. Outsourcing to local firms has long been seen by enterprises as an option to leverage the capabilities of larger specialist firms to fulfil business requirements whilst maintaining operations onshore. Maintaining operations onshore assists with maintaining control as it provides greater visibility to
the client and allows an organisation to ensure its operations are maintained within a nation with which it fully understands the location-based risks. Taking these measures to avoid relinquishing complete control to an outsourcing firm will also prevent the firm from being exposed to offshore risks. Of the organisations studied, only sixty (60) per cent of individuals indicated they agreed with this concept (see Figure 5.3), with thirty-nine (39) per cent indicating they did not feel that outsourcing locally provided the benefits of outsourcing without the inherent risks. This reveals that Australian organisations could potentially have more to learn on the real risks associated with the offshore locations that are outsourced to.

The research conducted included an analysis of the offshore locations that enterprises in Australia and New Zealand outsource to. Thirty-one (31) per cent of those that outsource currently do so to Australian firms or locations and twenty-eight (28) per cent of these indicated that they outsource to Australia exclusively (i.e. they do not outsource to any other location). Interestingly, although there is now evidence to demonstrate that a large number of the Australian organisations studied did not believe that outsourcing to local firms provided greater benefit and less risk in comparison to offshore firms, a large number of participants still indicated that their organisations
should be doing more to mitigate the risks associated with outsourcing. Figure 5.4 below illustrates that sixty-five (65) per cent of individuals believe their business should be doing more to mitigate the risks associated with outsourcing whilst thirty-four (34) per cent suggested that their organisation should not be doing more to mitigate the risks. This exemplifies the fact that there remain a significant number of Australian organisations that are failing to realise the potential disruption that outsourcing can have on their organisation. Thirty-four (34) per cent of those studied believe that their organisation is adequately managing the potential risks associated with their outsourcing ventures, suggesting that these organisations need not change their practices to further improve their threat-level, or a greater understanding of offshore risks needs to be obtained by these individuals in order to influence and shift their enterprise’s risk tolerance if they are to remain competitive.

![Figure 5.4 – More Required to Mitigate Risk](image)

5.4 Offshore Trust

More than 500 years ago, Machiavelli was raising thoughts on managing trust:

> Trust must be built up over the years and should not be assumed to be present at the first acquaintance. Years of employment, however, do not equate to trust.
Trust is a personal emotion and trust only truly works if it is found to flow in both directions. (McAlpine, 2000, p81)

Lynch (2008, p44) questions whether an enterprise can truly trust an outsourcing firm where there is a lack of public records to sufficiently complete background checks. Trusting a firm that resides on the other side of the globe to effectively deliver services can prove challenging.

There is an assumption that developments in ICTs have eliminated the difficulties of co-ordinating service work with vendors in remote locations. However, distance still matters and the characteristics of some services mean that culture, language and geographic distance are significant barriers to using vendors in remote locations. Studies on distributed software development have shown that distance creates difficulties in areas of communication, control, supervision, co-ordination, creating social bonds and building trust. (McIvor, 2010, p85)

In an offshoring engagement an enterprise is expected to relinquish control to an outsourcing firm and also limit its ability to supervise remote operations. The loss of control and limited visibility of remote operations provide a breeding ground for mistrust, siloed organisational units and increased risk. If an enterprise does not have visibility of remote operations it’s inconceivable to picture the systematic and comprehensive mitigation of all risk.

5.5 Australia’s Top 5 Offshoring Destinations

This research has revealed the locations outsourced to by Australian businesses. Of these locations, the top five most outsourced-to countries, depicted in Figure 5.5, indicate that Australians primarily outsource to nations in the Asia Pacific region. The focus of Lynch (2008), Linstead, Fulop and Lilley (2004) and Turban and Volonino (2011) on India and China as the primary outsourced-to nations has been validated by the data collected, clearly indicating that they are among the most outsourced-to countries. The most outsourced-to nation, India – with over sixty-eight (68) per cent of
respondents indicating that they actively outsource to India – is clearly the market leader based on the data collected from ANZ-based enterprises. Surprisingly, the Philippines (36.7%) and Malaysia (25.3%) were slightly more prevalent than China (22.8%) as an option to outsource to. Singapore rounds out the top five with just over sixteen (16) per cent of participants outsourcing there. The prevalence of Asia Pacific nations in the top five demonstrates Australia’s reliance on the region for doing business.

![Top 5 Offshoring Destinations](image)

An analysis of the top five outsourcing nations was conducted to capture the correlation between the country outsourced to and the amount of perceived risk. As outlined in Figure 5.6, twenty (20) per cent of those outsourcing to India and seventeen (17) per cent of those outsourcing to the Philippines advised that their organisation has a high tolerance for risk. Of those outsourcing to Malaysia and Singapore ten (10) per cent and twenty-three (23) per cent respectively indicated their organisation has a high tolerance for risk. The findings indicated that China, however, had the largest proportion of people currently outsourcing that indicated their organisation had a high tolerance towards risk. In comparison, only twenty (20) per cent of those that outsource to Australia indicated that their organisation had a high tolerance to risk.
As part of the study, participants were asked to indicate whether they believed outsourcing to local firms provided the benefits of outsourcing without the inherent risks in comparison with offshore firms. As shown in Figure 5.7 below, sixty-nine (69) per cent of those outsourcing to India indicated that they believed local firms would provide the same benefits with reduced risk. Those actively outsourcing to the Philippines and Malaysia indicated that fifty-nine (59) and fifty (50) per cent respectively saw local outsourcing as providing the benefits without the risk. Seventy-eight (78) per cent of those outsourcing to China and seventy-seven (77) per cent outsourcing to Singapore advised that local firms provided the benefits without the risk. Such a large proportion of individuals seeing equal benefit and less risk when pursuing local outsourcing engagements demonstrates that firms should be able to obtain the same outcome without the risk, which raises the question why organisations continue to pursue such arrangements, monetary drivers aside. In contrast, only fifty-six (56) per cent of those that outsource to Australian firms believed this to be the case.
The individuals that contributed to the study were questioned as to whether their organisation implemented measures to prevent the loss of intellectual property (IP). As illustrated in Figure 5.8 below, only forty (40) per cent of those offshoring to Malaysia had implemented controls to protect their IP. Of those outsourcing to India forty-four (44) per cent indicated that they had implemented controls and forty-five (45) per cent currently outsourcing to the Philippines responded likewise. Of those outsourcing to China, fifty-six (56) per cent advised their employer implemented controls and sixty-two (62) per cent of those offshoring to Singapore had measures to safeguard against the loss of IP. Only forty-eight (48) per cent of those outsourcing within Australia, however, said that they implemented measures to protect IP, indicating that, overall,
organisations were not vastly more concerned regarding the loss of IP when outsourcing offshore rather than locally.

Figure 5.9 represents the responses provided by participants when asked if their organisation should be doing more to mitigate the risk inherent in outsourcing and offshoring. Seventy-five (75) per cent of those outsourcing to Malaysia, seventy-seven (77) per cent of those outsourcing to Singapore, and seventy-six (76) per cent of those outsourcing to the Philippines and India indicated that their organisation should be doing more to mitigate the risks of outsourcing/offshoring. Of those that outsource to China, however, eighty-three (83) per cent believed their employer should be taking greater action to mitigate the risk of outsourcing. These metrics are considerably higher in comparison with those outsourcing to Australia, where only sixty (60) per cent believed their enterprise should be doing more. This suggests that those outsourcing to Australia perceive a lesser threat in contrast to those outsourcing to offshore locations, with a greater number of individuals believing their organisation is adequately treating the perceived risks.

![Figure 5.9 - Top 5 More Required to Mitigate Risk](image-url)
5.6 Outsourcing Locations

5.6.1 India

India has long been one of Australia’s most frequently outsourced-to nations, but it can pose some significant risk to an organisation seeking to offshore their operations to the nation. Health care can be an issue in India with the potential to contract diseases such as malaria, hepatitis and meningitis posing a risk to employees (Young Pelton, 1995, p271). Vagadia (2007, p7) advises that with a population in excess of one billion people, India poses a relatively high level of political risk, which, together with its ongoing dispute with Pakistan, makes it a high-risk destination in the eyes of many. Nevertheless, the IT industry is one of India’s fastest growing sectors (Vagadia, 2007, p7). Australian research participants claimed India was their most outsourced-to country with over sixty-eight (68) per cent outsourcing functions to the nation. This clearly highlights the fundamental link between outsourcing to save costs and offshoring increasing risk. Young Pelton (1995, p261) advises that India can be prone to religious violence and terrorism:

... every time a bomb goes off, and they go off a lot, the suspects include Indians, Pakistani agents, Kashmiri separatists, Sikh terrorists, Maoist rebels, Sri Lankan Liberation Tigers of Tamil Eelam guerrillas, Muslim militants, drug traffickers and even gangsters. (Young Pelton, 1995, p264)

Carmel and Tjia (2005, p46) raise the risk that India’s political interests can pose to an organisation, stating that:

... we heard an interesting rumour on this issue of controlling risk: during the Indian-Pakistani tensions of 2002, GE’s CEO spoke to India’s Premier and warned him that if war breaks out, GE will have to move most of its vast operations out of India. After a brief period of crisis, tensions subsided.

This rumour may demonstrate how much India’s position as a global offshoring destination influences its decision, but it also emphasises how volatile the ecosystem is and the speed at which an issue could arise. It may be important to keep in mind that
“the last full-scale war between India and Pakistan took place in 1971, and the threat of a nuclear conflict is the key restraint on both countries” (Hendel, Messner & Thun, 2008, p20). Although another war may not occur, the potential for war should be factored into the overall risk assessment when considering this nation as an offshore location.

Some parts of India may have subpar public infrastructure:

In 2012, a series of blackouts in India impacted 700 million people – 10 per cent of the planet’s population. Later investigations concluded that the domino effect was caused by overloading, which in turn was triggered by bad math, bad communication, and an information infrastructure that simply wasn't up to the task. (McDonald, 2015, p3).

With its high potential to obtain highly skilled IT labour and cost-effective rates, it would be foolish not to consider India as a nation to outsource to, yet the potential for these risks should be addressed by any organisation seeking to offshore to India. Considering over seventy-seven (77) per cent of individuals indicated their organisation has a low appetite for risk, it is surprising that such a large number of Australian organisations continue to outsource to the nation, if Young Pelton (1995) and Vagadia (2007) are correct in their claims that India is a high-risk nation.

5.6.2 China

The Chinese Government has large plans for developing its nation. The government has assigned future growth in science and technology sectors a high priority:

China has a national plan to expand the information technology outsourcing (ITO) and business process outsourcing (BPO) sectors. (Willcocks Cullen & Craig, 2011, pxvi)

The literature suggests that China can pose a risk to an enterprise in a number of ways. Terrorist incidents and political violence, boat, aircraft, railway and road safety
concerns all contribute to the potential risk level that China poses (Young Pelton, 1995, p709).

China is looking to compete with India on the global IT outsourcing stage. However, its progress has been slow due to a sluggish IT and business process services industry, a lack of IT talent and a bad reputation for intellectual property protection and security. (Overby, 2013a)

According to the survey conducted, China is one of Australia’s most outsourced-to nations; yet China has a history of IP theft. Sinovel, a leading Chinese wind-energy company, outsourced the electronic control systems and software used in its wind turbines to a United States-based firm, American Superconductor (AMSC).

In June 2011, a group of AMSC engineers testing a Sinovel turbine in northern China uncovered electrical components that were running a stolen version of AMSC software. Sinovel had somehow accessed AMSC proprietary source code and was manufacturing its own electrical components, cutting AMSC out of the operation. (Reynolds, 2014, p218)

Many authors have criticised China for the skill level of its resources. For example:

Lack of training in project management and process leaves many companies stuck doing low level work. And lack of English proficiency excludes most players from the lucrative outbound call centre business. (Overby, 2013a)

Yet China offers significant potential as an offshoring destination, primarily because it can be more cost-effective than other, more mature outsourcing nations such as India. China currently provides outsourcing services to just under twenty-three (23) per cent of research participants, indicating that China is ranked amongst the top-five outsourced-to nations in Australia and New Zealand.

5.6.3 Brazil

Brazil has experienced urban violence with terrorism, criminal activity and kidnapping plaguing the nation. Evidence suggests that there has been a “sharp increase in urban
violence” (Young Pelton, 1995, p506). Brazil also has a history of political violence as well as incidents where “guerrillas from Peru and Colombia occasionally cross Brazil’s western frontier” (Young Pelton, 1995, p506). Yet this has not stopped Australian enterprises from outsourcing to the nation with over five (5) per cent of those surveyed indicating that they outsourced to Brazil. Brazil presents a much more significant risk of violence than Australia and therefore should be approached with risk management at front of mind.

5.6.4 United States of America
The United States of America has a history of recent and current terror incidents along with a significantly high terror threat-level. The United States has also been considered the most murder-prone country in the developed world (Young Pelton 1995, p565). Therefore any company looking to outsource to the US could be placing their enterprise at increased risk. Over five (5) per cent of those surveyed indicated that they have outsourced to the US. As the US shares a number of similarities with Australia and New Zealand it is completely understandable that ANZ enterprises consider the United States as a location to outsource to. However, it is not clear that the US actually provides any significant cost savings in comparison to local ANZ resources, which should be deliberated by enterprises considering this nation. Furthermore, authors such as Rosenberg and Mateos (2011, p75) suggest that enterprises may be “concerned about using SaaS in the United States, given the US Patriot Act” and its related privacy issues. Any Australian organisation seeking to adopt an outsourced technology from the US should be aware that legislation allows the US Government to access the enterprise’s data at will. Measures to mitigate this risk, such as data encryption, require careful consideration when outsourcing to such a location.

5.6.5 Philippines
The popularity of the Philippines as an offshoring destination has grown considerably in recent years. Over thirty-six (36) per cent of participants indicated that they were outsourcing to this nation. Yet the Philippines provides some risk of “bomb blasts, assassinations and grenade attacks” (Young Pelton, 1995, p701). The Australian
Department of Foreign Affairs Smart Traveller website can be used by organisations as a quick and easy tool for measuring offshore location safety, as it is a resource that most Australians are familiar with, covers most locations in the world and is a free, readily available resource. The information available is kept up to date as international events unfold and, most importantly, safety advice is provided in accordance with Australian standards rather than foreign standards. For example, some locations in Asia may be considered safe for travel according to Asian standards; however, in comparison to Australian standards they may present risk. The Australian Department of Foreign Affairs and Trade (2015), through Smart Traveller, recommends that when travelling to the Philippines, Australians exercise a high degree of caution with some areas such as Eastern Mindanao, suggesting the need to reconsider travelling to the location. For some regions within the Philippines such as Central and Western Mindanao, including the Zamboanga Peninsula, and the Sulu Archipelago, Australians are advised not to travel at all. However the English language is far more widely spoken in the Philippines than in India, making it a popular option in the region for Australians (O’Malley, 2013, p75).

5.6.6 Malaysia
According to the Oxford Business Group (2010, p210), “Malaysia was a late entrant to the ITO industry, and as such it sometimes lags behind the Philippines, India and Thailand in competitiveness.” Malaysia ranks itself among the most outsourced-to destinations for Australia and New Zealand with over twenty-five (25) per cent of people indicating that their employer currently outsources to the location. The Australian Government (2015) suggests that in travelling to Malaysia, visitors should exercise a high degree of caution in locations around the Eastern Sabah and suggests that travel plans should be reconsidered to the coastal region and nearby islands altogether. That aside, Malaysia has long been considered one of the most investor-friendly nations (Gold, 2005, p118). Most importantly, interference from the government is considered negligible (Gold, 2005, p118), which is vastly different from other nations in the region.
5.6.7 Singapore

Singapore is considered one of the easiest countries with which an enterprise can do business (Gold, 2005, p118). Overall, Singapore is ranked among the safest nations being outsourced to, with the Smart Traveller website (Australian Department of Foreign Affairs & Trade, 2015) providing the all clear for travel safety. Over sixteen (16) per cent of participants indicated that they currently outsource to Singapore. Not only is it one of the most outsourced-to nations but it also represents low risk. Singapore has a “business and legal structure to support rights of foreign investors” (Gold, 2005, p118), thereby increasing the potential for foreign enterprises to invest in the nation. Singapore is also considered to have a low crime rate and a solid medical network with good doctors (Siepmann, 2013, p19), which also contributes to its overall appeal in comparison with other locations, such as India.

5.6.8 Argentina

Argentina is rated as a safe travel destination based on the Smart Traveller’s overall green status rating for safety (Australian Department of Foreign Affairs & Trade, 2015). With over five (5) per cent of participants indicating that they currently outsource to the nation, Argentina could be considered a low-risk location to outsource to. Although Argentina has had a tumultuous history, of the developing nations it represents excellent value in comparison to the inherent risk.

5.6.9 Ireland

Ireland presents a sound option for outsourcing, with the Smart Traveller providing a green safety ranking (Australian Department of Foreign Affairs & Trade, 2015). With fewer than four (4) per cent of individuals indicating that they are currently offshoring to Ireland, the nation offers a promising location for offshoring due to its stable location and cultural similarity with Australia and New Zealand. Ireland is considered to have promisingly low corporate tax rates as well as an industry-friendly and supportive government (Gefen, 2011, p16). That’s not to mention the potential that the European Union has provided the nation, such as economic and social benefits. Gefen (2011, p16) advises that in Ireland CEOs can actually talk directly with government
ministers. This may present a very promising location with lucrative opportunities for Australian enterprises. The enormous potential for Ireland in offshoring has led to the country going from one of the poorest countries in the EU to one of the richest over the past two decades (Roebuck, 2012, p73).

5.6.10 Israel
For a number of years now Israel has faced an increase in terrorist attacks (Young Pelton, 1995, p275). Since the British carved Israel out of Palestine after World War II, there remains contention between Israel and its neighbours that threaten its stability and the safety of its people (Young Pelton, 1995, p275). This makes travelling to the nation problematic. The Australian Government through the Smart Traveller website rates the safety of travel to the region as poor. It suggests that travellers to the nation should exercise a high degree of caution and advises against travel to a number of locations such as the West Bank, including Bethlehem and Jericho. It also advises that there should not be any travel to locations in the Gaza strip (Australian Department of Foreign Affairs & Trade, 2015). This has not stopped two point five (2.5) per cent of participants' employers outsourcing to the country. If Israel poses a risk to travellers, how will employees of the organisations in Australia travel to the nation on business without placing themselves at serious risk? Organisations should seek to implement measures to mitigate risk if they are considering outsourcing part of their enterprise to a greatly contested and volatile nation in order to ensure this does not have any impact on their enterprise in the future.

5.7 Natural Disasters and Business Continuity
Natural disasters can affect business continuity. Whether through volcanoes, floods, earthquakes, tsunamis or any other natural disaster, the risk that natural disasters pose to an enterprise is substantial. Those surveyed indicated that organisations based out of Australia frequently outsource to disaster-prone nations, increasing the threat potential that natural disasters can pose to their enterprise. For the purposes of analysing the change in threat-level experienced by an Australian enterprise that outsources offshore,
indexes have been utilised to formulate a benchmark for the measurement of a nation’s threat level. The nations outsourced to by ANZ respondents identified through the survey have been assigned index ratings to determine the risk level in comparison to Australia. The index summary illustrates the nation’s risk whereby green demonstrates the risk level for the nation is lower than that of Australia’s risk level and red indicates that the risk level is higher. Therefore in transitioning an operation from Australia to a nation with a red risk identifier, the organisation has increased the risk based on the indexes used to measure the threat.

To derive the below indicators, index ratings were obtained from the *World Risk Report* published by the United Nations University (Mucke, 2014, p63), which provides detailed metrics on natural disaster risk analysis for countries worldwide. An index metric for each country is determined through examining the risk of each nation in falling victim to natural disasters along with the potential exposure to natural hazards and the vulnerability of each society. Based on these data, an analysis has been completed for the countries currently outsourced to from Australia. Those that outsourced to India, the Philippines, Malaysia, China, Brazil, Ireland, Japan, Hungary, Netherlands, Peru, Thailand, Mexico, Indonesia and Bulgaria actually increased their organisation’s risk of being affected by natural disasters based on the data obtained from the United Nations University. Of the top five outsourced-to nations, only Singapore represents a lower risk of natural disasters than Australia. With such extreme risk, organisations outsourcing to these nations should be making adjustments to their ERM practices to compensate for the increased risk wherever possible.
In 2011, the 12 countries at extreme risk of natural disasters were identified using the Natural Disasters Risk Index (NDRI), from British advisory firm Maplecroft. The index was calculated through measuring the frequency of natural disasters over the past 30 years in each nation, in addition to the number of deaths caused and the death toll as a proportion of the total population (NDRI, 2011). Of the countries outsourced to from Australia, three of the top five most outsourced-to nations appear in the 12 countries most at risk of natural disasters, with the Philippines, India, China and Indonesia all making the list.

### 5.8 Social Unrest, Political Stability and Business Continuity

In 2011, the 12 countries at extreme risk of natural disasters were identified using the Natural Disasters Risk Index (NDRI), from British advisory firm Maplecroft. The index was calculated through measuring the frequency of natural disasters over the past 30 years in each nation, in addition to the number of deaths caused and the death toll as a proportion of the total population (NDRI, 2011). Of the countries outsourced to from Australia, three of the top five most outsourced-to nations appear in the 12 countries most at risk of natural disasters, with the Philippines, India, China and Indonesia all making the list.

### 5.8 Social Unrest, Political Stability and Business Continuity

In 2011, the 12 countries at extreme risk of natural disasters were identified using the Natural Disasters Risk Index (NDRI), from British advisory firm Maplecroft. The index was calculated through measuring the frequency of natural disasters over the past 30 years in each nation, in addition to the number of deaths caused and the death toll as a proportion of the total population (NDRI, 2011). Of the countries outsourced to from Australia, three of the top five most outsourced-to nations appear in the 12 countries most at risk of natural disasters, with the Philippines, India, China and Indonesia all making the list.
Social unrest can impact on an organisation’s operations by disrupting business and increasing activity that prevents an organisation from performing its functions. Conversely:

Political stability ensures that your outsourcing partner stays in business and you do not suddenly lose your investment that is located in a foreign country due to political unrest or a change in ruling party. (Siepmann, 2013, p8)

The Global Peace Index (Institute for Economics and Peace, 2014, p5) ranks nations according to their level of peace. The index provides a gauge for the overall safety and security in society, the extent of domestic or international conflict and the degree of militarisation. The nations outsourced to by ANZ respondents identified through the survey have been assigned index ratings to determine the risk level in comparison to Australia. Of the countries outsourced to, India, the Philippines, Malaysia, China, Singapore, USA, Brazil, Argentina, Great Britain, Poland, Russia, Israel, Hungary, Netherlands, Peru, Thailand, Mexico, Indonesia and Bulgaria all represent a greater risk of social unrest. The only nations that are considered to have greater political stability than Australia are Ireland, Japan and Canada. Of the top five outsourced-to countries, there are no nations that present a lower risk than that of Australia, based on this index.

### 5.9 Criminal Activity

<table>
<thead>
<tr>
<th>Country</th>
<th>Crime Risk Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>46.55</td>
</tr>
<tr>
<td>USA</td>
<td>50.01</td>
</tr>
<tr>
<td>Poland</td>
<td>32.99</td>
</tr>
<tr>
<td>Canada</td>
<td>37.46</td>
</tr>
<tr>
<td>Indonesia</td>
<td>47.22</td>
</tr>
<tr>
<td>Philippines</td>
<td>43.11</td>
</tr>
<tr>
<td>Brazil</td>
<td>68.95</td>
</tr>
<tr>
<td>Russia</td>
<td>51.33</td>
</tr>
<tr>
<td>Netherlands</td>
<td>35.41</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>43.45</td>
</tr>
<tr>
<td>Malaysia</td>
<td>69.97</td>
</tr>
<tr>
<td>Argentina</td>
<td>62.40</td>
</tr>
<tr>
<td>Japan</td>
<td>20.24</td>
</tr>
<tr>
<td>Peru</td>
<td>57.63</td>
</tr>
<tr>
<td>Thailand</td>
<td>37.06</td>
</tr>
<tr>
<td>China</td>
<td>41.75</td>
</tr>
<tr>
<td>Ireland</td>
<td>49.07</td>
</tr>
<tr>
<td>Israel</td>
<td>30.40</td>
</tr>
<tr>
<td>Mexico</td>
<td>53.84</td>
</tr>
<tr>
<td>Singapore</td>
<td>17.59</td>
</tr>
<tr>
<td>Great Britain</td>
<td>42.01</td>
</tr>
<tr>
<td>Hungary</td>
<td>41.76</td>
</tr>
<tr>
<td>Australia</td>
<td>42.16</td>
</tr>
</tbody>
</table>

**Figure 5.12 – Crime Risk Indicators**
Crime can impact on an organisation’s operations by disrupting its business directly or indirectly. Most importantly, criminal activity places the organisation’s resources at risk, which can impact not only on the employees located in the country, but also the Australian employees who are required to travel to the nation on business. Seipmann (2013, p8) points out that:

... a high crime rate is an indicator for many problems. It also puts your personnel at risk when traveling to that foreign country. Physical assets and intellectual property are particularly at risk in countries with high crime rates.

The recent Crime Index (Numbeo, 2015a) provides a ranking of the overall level of crime across each country. Based on this index, a number of countries that are outsourced to present an increased risk in comparison to that of Australia. These nations include India, the Philippines, Malaysia, USA, Brazil, Argentina, Ireland, Russia, Peru, Mexico, Indonesia, and Bulgaria. Three of the top five outsourced-to nations pose an increased risk of criminal activity, although there are 10 nations that provide a more favourable risk level, as illustrated with green indicators.

5.10 Health Care

<table>
<thead>
<tr>
<th>Country</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>66.86</td>
</tr>
<tr>
<td>USA</td>
<td>67.75</td>
</tr>
<tr>
<td>Poland</td>
<td>58.03</td>
</tr>
<tr>
<td>Canada</td>
<td>69.60</td>
</tr>
<tr>
<td>Indonesia</td>
<td>66.09</td>
</tr>
<tr>
<td>Philippines</td>
<td>71.66</td>
</tr>
<tr>
<td>Brazil</td>
<td>52.15</td>
</tr>
<tr>
<td>Russia</td>
<td>51.80</td>
</tr>
<tr>
<td>Netherlands</td>
<td>67.23</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>58.47</td>
</tr>
<tr>
<td>Malaysia</td>
<td>69.14</td>
</tr>
<tr>
<td>Argentina</td>
<td>75.18</td>
</tr>
<tr>
<td>Japan</td>
<td>87.07</td>
</tr>
<tr>
<td>Peru</td>
<td>64.68</td>
</tr>
<tr>
<td>Australia</td>
<td>71.85</td>
</tr>
<tr>
<td>China</td>
<td>58.74</td>
</tr>
<tr>
<td>Ireland</td>
<td>49.53</td>
</tr>
<tr>
<td>Israel</td>
<td>76.35</td>
</tr>
<tr>
<td>Thailand</td>
<td>82.47</td>
</tr>
<tr>
<td>Singapore</td>
<td>66.14</td>
</tr>
<tr>
<td>Great Britain</td>
<td>73.88</td>
</tr>
<tr>
<td>Hungary</td>
<td>51.58</td>
</tr>
<tr>
<td>Mexico</td>
<td>67.79</td>
</tr>
</tbody>
</table>

**Figure 5.13 – Health Care and Medical Risk Indicators**

Many scholars have highlighted healthcare availability and quality as a concern in some of the developing nations. Much like the risk of crime, health care can impact on an organisation’s local resources as well as those people that travel to the nation. The
Health Care Index provides an overall estimation of the cost, equipment, quality of healthcare systems and healthcare professionals including staff and doctors (Numbeo, 2015b). Based on this index, the countries that pose a more significant risk in comparison to Australia are India, the Philippines, Malaysia, China, Singapore, USA, Brazil, Ireland, Poland, Russia, Hungary, Canada, Netherlands, Peru, Mexico, Indonesia and Bulgaria. Overall, only five countries outsourced to present a lower risk. These nations are Argentina, Great Britain, Japan, Israel and Thailand. However, all nations in the top five outsourced-to countries pose an increased risk; therefore, a very large proportion of the enterprises that outsource could be in serious danger.

### 5.11 Economic Stability

![Figure 5.14 – Economic Stability Risk Indicators](image)

Economic stability is an important measurement for understanding how stable or volatile a nation is from an economic perspective. Siepmann (2013, p8) highlights the potential impact that the economy can have on outsourced operations, and how this can affect quality of service:

A healthy economy ensures growth and educated talent that the outsourcing company can use to support your operation. This aspect ensures that the outsourcing company stays competitive and provides quality service.

The Trading Economics index has been utilised to rank the nations outsourced to in terms of the stability of their economy. The index rating is compiled based on
economic indicators, financial markets and the credit ratings for each nation (Trading Economics, 2015). Based on this information, the following outsourced-to nations present an increased risk in comparison to Australia: India, the Philippines, Malaysia, China, Brazil, Argentina, Ireland, Great Britain, Poland, Russia, Japan, Israel, Hungary, Peru, Thailand, Mexico, Indonesia and Bulgaria. Four of the top-five most outsourced-to countries have an increased risk of economic volatility. Overall, only four nations – Singapore, USA, Canada and Netherlands – represent a more stable economy than that of Australia.

5.12 Terrorism – The New Threat to IT Operations

Terrorism shares a number of traits with other location-based risks such as natural disasters or social turbulence. Terrorist attacks are difficult to predict, have the potential to disrupt business and can be rampant in a majority of countries that Australians and New Zealanders outsource to. At its heart, terrorism has the potential to affect business continuity. India, Australia’s most outsourced-to country, according to the survey conducted, has been the victim of attempted terrorist attacks targeting the outsourcing industry.

Local police have identified India’s software and services outsourcing industry as a likely target for a terrorist group operating in the country. Documents seized from three members of the Lashkar-e-Toiba terrorist group killed in an
encounter with the police revealed that they planned to carry out suicide attacks on software companies in Bangalore. (Graham & Kaye, 2006, p178)

Yet the Western countries that Australians outsource to are not immune. The USA, the sixth most outsourced-to country, according to the survey results, has also been the victim of a number of terrorist incidents. Although the impact of the September 11 terrorist attacks on the public has been well publicised, there was also an impact to businesses. In total, the incident resulted in a:

... loss of 6 buildings (13.42 million sq. ft.), 9 buildings heavily damaged (15.1 million sq. ft.), 16 other buildings suffered minor damage (10 million sq. ft.), 36 miles of telecomm cabling, 300k phones, 4.5 million data circuits serving 140,000 Verizon customers. (Lynch, 2008, p50)

It’s clear how such an unexpected event can have an impact on business operations when it has the potential to affect buildings, telephones and data circuits on such a large scale.

The Global Terrorism Index report (Institute of Economics and Peace, 2014, p8) provides an index for world countries based on their potential terrorism threat level. The index is formulated based on global trends and patterns over the last 14 years commencing from the year 2000. Based on data obtained from this index report, an analysis of the countries outsourced to was completed, and based on this analysis, it is evident that India, the Philippines, Malaysia, China, USA, Brazil, Argentina, Ireland, Great Britain, Russia, Israel, Canada, Netherlands, Peru, Thailand, Mexico, Indonesia and Bulgaria all present a greater risk of terrorism than does Australia. Four of the top five most outsourced-to countries pose an increased risk and, overall, only four of the outsourced-to nations provide an improved position on the risk of terror for organisations that outsource offshore. These nations are Singapore, Poland, Japan and Hungary.
5.13 Adjustments to ERM Practices

With the potential for outsourcing risks to have commercial impacts, organisations should be making adjustments to their ERM practices in order to safeguard themselves against the potential impacts. Transitioning a software development function based out of, for example, North Sydney to an offshore location such as the Philippines can generate additional risk. Although the cost associated with the function will be reduced through the reduction in operational (primarily resource) costs, the potential natural disasters, social unrest, crime and economic conditions result in a change to the probability of these risks occurring and impacting the enterprise. If an organisation assesses the risk of the new location and deems the location to be acceptable, an enterprise should still be making adjustments to their ERM practices to compensate for the increase in risk. For instance, the enterprise may decide to develop more stringent business continuity plans and processes to mitigate the impact of natural disasters or social unrest impacting on the organisation’s operations. This does not prevent the organisation from pursuing offshore engagement; it merely serves as a mechanism to reduce the probability of its operations being impacted and provides a lever to reduce the severity if it occurs.

Authors such as Siepmann (2013) and Lynch (2008), among others, have documented in detail the potential for impacts; however, only thirty-five (35) per cent of professionals that took part in this study advised that their organisation actually adjusts their risk-management practices to compensate for the increase in risk. As indicated in Figure 5.16 below, almost half of the sample group, forty-four (44) per cent advised that they were unsure if their organisations have made adjustments to ERM practices when outsourcing. If an organisation’s senior technology professionals are unsure whether or not the ERM practices have been adjusted, this suggests that either no adjustment has been made or there has been little effort by the organisation to implement measures and communicate them effectively to its senior staff. Finally, over twenty (20) per cent of Australian IT professionals surveyed advised that their
organisation has not implemented any adjustment to its ERM practices to safeguard against the risk of outsourcing.

When outsourcing, risks have the potential to erode the anticipated cost savings. Carmel and Tjia (2005) suggest that it is important for risk assessments to take place prior to moving operations offshore. They advise that:

... risk assessment needs to take place up-front, before going offshore, but also on an ongoing basis. Many firms conduct some type of country risk assessment before they enter a country. However, it is rare that firms continue to conduct regular assessments once they already have operations in-country. This is a mistake. (Carmel & Tjia, 2005, p49)

It would be difficult to conceive that if an organisation is not adjusting their ERM practices as part of an outsourcing engagement that they would have an appetite for, or the ability to conduct, ongoing analysis of the risk. Yet this research has exposed an overall lack of attention to ERM practices and revealed a theory that overlooking ERM could have the potential to increase the risks associated with outsourcing significantly. This is because risk management is primarily based on probability. The more functions
and processes an organisation outsources, the more likely it will be exposed to the risks eventuating. The more offshore locations an organisation outsources to, the greater the probability that the organisation will be impacted by a location-based risk occurring. The more outsourcing providers an enterprise engages, the greater the likelihood the enterprise will face the eventuating of an outsourcing risk such as IP loss. The number of organisations not adjusting their ERM practices and the increase in the probability for risks to occur may be extrapolating the potential for commercial harm.

5.14 Location Assessment Tool

As part of the research, the literature was evaluated prior to the survey being conducted to assist in formulating the survey questions. The risks identified by authors in the literature were collated and analysed in order to identify all the potential elements that could contribute to a location’s risk. The survey results were reviewed to ascertain whether or not the enterprises surveyed considered the risks identified by authors as being of genuine concern when outsourcing in practice. The literature was then reviewed again, with the intention of identifying linkages and correlations between the literature reviewed prior to the survey, and the survey responses. As a result, similarities between the situations of today and in historical times were discovered and incorporated into the analysis, providing an entirely new and unique dimension to the research. The risks identified by authors, the concerns of enterprises in practice obtained from the survey, and the risk-management perspective from literature on ancient and medieval history were used by the Chief Investigator of this study to formulate the key elements that comprise the Location Assessment Tool.
As a result of this research, key tactical influences have been derived to form the offshore strategic pillars – i.e. 15 strategic components that uphold a successful offshoring venture. All 15 areas warrant some form of consideration in the assessment of a location, considering the survey results indicated that many of the risks associated with offshoring were not of genuine concern to enterprises in practice. If organisations are serious about conducting a thorough assessment they will need to consider all 15 areas independently.

![Offshore Strategic Pillars](image)

Figure 5.17 – Offshore Strategic Pillars

Portrayed in Figure 5.17, these 15 critical areas form the basis of any sound location analysis. In order to assist organisations in mitigating the risks associated with offshoring, the Location Assessment Tool, a form used for comprehensive analysis and provided in Appendix A, has been developed to be used for analysing and comparing different offshore nations. Utilising the Location Assessment Tool ensures that the key selection criteria for determining the most suitable country is employed when finalising the decision to offshore.
The Location Assessment Tool in Appendix A is based on the 15 strategic pillars. Using a blank Location Assessment Form, a score is added for each of the 15 strategic areas. An enterprise determines the weight of each area based on their risk appetite, their investigation of the country being considered and the exact conditions at the time of assessment. The score is obtained from the risk matrix in Figure 5.18 below by selecting the most suitable number based on the combination of probability and impact. For example, if a location has been assessed and the probability of crime is very low and the impact is considered high, the score of 0.50 should be recorded on the Location Assessment Form under the “Crime” pillar in Appendix A. Ultimately the weight applied to the ratings for each pillar will be determined by the organisation completing the Location Assessment as the risks vary from enterprise to enterprise, from outsourcing vendor to outsourcing vendor, and from city to city. The individual conducting the assessment should give careful consideration to the weight applied to each item as it pertains to their individual enterprise.

Once completed for all the required nations and all 15 strategic areas the results can be tallied to reveal the total threat rating for each nation. As most offshoring ventures are typically established through projects, the risk matrix in Figure 5.18 has been based on the Prince2 project management methodology (Hedeman, Van Heemst & Fredriksz 2009, p80), thereby making it easily relatable to the project managers managing the offshoring project, but easy enough to be utilised by any delegated party. Further information on each of the strategic pillars for assessment has been detailed in subsequent sections.

<table>
<thead>
<tr>
<th>Threat Assessment</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Low</td>
</tr>
<tr>
<td>Certain</td>
<td>0.60</td>
</tr>
<tr>
<td>High</td>
<td>0.50</td>
</tr>
<tr>
<td>Medium</td>
<td>0.40</td>
</tr>
<tr>
<td>Low</td>
<td>0.30</td>
</tr>
<tr>
<td>Very Low</td>
<td>0.20</td>
</tr>
</tbody>
</table>

Figure 5.18 – Risk Matrix Customisable Scoring System
5.14.1 Location Assessment – Cost
Typically, costs can vary from nation to nation. The cost of resources with the required skill sets can vary depending on the demand and supply of resources in each country at a particular point in time. However, considerations need to be made for all costs, not just the cost of labour. Setup and ongoing costs to be considered can range from fixed-price services to high-speed Internet connectivity. The potential for cost fluctuations in a given market also need to be factored into the threat level, keeping in mind that, depending on the contract, an outsourcing engagement could be a five-year commitment or greater.

5.14.2 Location Assessment – Economy
Outsourcing to a country that is experiencing economic growth may provide less risk, but outsourcing to a nation with a weaker economy may prove more cost effective with increased risk. In determining the threat level, the current economic conditions need to be considered. This includes considering whether the economy is performing well in addition to the history of economic stability in the nation. Many basic economic factors that could contribute to the assessment include the strength of the local currency, exchange rates, interest rates and the overall cost of living. Offshoring to a nation with a volatile economy may present sufficient risk to perform further analysis whilst completing the Location Assessment Form.

5.14.3 Location Assessment – Politics
In assessing the political risk, there are a number of areas that require consideration in addition to the current political climate and recent trends. The nation’s history must be assessed, as well as its risk of social stability. How supportive the current government is of the economic conditions must also be considered. How aligned the current government is with the organisation’s ethics may indicate whether the organisation has potential to prosper in the region. At what point in the political cycle the nation is and whether an upcoming election could dramatically change the political landscape must also be considered.
5.14.4 Location Assessment – Communication and Language

Based on the locations identified through this research, a vast majority of the countries outsourced to do not speak English as a first language. Whether English is common as a second language and delivered at school or university level may have a bearing on how much of an issue the language barrier will be. Miscommunication also has the potential to magnify or exacerbate other risks; therefore, the quality and availability of the education system as well as the abundance of high English language proficiency requires consideration if the risks associated with communication are to be addressed.

5.14.5 Location Assessment – Location

McIvor (2010, p141) warns that although time-zone differences can often be viewed as an advantage of offshoring, there could be impacts that see clients having to put in place additional resources to manage and monitor outsourcing arrangements as well as significant challenges for the outsourcing vendor. The location of the nation being assessed also forms part of the Location Assessment process. If the customer organisation utilises a follow-the-sun model, the nation needs to be analysed to ensure it conforms to the required times. The time-zone difference between the outsourcer and outsourcer must be analysed to determine the level of risk that time-zone-related challenges can reveal. The geographical proximity of the location in comparison to the customer’s organisation may also pose some additional threat. For instance, travel time for executives to access the location during catastrophic events impacting business operations could dampen crisis efforts. Outsourcing to nearer locations should be factored into the overall threat level during the assessment process. The time zone for the location being assessed also needs some consideration within the context of the service conditions.

The client can stipulate in the contract that the vendor synchronises some of its working hours with the client’s to deal with time zone differences. (McIvor, 2010, p141)
If similar mitigations can be adopted, this needs to be factored into the rating determined for the location being assessed.

5.14.6 Location Assessment – Crime

An analysis of criminal activity is required to contribute to determining the threat level for each nation. Crime can impact both the customer organisation and the outsourcing firm, both of which will impact on the organisation’s operations. The metrics for crime should include the current crime rates, historical trends and the potential for criminal activity. The Department of Foreign Affairs Smart Traveller website can be used by an enterprise as a fast and easy method to assess a country’s overall safety; yet as part of the location assessment, detailed metrics on crime should be obtained. The Global Peace Index published by the Institute for Economics and Peace (2014) and the Crime Index published by Numbeo (2015a) may assist in measuring the country’s risk. How crime data influence the analysis of this section of the assessment form will be heavily geared by the organisation’s risk appetite for crime.

5.14.7 Location Assessment – Legal

Legal and regulatory requirements can have significant impacts. Whether there is legislation in place that could constrain the offshoring engagement as well as regulatory requirements and restrictions should be factored into the assessment. For instance, if the nation has data-retention requirements that must be met, these requirements could contribute considerable costs to the venture and should be included in this risk assessment. Some legislation could trigger privacy concerns, limiting the options available to mitigate any risks. A strong legal framework can be critical in protecting an enterprise. A sound contract in the absence of a strong legal system to enforce the contract will not be sufficient to protect the enterprise during contract disputes and challenges. Whether legislation is in place to protect the firm’s IP rights and a strong legal system to support its rights should also be factored into the analysis that is being completed.
5.14.8 Location Assessment – Terrorism
Terrorism has the potential to impact on business operations and therefore is included in the location analysis. Measuring the risk associated with terrorism can be difficult as events can be fairly unpredictable, yet major when they occur. Whether the nation has a history of terror and the current terror-threat level for the country should be considered in scoring this section. Whether there is a likelihood of terror attacks may also provide assistance in measuring the overall threat level using the assessment form. The Global Terrorism Index Report published by the Institute of Economics and Peace (2014) can be leveraged to assist in capturing quantitative metrics to measure the probability of terrorism in conjunction with other qualitative sources such as the Department of Foreign Affairs Smart Traveller website.

5.14.9 Location Assessment – Environment
A variety of environmental factors could pose a significant risk to business operations and as such contribute to the location analysis.

Natural disasters like the 2011 earthquakes in Japan or the floods in Thailand are somewhat predictable in the sense that Japan is a volcanic region and Thailand is prone to flooding. But the scale of the 2011 events proved more extreme than most risk managers could account for. The Honda factory in central Thailand was under 15 feet of water at the high point of the flooding. This incident was minor compared to the March 11 earthquake, tsunami, and subsequent nuclear crisis that engulfed Japan. Toyota suspended production of the Prius in Japan after this event, losing 140,000 badly needed vehicles. (Stank et al., 2015)

Natural disasters such as earthquakes, cyclones, tsunamis, floods and volcanic eruptions are just some of the events that need to be considered as part of this analysis. The environment that the nation is located in does not only have the potential to disrupt human resources – any hardware and software located in the country could be placed at risk if a natural disaster were to occur.
5.14.10 Location Assessment – Infrastructure

Carmel and Tjia (2005) raise two risks that are more likely when offshoring – contractual risk and infrastructure risk. They advise that “the dependability of the communications infrastructure is lower in some offshore destinations” and as the probability of failure may be higher companies need to “mitigate this risk by securing multiple communication links to the offshore unit or provider” (Carmel & Tjia, 2005, p48). Infrastructure forms an important part of the assessment as it contributes to the location’s suitability. For developing nations, confirmation that sufficient funding is being invested to improve pain points in the nation’s infrastructure should form an important part of the rating for this section. The quality of public infrastructure such as roads and rail will assist in determining whether the country poses a tolerable amount of risk. Most importantly, telecommunications and data-network infrastructure is a critical dependency for most outsourced operations, yet adequate services may not be available in some countries.

5.14.11 Location Assessment – Records

As part of the analysis for this section, a rating should be determined for the availability of public records to sufficiently complete accurate background checks. Background checks may need to be completed for criminal convictions and employment history checks to determine if resources are suitable. For example, organisations in the finance sector, such as banks, may feel the need to have increased control over the selection of resources, which is neither as effective nor as possible in some nations.

5.14.12 Location Assessment – Health Care

The quality of the medical system and the availability of health care are assessed in this section to determine the overall threat level posed by the nation’s health care. Affordability of health care should also be factored into the assessment. Consideration is required for both the local resources as well as visitors that travel on business to the region on behalf of the customer’s organisation. As adopting an offshore outsourcing model extends the organisation’s operations to the offshore location, the employees of
the outsourcing firm in that location become a contributing factor to the success of the enterprise. The health and wellbeing of employees of the outsourcing firm can influence the quality of the service provided. Poor healthcare systems can also “affect quality of life, which may deter many employees from the West moving to India for extended periods, making knowledge transfer and control more difficult (Vagadia, 2012, p86). This has the potential to impact on the effectiveness of the outsourcing venture and requires consideration when selecting a suitable location that aligns with the organisation’s risk appetite.

5.14.13 Location Assessment – Quality

Throughout the literature review, quality is the single most raised threat to outsourced operations. Dhar (2009, p252) suggests that quality and reliability form some of the “hidden costs involved in outsourcing”. Furthermore, eighty-three (83) per cent of people surveyed advised they are concerned about quality output when outsourcing.

Many service processes are characterised by heterogeneity, as both the vendor and customer interact in the service delivery process, which creates potential for variation in service quality. (McIvor, 2010, p39)

The nation’s track record for quality output and its reputation for quality controls and sound practices must be reflected on in scoring this particular section. The risks associated with inferior product quality standards “increase exponentially when the value chain transitions from a vertically integrated, self-contained set of processes to a geographically dispersed linked set of relationships” (Lynch, 2008, p28). With the risk of quality output increasing, the organisation’s ability to implement sufficient quality-control measures should be considered carefully in assessing this section of the Location Assessment.

5.14.14 Location Assessment – Resourcing

An analysis of skilled resourcing should be completed to ensure the organisation is comfortable with the current availability and future labour force of the nation. Whether there are sufficient students commencing studies in the region to facilitate industry
growth and whether there are sufficient entry-level roles in the areas being outsourced to should form part of this analysis. The size of functions being outsourced, complexity and amount to be invested need to be taken into account when analysing the capabilities and competencies available.

5.14.15 Location Assessment – Back-out
The venture back-out potential ensures that the organisation can quickly and easily withdraw from the country. The speed at which the people and infrastructure can be withdrawn is important in order to determine whether the customer has potential to relocate operations if the conditions were to change. Physical access as well as proximity to public transport and sound airports could assist an organisation in ensuring it remains agile and therefore may offset some of the location-based threats that are at risk.

5.15 Evaluation Cycle
The Location Assessment Tool must be re-evaluated on a regular basis to re-assess and validate the outsourcing decision. This is important because environments change so rapidly that they are susceptible to rapid and prolific change. The four fluctuations identified through this research encompass the four areas that are susceptible to significant fluctuation in an outsourced setting. The four fluctuations are as follows.

- Benefits
- Climate and conditions
- Costs and pricing
- Performance and quality

An explanation of the four fluctuations depicted in Figure 5.19 has been provided below:

**Benefits** – The benefits associated with an outsourcing venture may fluctuate depending upon the agreement in place, the committed deliverables and the function
outsourced. Following the evaluation cycle to re-assess the location regularly will validate that the benefits being obtained by the firm continue to be realised and remain intact. A deviation in benefits may prevent the firm from solidifying the desired outcomes.

**Climate and conditions** – Any changes in the ecosystem could impact the overall threat level of the location. As the rating for a location is only valid at the particular time of assessment, changes to the economic, political and ecological climate could be prone to deviation throughout the engagement. Each location will be prone to fluctuations in the climate at different rates; therefore how delicate the location is will need to be considered as part of the assessment.

**Costs and pricing** – Fluctuations in pricing are possible across a multitude of cost areas. The costs considered as part of the location assessment could deviate, impacting the return-on-investment analysis that was completed prior to the engagement commencing. There may also be hidden costs such as unexpected operating costs and the cost of unknown risks that eventuate, which may need consideration outside of the planned contract pricing.

**Performance and quality** – Until the venture commences, it may be difficult to measure the quality of the anticipated outputs. The outputs may not be as expected or the overall performance of the country or region may deteriorate based on supply, demand and capability of resources, thereby creating a fluctuation in the overall performance of the country or region.
The evaluation cycle for each location may differ depending on the impact of the four fluctuations. The process for evaluating and re-evaluating the location assessment involves four stages as depicted in Figure 5.20 below. The first stage involves the evaluation of the location utilising the Location Assessment Tool. Once suitability is determined and a location is selected, the outsourcing engagement should be watched and documented as part of the monitor stage. Performance metrics obtained throughout the monitoring stage can be utilised to form the review process in the third stage of the evaluation cycle, the review stage, ensuing that the location assessment is always up-to-date and a reflection of the current conditions. The final stage of the cycle, the act stage, is the stage in which the levers and controls established could be adjusted to aid with continuous improvement.
The duration of the evaluation cycle should be determined based on the location’s susceptibility to the four fluctuations. The Asia Pacific region, for instance, is considered to be quite mature, as it has been an outsourcing destination for a number of years. Therefore an annual review cycle may be sufficient to identify increases in exposure to risk as a result of the four fluctuations. The evaluation cycle for locations in developing markets such as Latin America or more volatile markets such as Africa and the Middle East may have a requirement for more regular reviews. The organisation conducting the assessment should determine the most suitable duration for its intended reviews, based on its particular circumstances, experience with offshoring and its own risk appetite.

5.16 Context of Location Assessments
An important part of any organisation’s outsourcing strategy must be to conduct location assessments to understand and make an informed decision on which nation or region to outsource to. However, outsourcing firms that operate with a presence across multiple nations and sometimes regions can complicate the assessment. With more and
more vendors adopting follow-the-sun style operating models, which involve resources throughout multiple regions providing services at different times to allow for 24-7 services, the likelihood that an enterprise will outsource to a firm solely based out of one nation is increasingly unlikely.

Overby (2013b) advises that:

... many IT service providers are now multinational with the ability to shift work between delivery centres, so looking at location in conjunction with supplier specifics provides a clearer picture of overall risk.

In order for the benefits of the location assessment to be maximised in this situation, all locations need to be assessed in conjunction with the provider. Assessing the locations within the context of the provider will allow an enterprise to effectively measure the risk based on the amount of work allocated to each location as well as the type of work likely to be delivered within that nation. For instance, in outsourcing a software development function to a multinational firm, the enterprise must ascertain visibility from the outsourcing firm as to how much of the development is likely to be completed in that particular location. If the outsourcer only intends to assign work to other nations for a workload-balancing purpose, the enterprise must be cognisant of the percentage split between the locations in order to factor this information into their location-assessment calculations, thereby ensuring their analysis is indicative of the correct probability of occurrence for each risk. In some instances maintaining a split of resources across multiple nations may improve the potential risk, acting in a way as a contingency in the event of an incident.

In some instances introducing other nations could raise the risk level and this is something that should be considered by each enterprise throughout the assessment process. Establishing a model based on a split across two nations could have negative impacts if the two are prone to the same risk. For example, a single tsunami could disrupt services split between Malaysia and Singapore due to their geographical proximity. If the introduction of a second (or third and fourth) nation is unavoidable,
selecting nations with better risk profiles for the element in the strategic pillars (i.e. economic stability) may assist in diversifying whilst reducing the exposure to risk. Although deliberately splitting the venture across multiple locations may assist in mitigating some of the location-based risks, it can introduce additional risks because of the complexity introduced in operations, processes and the relationship with the vendor. Although the location-based risks may have been mitigated, these additional risks introduced form part of the residual risk that enterprises must monitor to ensure their mitigating actions are effective enough in reducing the overall risk level of the outsourced function. Further analysis of the potential impact of residual risk is detailed in section 5.18.

5.17 Vendor Assessment

Fifty-two (52) per cent of those surveyed indicated that they outsourced technology solutions such as IaaS, SaaS, and so forth. A further eighteen (18) per cent indicated that they were currently looking to outsource such a technology. With such a large proportion of Australian organisations outsourcing these sorts of technologies, vendor assessments should form an integral part of selecting the firm to outsource to. Just as an assessment of the location needs to be conducted prior to selection, assessing the vendor is vital to ensuring the provider is aligned with the risk appetite of the organisation. The outsourcer should also be assessed for competitive behaviour – that is, the potential for the outsourcing firm to expand into the market of the client. If there is potential to expand, or any blurred segregation between the functions of the firm and the outsourcer, this should be incorporated into the decision and the relevant risk-mitigation strategies formulated. Any conflict of interest should be assessed to ensure the outsourcing firm acts in the best interests of the client. Apple famously engaged Microsoft for development of the Macintosh computer:

While developing the system for Apple, Microsoft was also developing Windows for itself; the two competing systems appeared within a short time of each other
with the Mac debuting first in early 1984 ... and Windows in early 1985. (Cross, 2013, p543)

Such a competing interest from another entity has the potential to destroy an enterprise.

With multi-tenancy-based solutions such as cloud computing on the rise, the potential that an enterprise will be sharing infrastructure and applications with another enterprise is increasing rapidly. In selecting a vendor from which to obtain these services, consideration should be given to the potential to share infrastructure and applications with a competitor. The organisation should seek to obtain visibility of other tenants to determine whether a likely security breach could result in a firm being exposed to a competitor, and ensure that instance separation has been adequately established. The organisation throughout the decision-making process should determine whether this risk warrants a security review that could be incorporated into other cloud-sourcing-related activities and, if required, build the relevant requirements into outsourcing contracts.

5.18 Residual Risk

Roebuck (2012, p273) defines residual risk as:

... the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied.

It is formed from the risk that remains after risks have been treated or mitigated. The risk that remains can pose an insurmountable threat to a business and therefore requires attention from the enterprise to minimise exposure. Monahan (2008) clearly articulates the importance of residual risk, stating that:

... residual risk should be the main focus of the enterprise risk manager as residual risk drives the distribution of possible outcomes and it is the distribution of possible outcomes that we are aiming to understand and manage.
If residual risk is required to be a priority of enterprises, the residual risks as a result of outsourcing and offshoring, intrinsic practices need to be embedded into the organisation’s operations. An organisation can no longer assume that the treatment of the initial threat was sufficient to minimise what could be an enormous impact.

With the fact that the outcome of a risk is largely unknown, an enterprise should be addressing all potential hazards at both the time of treatment and the residual threats if an enterprise is to remain truly in control of their environment. Yet only seventy-two (72) per cent of research participants indicated that their organisation actively mitigated all risk with two (2) per cent indicating they did not mitigate risk and over twenty-five (25) per cent indicating their organisation only mitigated risk sometimes. This essentially means that over twenty-seven (27) per cent of enterprises are not actively treating all initial risks; therefore, it is impossible that all residual risk is being addressed. This revelation indicates that an enormous number of businesses in Australia are continuing to operate whilst their organisation’s success is in serious jeopardy. Some may continue to operate in this mode successfully for a considerable period, but they may all be one unmitigated risk away from disaster.
6. Outsourcing and Intellectual Property

6.1 The Threat of Outsourcers

In outsourcing and offshoring, there are a vast number of risks that any party should seek to mitigate when establishing the endeavour. Embarking on an outsourcing venture could uncover a number of new risks with potential to impact on a business, but they could also be exposed to risks from the outsourcing firm itself. Risks can emerge as a result of anything from the outsourcer’s governance procedures to communication to skill level and capability. One such example arose in 2009 when US-based telecommunications provider T-Mobile experienced a significant outage due to an outsourced service. It seems T-Mobile outsourced part of its service to Danger, a Microsoft-owned company, which in turn is rumoured to have outsourced its Storage Area Network (SAN) to Hitachi. As a result of a failed attempt to upgrade their SAN, and their failure to complete a backup prior to the upgrade attempt, the pair was reportedly responsible for the loss of T-Mobile customer’s personal data consisting of calendar entries, contacts and photos (Conneally, 2009). In outsourcing to Microsoft/Danger, T-Mobile relinquished most of its control over the risk-management practices (such as performing a backup) associated with its environment. Could the loss of control have been exacerbated by the introduction of yet another outsourcer (Hitachi) into the equation? Such a high-impact, high-profile blunder is likely to have damaged T-Mobile’s image, as well as individual users as a result of the data loss.

Rosenberg and Mateos (2011, p73) advise that cloud architectures in particular “create more opportunities for misconfiguration and malicious conduct”. Conversely, this could be the case for all outsourced operations. Outsourcing often places the outsourcing firm in control, and it’s very probable that its control could be misused. Organisations should seek to mitigate all of the many potential threats that an outsourcer may pose; however, the potential for malicious employees provides the greatest unease. If a malicious employee in an outsourcing firm has such great access to wreak havoc – and India, which is Australia’s most outsourced-to nation, has
inadequate public records to satisfy thorough background checks – organisations should be gravely concerned. It may be high time enterprises contemplating an outsourcing engagement consider whether or not the function being outsourced provides sufficient benefit to justify the exposure of additional risk.

All organisations have different ERM practices but there is little evidence to suggest that considerations are actually being made to compensate for the risk. Most of the literature on outsourcing focuses on the benefits; therefore, it is no wonder that the significant threat of the outsourcer itself is receiving very little attention in practice. Of the research participants that contributed, only seventy-two (72) per cent indicated that their enterprise took action to mitigate the risks inherent from outsourcing. This reveals a significant gap whereby enterprises are entering into outsourcing ventures without considering how to manage the risks inherent in outsourcing. Arbitrarily deciding to outsource purely on the basis of cost savings is surely a recipe for disaster. Taking a more farsighted approach must be more prudent in the long term if an organisation is to continue to remain successful. There is significant potential for an outsourcing firm to pose a risk to its client. Frost et al. (2001, p175) cite specific examples of outsourcers impacting their clients:

  Potential operational risks have already been made apparent. For example, in an aerospace company outsourcing arrangement, a subcontracted employee temporarily disrupted its e-mail system through malicious behaviour.

Outsourcing providers have the access and ability to disrupt a business; however, an enterprise will have reduced visibility and control whilst outsourcing. Therefore it could be considered that they have incurred increased risk with an inability to effectively control and mitigate the risk.

6.2 The Illness of Dependency

Vagadia (2007, p16) warns of a loss of control of day-to-day management and the potential to become excessively dependent on the service provider for performance. Therefore, outsourcing to another entity and developing the “illness of dependency”
could leave an organisation in a position where the client’s performance is controlled by the outsourcing firm. McAlpine (2000, p89) describes Machiavelli’s theory on the outsourcing of military forces to third parties:

Auxiliary troops, which are the second kind of useless soldier, are those sent when you ask a powerful ruler to help to defend you with his troops. Pope Julius did this recently when, having observed his mercenary force’s poor performance during the Ferrara campaign, he turned to auxiliaries and arranged for the soldiers and armies of Ferdinand, King of Spain, to help him. These troops can be useful and effective in their own right. However, they are almost always harmful to those who have recourse to them, as if they lose, you are undone; if they win, you become their prisoner.

Machiavelli’s theory seems plausible in today’s business context. When utilising outsourced labour, it is obvious how an enterprise may be seriously affected if the engagement is not successful. However, Machiavelli suggests that even if the outsourcing engagement is successful, the firm could be locked in, and a “prisoner” to the outsourcing provider. Developing a dependency on an outsourcing firm could limit the organisation’s ability to make strategic decisions, control its operations and, finally, govern its fate. Relinquishing this control whether consciously or unconsciously will likely have a detrimental impact on the enterprise. The impact may not necessarily bring down an empire in today’s world, as Machiavelli predicted, but the fate of the organisation may be just as grim.

McIvor (2005, p196) provides considerable analysis of outsourcing strategies that could result in dependence on the provider:

Companies can become overly dependent upon opportunistic suppliers due to a lack of awareness of the issues involved in understanding the supply market. Therefore, when considering outsourcing an activity, it is crucial that a company has an in-depth understanding of the relevant supply market. If supply markets were totally reliable and efficient, companies would outsource all business
activities except critical activities that are regarded as a source of competitive advantage. However, most supply markets are imperfect and the buyer must incur some level of risk depending upon the characteristics of the supply market.

Yet to what level should the risk analysis be administered to adequately minimise the risk of dependency that is evident from the use of any outsourcing firm?

Could it be possible that some enterprises today may not even be conscious of the dependency developing? Thirty-eight (38) per cent of participants advised that they believed their organisation could be developing a dependency on one of its outsourcing providers, as indicated in Figure 6.1 below. Sixty-two (62) per cent, however, indicated that they believed their organisation was not developing a dependency on its outsourcing firms. Is it possible that enterprises are developing a dependency and the professionals surveyed are none the wiser? Further analysis was completed as part of this research to determine if the most damaging characteristic of this illness of dependency could be the failure to consciously identify the affliction.

![Figure 6.1 – Becoming Dependant on an Outsourcing Firm](image-url)
6.3 Quality and Performance Degradation
Outsourcing can have a negative effect on quality and performance output. Overby (2003, p2) suggests that an enterprise can experience a significant reduction in performance as a result of outsourcing, advising that in the software-development space, for example, offshore vendors often lack the experience in comparison to onshore firms. Overby advises that IT organisations transitioning offshore will experience, on average, a 20 per cent decline in their application development efficiency throughout the first two years of their contract (Overby, 2003, p2). Considering the primary motivation for migrating operations offshore tends to be to reduce costs, this potential reduction in efficiency needs to be factored into the anticipated savings and return-on-investment estimates. This will ensure the enterprise has accurately measured the benefits of establishing the outsourcing venture and can be used as a benchmark to measure the performance of the desired outcomes. An enterprise should have a mechanism to monitor and report on the performance of the service that has been outsourced. This mechanism will allow the organisation to identify and mitigate any performance degradation during the contract period.

6.4 Intellectual Property Rights
As an outsourcing model involves the extension of an enterprise’s operations to another entity, there is potential for an organisation to endanger some sort of IP throughout the course of the engagement. Over eighty years ago, Griffith (1935, p78) noted the impact that employing outsourced soldiers had on armies since the time of Antigonus Gonatas, the Greek emperor that ruled the ancient region of Macedonia circa 300 BC. Employing barbarian mercenaries to fulfil short-term tactical requirements was a tactic used by many ancient armies. Griffith (1935, p261) advises that Roman generals such as Marius established contracts whereby grants of land or bonuses were paid to outsourced mercenaries. Griffith (1935, p78) also explains that the barbarian mercenaries utilised by the Macedonian armies also expected grants of land upon their discharge. Could it be possible that these ancient contractors, which were recruited as short-term, cheap labour, became so ingrained in their employer that
the only way to discharge them without being impacted by the IP they had acquired was to offer them an expensive settlement? It is more than likely, considering the number of organisations that outsource, that a similar impact of IP loss could burden an enterprise of today. Over fifty (50) per cent of respondents are currently concerned about an outsourcing firm absorbing their IP based on the study conducted of ANZ enterprises. With over half of respondents indicating they are concerned, it is evident that IP loss is a legitimate threat in the IT industry. There are a number of considerations that should be made in weighing up the decision to adopt an outsourcing model.

The service provider’s track record for protecting intellectual property is very important, because the foreign company will have less control over intellectual property protection procedures. Along with the adequacy of enforceability mechanisms, it is important to understand the country’s legal framework for intellectual property protection, such as moral rights and ownership assignment requirements. (Sharma, Sharma & Rajasekaran, 2012, p84)

Selecting an offshoring nation that has a legal framework that protects IP may ensure a firm has the mechanisms available to contest any loss of IP, but this makes two very critical assumptions: 1) that the enterprise has the legal recourse to pursue damages and 2) that the enterprise actually knows it has lost its IP. Ensuring contracts entail the necessary clauses to prevent IP theft and mitigating the risk of IP loss by establishing ERM practices to monitor the outsourcing engagement may prove to be much safer options for the enterprise in the long term.
IP is not just a 21st century concern. Disagreements are often played out publicly in courts as organisations attempt to defend themselves against IP theft. IP risks can affect even the greatest of organisations. Cisco filed a lawsuit against Huawei, in which the US-based Cisco accused Chinese technology giant Huawei of stealing its IP. Huawei suggested that its “brilliant engineers” were responsible for producing its sophisticated high-tech equipment, challenging the accusation that Cisco’s IP had been stolen. The lawsuit was dropped in 2003 and Cisco settled with Huawei (Karabell, 2009, p177), evidence that not even the largest of global conglomerates is immune to the pernicious theft of IP.

China itself has also long received criticism for its stance on IP.

In the negotiations surrounding China’s entry into the WTO, the issue of intellectual property was never far from the surface. Western companies had long complained that while China’s market was hugely attractive, it came with a cost. (Karabell, 2009, p175)

With China being ranked in the top five of most outsourced-to countries, the potential for the loss of IP to Australian organisations is great. Yet McIvor (2010, p100) takes
this theory one step further in linking the loss of IP to the potential loss of competitive advantage:

In some contexts, the creation of a service involves the development of IP. Where this IP is valuable and important to competitive advantage, the client has to ensure that the sourcing model and contract protect its IP rights. The client will have to incorporate additional control mechanisms to ensure that employees cannot disclose any valuable information to competitors.

If there is real potential for IP loss, and the IP relates to the organisation’s competitive advantage, the potential for these risks to severely impact and possibly destroy an enterprise is obvious.

**6.5 Intellectual Property and Competitive Advantage**

Competitive advantage lies at the heart of any successful firm. Developing a plan to compete with competitors is primary to any organisation establishing a successful strategy.

The firm must be concerned not only with profitability in the present and growth in the medium term but also with its future position and source of competitive advantage. Firms must think about how they will compete when their current strategies are copied or made obsolete. (Vibert, 2004, p50)

Yet why would any firm risk losing their competitive edge? Firms are at risk of having their competitive advantage lost to their outsourcers gradually through stealth and absorption of their competitive strategies, making organisations that outsource considerably more vulnerable to this occurrence. Vibert (2004, p50) describes how competitive advantage can only be sustained if the capabilities creating the advantage are supported by resources that are not easily duplicated by competitors. Losing your competitive advantage to an outsourcing firm increases the likelihood of the capabilities sustaining your competitive advantage will be duplicated, as they are no
longer within the ownership, visibility and control of the enterprise; they are now in the possession of another entity.

During the time of Vespasian, circa 70AD, part of Rome’s grain supply was outsourced to and controlled by Alexandria (Grant, 1970, pii). With grain forming a vital part of the Roman Empire’s food supply, sourcing the grain supply from an offshore location was a potentially risky endeavour. Like the ancient empires, today’s organisations outsource infrastructure and services in the form of solutions such as IaaS and SaaS. In doing so, these enterprises regularly outsource the most critical functions of their business. Call centres form an organisation’s front-line providing the channel that is utilised to interact with customers and can be vital to making an organisation successful. Back-end IT services form the backbone of an enterprise’s ability to do business, often forming the face of an enterprise through its website, associated interaction points and transactions with customers. Although key to competitive advantage, these critical functions and interaction points are often the most frequently outsourced; contrary to this, this research suggests that inadequate attention is being focussed on mitigating the risk of IP loss. Figure 6.3 outlines the proportion of enterprises that implement measures to protect against the loss of IP. While 46.8 per cent of respondents indicated that their enterprise had established measures to protect against the loss of IP, nineteen (19) per cent specified that their organisations had not put measures in place. Over thirty-four (34) per cent advised that they did not actually know whether their organisation had established measures to protect against the loss of IP. With less than half of the individuals surveyed indicating that their enterprise actively established measures to protect itself, there is potential that more than half of Australian enterprises’ intellectual capital could be at serious risk.
Figure 6.3 – Establishing Measures to Protect Against Loss of IP

Solli-Saether and Gottschalk (2010, p130) highlight the potential for hidden costs to easily undermine the anticipated benefits when outsourcing. This stems from a loss of control whereby a firm allocates responsibility for its IT operations to an outsourcing firm, affirming control of the client’s IT operations.

If the organisation lacks the expertise to negotiate a sound contract, the firm’s dependency on the vendor might result in high costs or loss of control over technological direction. Firms should be especially cautious when using outsourcers to develop or to operate applications that give it some type of competitive advantage. A firm is most likely to benefit from outsourcing if it understands exactly how the outsourcing vendor will provide value and can manage the vendor relationship with an advantageous benefit/cost ratio both on contract paper and in reality. (Solli-Saether & Gottschalk, 2010, p130)

This suggests that managing the client–vendor relationship is the key to mitigating the risk to IP and competitive advantage. Most importantly, the nineteen (19) per cent of respondents that had not put measures in place to prevent the loss of IP, and the thirty-four (34) per cent that did not know if their enterprise had established any
measures to protect itself, should seek to maintain a close relationship with their outsourcing provider to aid in both maintaining control and monitoring any IP leakage.

Bryce (1871) outlines how the barbarian mercenaries grew to form a significant part of the Roman army:

This was found even more convenient by the hirer than by the employed; till by degrees barbarian mercenaries came to form the largest, or at least the most effective, part of the Roman armies.

The barbarians formed the most effective part of the Roman armies, just as enterprises of today outsource some of their most critical parts of their business, key to their competitive advantage. Furthermore, McAlpine (2000, p85) describes how the Thebans from the Greek city-state of Thebes appointed Philip of Macedon as their Captain of the Soldiering. Philip of Macedon then led the Thebans to victory and shortly after took away the liberty of the Thebans. Through his appointed role, Philip of Macedon posed a greater threat to the Thebans than their assumed enemies. This is no different from what can occur in the modern world when outsourcing to a firm. Apple suffered significant intellectual property losses when the firm they were outsourcing to copied the designs for their operating system. “Apple outsourced its operating system to Microsoft, which then became a serious competitor” (Di Biase, 2014, p160). After separating from its outsourcing engagement with Apple, Microsoft became Apple’s biggest threat. By allowing outsiders to establish an influential role in your enterprise you potentially run the risk of allowing the outsiders to gain inside knowledge of your organisation, suggesting that outsourcing firms may actually pose a greater risk to an organisation’s prosperity than its actual competitors.

6.6 Competitive Mitosis

6.6.1 Definition

*Competitive mitosis* is a new term coined in this research to describe the process by which an outsourcing venture allows for knowledge and IP to be replicated from an
organisation to another party. It is based on the concept of mitosis whereby existing cells are split producing two new cells. The lifecycle for this process includes three distinct stages, demonstrated in Figure 6.4 below.

![Figure 6.4 Competitive Mitosis Lifecycle](image)

The first stage of the competitive mitosis process is named the engagement stage, depicted in Figure 6.5.

![Figure 6.5 – Competitive Mitosis Stage 1](image)

During this stage of the process, two organisations join through sales activities to establish the outsourcing venture. The commercials and contractual arrangements are
finalised and the relationship between the outsourcer and outsourceree is established. The outsourcing engagement has effectively extended the customer’s enterprise to the outsourcer’s enterprise. Depending on the operations of the customer and the scope of the outsourcing venture, the outsourcer is now in a prime position to commence absorbing the customer’s IP, whether deliberate or not. As the organisations continue to do business together and the merger results in a new ecosystem being established, the outsourcer will begin to acquire knowledge about the customer’s operations, commencing the replication stage depicted in Figure 6.6.

Throughout this stage, the channel is opened for the replication of IP, and this can occur without either party realising that the process is taking place. If the business functions outsourced are critical to competitive advantage, the ability of the customer to compete can be shared with the outsourcer. Like a parasite absorbing from a host, intellectual capital can be absorbed to the extent that the host allows. Robust processes, quality checks, solid contracts and a strong legal system to enforce the contract could prevent this process from occurring. Yet it is quite possible that the organisation’s advantage could be completely absorbed or replicated, resulting in serious repercussions in the subsequent and final stage – the separation stage.
The separation stage, depicted in Figure 6.7, as the name suggests, commences with the separation of the parties. Either party may establish separation through the completion or cancellation of the outsourcing arrangement. During this stage, the organisations go their separate ways, resulting in intellectual capital being retained by the outsourcing firm. Although there may not be malice intended to commence with, knowledge being transitioned from the customer to the service provider is unavoidable. As a result of having undertaken the venture, detailed knowledge of the customer’s operations now resides with another entity. If the venture involved outsourcing a critical component of the business, which is linked to competitive advantage, the implications could be much greater. Not only would the outsourcing firm have detailed knowledge of the customer’s operations, the outsourcer could use that information to compete in the marketplace for future customers. Should the firm decide to establish an outsourcing engagement with the customer’s competitor, there is a risk that the competitor could have a greater capacity to compete in the marketplace with the capital absorbed.

It is relatively easy to conceive how this could impact on an enterprise in practice. Organisations regularly outsource call-centre operations to firms based in India, China and the Philippines, among other locations. If the call centre is responsible for sales and their method and approach for enticing customers to purchase products provides the organisation with a competitive advantage, absorption of that ability into the
service provider could impact on the organisation’s competitive edge. The ability of an organisation to differentiate itself from competitors could be at risk, completing the lifecycle of competitive mitosis and cannibalising the costs saved in establishing the outsourcing venture – the very reason the business outsourced in the first place.

6.6.2 Identifying Competitive Mitosis
Breaking the cycle of competitive mitosis starts with identification. It is important that an organisation identifies the engagements in place that could pose a risk. If the engagement has already been established, determining where in the cycle the venture is at is critical to mitigating the risk. The organisation should go through a review process to determine which business functions have been outsourced and precisely what information could be absorbed through the established channel. Those functions identified as contributing to competitive advantage should be mitigated as a priority. Through the identification process, the business will be able to determine what IP can be absorbed in addition to determining how quickly the absorption process can take place. If absorption is fragmented, identification on whether the portions of information can be amalgamated to form a competitive edge should be conducted wherever possible to fully assess and understand the impact. The more information gathered through the initial triage activities, the greater chance of addressing the information leak. Ensuring the traits of competitive mitosis are well known throughout an organisation's management will ensure that the process is stopped and measures are put in place prior to separation, the phase where the majority of damage occurs.

6.6.3 Mitigating Competitive Mitosis
The approach for mitigation is heavily dependent on which stage of the process an organisation is at. It is quite possible that an organisation may have multiple engagements in place at different stages within the process; therefore, the treatment must be determined based on the threat. Occurrences identified in the engagement stage may be mitigated through contractual arrangements and adjustments to strategic direction. Changes to strategy may involve outsourcing a different part of the enterprise or ensuring that sufficient functions remain within the organisation to limit (and
monitor) the leakage of IP. Supervisory processes will assist the enterprise to oversee the outsourcing engagement to both monitor and track any potential loss of IP. By ensuring outsourced operations are supervised by internal management, any potential breaches will be easier identified. Establishing quality assurance processes can also assist the venture to go ahead whilst minimising the risk of IP loss. This is done through establishing QA (quality assurance) processes, which involve the organisation’s internal resources monitoring the output of the outsourcing firm’s artefacts and deliverables, leading to improved visibility and traceability. Mitigation during the replication stage may also be possible through establishing processes to prevent the absorption and if possible retract any information and knowledge that may be in transit. Revoking access and retaining control may ensure that the impact is limited, prior to any loss of IP occurring, malicious intent or potential skulduggery emerging. Recalling artefacts and data may be possible; however, once the knowledge has been transferred into the minds of resources, the intellectual capital may be lost.

The single, most important mitigation method for an organisation at risk of competitive mitosis is to avoid outsourcing critical business functions to third parties. It is vital to bear in mind that outsourcers are external parties and although a particular engagement can create a joint venture whereby the demarcation points between organisations can be blurred, outsourcing firms are shared service providers and by their nature will be providing services to other parties, both now and in the future.
7. Supply Chain Detriment

7.1 Definition

The perceived risks associated with outsourcing and offshoring have been covered extensively in the literature, and the impact of not adjusting ERM practices has been covered at length in previous sections. However, it is important that the outsourcing firm is not the only entity considered when establishing risk-management practices for outsourcing. As it is common in the IT industry to outsource and subcontract, an enterprise needs to be aware that risks may become evident further down the supply chain. Moreover the number of risks may be more numerous as the length of the supply chain increases and additional subcontractors are introduced. As the supply chain increases, the enterprise’s ability to mitigate the risks associated with outsourcing may also deteriorate. Supply-chain detriment is a new concept identified through this research, whereby an enterprise outsources a service or business function to an outsourcing firm, which in turn subcontracts part or all of the work to another entity. In this scenario, the outsourcer is effectively outsourcing to another party, introducing additional risk with even less visibility. It can be challenging for an enterprise to obtain adequate visibility to assess risk at the best of times; introducing another party will surely dampen visibility further. The more parties that are introduced into the relationship, the less control and visibility the organisation will likely have on its outsourced operations. This can intensify the level of risk associated with the venture, not only by introducing more risks and greater potential for IP loss, but also through reducing the organisation’s ability to identify and exercise control over the multitude of risks described in previous sections. With more parties involved in delivering the outsourced function, the probability that a risk may eventuate could be significantly increased. Furthermore, the risk assessments completed in establishing the venture may be invalidated by the introduction of a third or even fourth party, potentially residing in a completely different location to the outsourcing firm the venture was established with; introducing new, unmitigated location-based risks that were not considered as part of the Location Assessment process.
7.2 Identifying Supply Chain Detriment

Supply-chain detriment can be identified through its multiple characteristics. Firstly, the subcontracting of work to multiple parties can be identified through a review of the supply chain and associated recruitment practices of the outsourcer’s organisation. This should be followed by a review of the ERM practices currently in place to determine whether or not the organisation has addressed the risks inherent from outsourcing. In the event that an outsourcing firm has subcontracted or outsourced components of the engagement, and the organisation has not considered the risks that may be incurred further down the supply chain, it is very likely that the organisation could be experiencing supply-chain detriment. As a result, the symptoms that may be apparent could include a failure to mitigate risks associated with the location of all outsourcing parties in the chain, short-sighted decision-making when assessing threats that could impact on the business and poor visibility of the current operations and how the
services are being delivered by the outsourcer and its subcontractors. If an outsourcing firm is unwilling to cooperate with the investigation and is generally unwilling to provide information on how it sources its resources to deliver the outsourced function, an organisation will be unable to determine how significant the risk is and may need to take action in mitigating risks, assuming the worst.

7.3 Mitigating Supply-Chain Detriment

Mitigation of supply-chain detriment can occur through the implementation of a number of treatments to mitigate risk. Most importantly, establishing thorough contracts with the outsourcer can ensure that the terms of the agreement are relevant to the outsourcer and all of its subcontracted partnerships. Tight IP clauses will ensure that the enterprise is not at risk of IP theft from any of the subcontracted parties and can be used to ensure that visibility is maintained throughout the engagement. Robust processes to manage quality and maintain control of operations can also assist in ensuring that any new threats incurred through the supply chain are identified and treated in a timely manner. Quality-control processes allow the enterprise to establish standards and monitor compliance against these standards for the quality of outsourced outputs. This can be achieved through spot checks, audits or more stringent management of, and involvement in, outsourced functions. Ensuring that actions address the threats that could be experienced from all known parties in the supply chain will ensure that adequate mitigation coverage is established. This will also need to take into account the locations of the various (and potentially disparate) resources that could be working on the venture. For instance, mitigating risks associated with natural disasters in Asia may not be effective if the outsourcer has also subcontracted to an organisation located in Africa. In this scenario further risk assessments and mitigating actions will be required to address risks from Africa, if the organisation is serious about limiting its exposure to all threats.
8. Barbarian Syndrome

8.1 Definition

*Barbarian syndrome* is a new discovery identified through this research. It describes an affliction whereby an enterprise, in outsourcing parts of its business to an outsourcing firm, unwittingly introduces a threat that could lead to the demise of the enterprise. Since ancient times, military duties have been outsourced to barbarian mercenaries. During the time of Alexander the Great, the proportion of Greek to barbarian mercenaries employed by Alexander’s army was perhaps as high as 10:1 (Griffith, 1935, p79). In the army of Perseus, the King of Macedonia in 171 B.C., the ratio of Greeks (including Cretans) to barbarians was roughly 4:5 (Griffith, 1935, p79). With such a large proportion of these armies outsourcing to barbarian mercenaries, it is evident that the Greeks were willing to risk utilising third parties in order to achieve their objectives, much like the enterprises of today. Although employing such resources could be beneficial, there is potential to build a dependency on these outsiders and, although they may appear to be under the control of their employer, it is possible that such resources could be a greater threat than they are a benefit. The Venetians also hired outsiders to fulfil military functions. Machiavelli tells of the time the Venetians hired an outsider as a military commander. Although the commander made the Venetians rich through acquisition, they had no loyalty towards him and suspected he...
had no loyalty towards them either. The Venetians began to believe that if this outsider was to leave their employment, he might take the empire that he had won for them back and hand it over to their rivals. For the Venetians, the solution to this problem was to kill the commander (McAlpine, 2000, p86). Although at first the outsourcing to this commander had assisted the Venetian Empire to expand, in the long run the outsider was seen as more of a threat.

According to Pocock (1976, p154), outsourcing to barbarian mercenaries led to invasions that weakened the Roman Empire:

The principate therefore reflected the decline of republican virtue, and neither corrupt citizens nor corrupt soldiers had been able to prevent the growth of civil conflict or the progress of barbarian invasion and the employment of barbarian mercenaries.

Machiavelli also describes in detail the potential impact of outsourcing services to mercenaries:

The arms with which a Prince defends his state are either his own or they are mercenaries, auxiliaries or mixed. Mercenaries and auxiliaries are useless and dangerous and if one holds his state based on these arms, he will stand neither firm nor safe; for they are disunited, ambitious and without discipline, unfaithful, valiant before friends, cowardly before enemies. (McAlpine, 2000, p81)

Outsourcing firms today exhibit many of the characteristics defined by Machiavelli. Machiavelli stresses that mercenaries are unfaithful and ambitious. They pose a danger to their employer, just like outsourcing firms of today. Those that employ mercenaries are neither stable nor safe, much like enterprises of today. Gibbon (1826, p418) blames outsourcing to barbarians for the fall of the Roman Empire stating that:
... in the preceding volumes of this History, I have described the triumph of barbarism and religion; and I can only resume, in a few words, their real or imaginary connexion with the ruin of ancient Rome.

Outsourcing to barbarians may have contributed to the fall of the most powerful empire in the ancient world; yet could the organisations of today that outsource with the intention of improving their enterprise be following in the same footsteps as the Romans? We’ve seen many modern firms suffer severe impacts due to their outsourcing ventures. Boeing’s highly publicised debacle with their Dreamliner project, caused by the aviation giant losing flexibility and control by outsourcing (Sople, 2012, p220) demonstrates how significantly an enterprise’s quality, competitiveness, performance and image can be endangered by an outsourcing endeavour today.

There is an immense amount of wisdom that can be learned from the historic events that have shaped our world. History shows similarities between the enterprises of today and the civilizations of the distant past. They are both built on complex organisational structures, rife with politics, and function within complex ecosystems in cut-throat climates; rivalry runs deep and ruthless competition is endemic. To succeed one must ensure one’s strategic direction is not compromised and to mitigate risks to ensure that the organisation does not succumb to the volatile atmosphere where those that blunder are superseded by their rivals. Regardless of how large, successful and ingrained a firm may be, the potential that outsourcing has to bring down an enterprise is significant. If it were possible for an institution as large as the Roman Empire to fall, any enterprise is susceptible.

8.2 Identifying Barbarian Syndrome

Barbarian syndrome is shaped through nine key characteristics. Although the magnitude of the affliction can vary significantly, these basic traits can be used to assist a firm in initially diagnosing whether it is currently suffering from barbarian syndrome. If the prognosis suggests that the enterprise may not be affected, analysis of these traits can
still assist in identifying whether the firm is exposed to the potential for the syndrome to develop in the future. These traits include:

- **Loss of IP** – The potential for loss of IP as described in Chapter 6. This can be caused through competitive mitosis (covered in section 6.6) or other methods, for instance, poorly written contracts, contracts that cannot be enforced due to the absence of a legal framework to support the contract, or shortfalls in the underlying legal system (as described in section 5.14.7).

- **Loss of Strategic Influence** – The firm is unable to influence the outcome of critical business and technological strategies due to the reliance on a third party for acceptance, agreement or commitment (as described in section 6.5).

- **Loss of Visibility** - The firm has lost, or is at risk of losing, clarity and visibility of the function being outsourced, worsened by supply-chain detriment, (as described in Chapter 7).

- **Loss of Control** – The firm loses control of business operations (as described in sections 6.2 and 6.3). This can occur when an enterprise relinquishes control for an entire function rather than just outsourcing the “doing” work to the third party.

- **Scope Expansion** – The venture is in an expanding business area resulting in the scope of the outsourced activity increasing over time, providing the outsourcer with a greater presence and greater control than originally intended, and defined in section 8.3.5.

- **Dependency Developing** – The customer becomes dependant on the outsourcer and the venture cannot be reversed without adversely affecting the enterprise, as a dependency has been established, as depicted in section 6.2

- **Critical Functions Exposed** – Critical parts of the business are outsourced (as described in sections 5.1 and 6.5), resulting in the customer being at the mercy
of the outsourcer, minimising the ability for the business to negotiate with the outsourcer

- **Flaws in ERM** – The organisation’s ERM framework (covered in sections 4.2 and 5.13) is either non-existent or the ERM practices have not been adjusted to cater for the threats associated with outsourcing and offshoring

- **Realisation** – The environment allows for IP leaks through competitive mitosis (covered in section 6.6) and loss of control of operations, strategy and bargaining power (covered in sections 6.2 and 6.5) to occur without the enterprise even realising that it is occurring, thereby allowing the affliction to progress to a point where it cannot be reversed and the health and prosperity of the organisation is at threat, potentially to the point of complete collapse, as experienced by the Roman Empire.

![Barbarian Syndrome Diagram](image)

**Figure 8.1 – Barbarian Syndrome Traits**
8.3 Mitigating Barbarian Syndrome

Why was Alexander the Great able to outsource to barbarian mercenaries and achieve great success, yet outsourcing to barbarians led to the fall of Rome? Many scholars have been able to aid in delving into the mind of Alexander.

The risks Alexander took in the course of the expedition were calculated ones; he never embarked on a new phase without being certain of the situation to his rear or without informing himself about the country he was trying to conquer. (Briant, 2010, p27)

Much can be learned from Alexander the Great’s leadership. Through his superior abilities in gathering intelligence, planning, preparation and organisation, Alexander was able to defeat his enemies (Engels, 1978, p122). One of Alexander’s hallmarks was diligent analysis and planning, as well as devising strategies and tactics to overcome his enemies (Patrick, 2013). Could Alexander’s diligent planning and risk mitigation have prevented the Macedonians from being significantly impacted by outsourcing to the barbarians? Organisations that follow the lead of Alexander in thoroughly formulating their strategies and mitigating risk may be able to withstand the threat of outsourcing to the barbarians of today. The mitigation of barbarian syndrome involves a multipronged treatment applied across all traits in order to ensure the mitigation is effective across the multiple facets of risk.

8.3.1 Loss of Intellectual Property

There are a number of activities that can be utilised by an enterprise to reduce the loss of IP. In the first instance, an enterprise should identify the areas in which the loss of IP could take place. Similar to the way in which plumbers execute a smoke test to identify leakages within pipes, the enterprise should review their existing contracts and vendor engagements to identify the areas in which there is scope for loss. For those vendor engagements identified, a review of contracts should take place as a priority to determine which engagements have the least legal and commercial support to prevent loss. Once this has been completed the enterprise can work on minimising the risk of
loss across the engagements that are contractually weakest, followed by the contracts that may be more commercially sound. Establishing the priority based on contract strength will ensure that the enterprise focuses on the engagements with the most potential for impact first. Once prioritised, communications with the outsourcer can be shut down temporarily until the environment is deemed to be stable and the rules of engagement have been reiterated to the outsourcing firm and its employees. Ensuring adequate representation of the client’s organisation is available to actively manage and monitor the engagement will also assist in mitigating the potential for the loss of IP. Assigning an internal resource to manage the engagement will assist in maintaining visibility of the operations as well as allowing the organisation to identify leaks sooner, increasing agility and response and therefore minimising exposure. IP theft requires the involvement of law enforcement and legal expertise, whereas IP loss and leakage should be addressed by the organisation internally and mitigated as part of its other ERM and quality processes. To aid in mitigation an organisation’s management should also implement measures to prevent competitive mitosis such as minimising the number of concurrent outsourcing engagements that involve critical business functions as well as implementing controls to protect intellectual capital.

8.3.2 Loss of Strategic Influence

Outsourcing can lead to relinquishing control, and when the function being outsourced forms a vital part of an organisation’s strategy or operations, such as that of IT, the organisation can begin to lose control over its business strategy. An enterprise should ensure that the functions outsourced include only the execution of work, because delegating full control of a function can lead to a reliance on the outsourcing firm. Outsourcing firms can use this reliance to manipulate and even dictate the strategic direction of the outsourced function. It is important that an organisation engaging an outsourcing firm should aim to maintain control of the operation, allowing the outsourcing firm to perform the execution of the required output without relinquishing strategic control. For example, in outsourcing website development, a firm should outsource code development to the firm whilst maintaining control over the content
management system. This will allow the outsourcing provider to deliver the code without allowing the third party to have any influence over the content of the website. Allowing the outsourcer to also involve themselves with the content management aspects of the engagement may result in the outsourcer having input and influence into what content is actually made available on the website, limiting control and providing the outsourcing firm with greater power than necessary. The first step to mitigation should include preventing these types of engagements from occurring; however, if an organisation is serious about addressing such a threat, all active engagements should be reviewed to ensure the scope of the services offered does not lead to a potential loss of influence. Even a microcosm of power could eventually lead to loss of strategic influence as the engagement evolves.

8.3.3 Loss of Visibility

Mitigating barbarian syndrome involves maintaining visibility and, if required, identifying the areas in which visibility could be at risk. If the firm has lost, or is at risk of losing, clarity and visibility on the function being outsourced, it is important for it to establish a new mechanism to reclaim visibility. There are a multitude of management techniques that can be used to reign in vendors in this situation. For instance, the scrum approach whereby resources operate in a team-oriented, collaborative fashion can be used to improve communication between parties and encourage less siloed behaviour. Establishing a daily scrum attended by the business and the outsourcing vendor will help ensure the organisation is across daily developments and that day-to-day visibility is retained. The introduction of reports, such as status reports, can also aid in maintaining the required visibility of operations, provided they are actively distributed and consumed by the required parties. These techniques and other management techniques used to improve communication and retain control should be incorporated into standard operating practices and built into outsourcing contracts to ensure the third party is commercially required to provide adequate visibility to the client.
8.3.4 Loss of Control

A loss of control primarily stems from the outsourcing provider affirming dominance over the client within the area with which the outsourcing venture has been established. This can occur as a result of the outsourcer taking on too much of the governance aspects of the function rather than focussing purely on execution or when the firm believes that the outsourcer has a greater grasp of the business requirements than the client itself. Somewhat different from the loss of strategic influence, loss of control enables the outsourcer to make small decisions, minimising the ability of the enterprise to take part in day-to-day decision-making. By allowing an outsourcing firm to ascertain control, the organisation may begin to develop a disconnect between the required deliverables and the actual outputs, which could be masked by the outsourcer’s control over the environment. Mitigation plans to combat this risk should involve establishing measures to control decision-making, addressing gaps in communications strategies, monitoring performance through KPIs and equivalent metrics, and conducting an audit to identify and eradicate any excessive delegation of authority to the outsourcing firm. Compounded by any underlying mistrust, the long-term effect of the loss of control can result in breaches of policy, in decisions that are not in the best interests of the client, and in siloed behaviour between the enterprise and the outsourcing firm.

8.3.5 Scope Expansion

Control over scope serves as the key to ensuring vendors remain focussed on their deliverables, rather than being distracted by the potential to deliver or sell more services. As most vendors are sales-oriented organisations, it is within their nature to identify and pursue additional services. However, this poses a risk to the outsourcer. The more an outsourcer delivers, the greater the probability of building dependency, loss of IP and loss of control. It is imperative that organisations mitigate this risk through ensuring their outsourcing provider operates only within the boundaries of the engagement and any potential for increase in scope is initiated, managed and controlled by the client. The greater the outsourcer’s presence, the greater control and influence can be developed, making this risk one of the most critical to mitigate early. If the
enterprise already has an established outsourcing model, mitigation must commence through a review of existing vendors to determine how many have been engaged for multiple functions. This will then allow the firm to review and revise its operating model and build a strategy to diversify its vendors. There are benefits to allowing an organisation to increase the scope of its outsourcing vendors, such as improved synergy, simpler operating and commercial models, and greater economies of scale; however, it is critical that an enterprise interpret this as a risk and ensure the scope is tightly managed without being misled by the short-term benefits.

8.3.6 Developing Dependency

Developing a dependency on an outsourcing firm can result in an organisation feeling locked-in – that is, unable to operate without the venture in place. In determining the mitigating actions that will be applied, an enterprise must first determine with which vendors dependence is developing or has potential to develop in the future. The easiest method to determine whether an organisation is dependent on its providers involves identifying which engagements allow the client to “shop around” at the time of contract and services renewal. If the organisation believes that there is no potential for another entity to take over the engagement, the organisation has likely formed a dependency. To assist in mitigating this risk, an enterprise should seek to create a competitive procurement framework, ensuring that keeping vendors honest and competitive is an important part of establishing the services relationship. Maintaining an environment where a venture can be reversed without adversely affecting the enterprise will play an important part in reducing the likelihood of developing a dependency. It is paramount that those dependencies that already exist are identified and addressed prior to developing any further. This can be achieved by assigning business and process owners from within the enterprise to own the outsourced service, allowing the organisation to remain aware of the detailed nature of the engagement and developing a strategy to separate the organisations prior to the onset of competitive mitosis. It may be extremely challenging for an organisation to sever its ties with an outsourcing provider, but the long-term impact of not doing so could be significantly
greater, and the longer the enterprise takes to implement controls the more dependant (and challenged) the organisation will be.

8.3.7 Critical Functions Exposed

Where critical parts of the enterprise are exposed, these functions should form the priority for any organisation’s risk-mitigation strategy. Critical business functions, regardless of the revenue-saving potential, should be maintained within an enterprise at all costs for they contribute to what makes the enterprise successful. Losing control of these strategic areas of a business places a burden on even the most successful organisation, because any impacts in these areas could endanger the business. Much as the Romans outsourced defence, a critical function of the empire, to barbarian mercenaries, outsourcing a critical function can pose an enormous amount of long-term risk today. The Romans may have outsourced this function to barbarians because army duties were dangerous and they did not want to expose their own citizens to the threat. An enterprise of today must identify these areas and avoid making the same mistake. Some of the most challenging and tedious activities form ideal candidates for outsourcing; however, an organisation needs to prevent the exposure of critical functions regardless of how appealing the financial benefits appear to be. An important part of mitigating this risk involves ensuring that the detailed risk analysis includes the potential financial impacts to the firm should the critical function be exposed. The financial savings from outsourcing the function must always be analysed within the context of the overall financial impact that outsourcing the critical function poses.

8.3.8 Flaws in ERM

Flaws in an organisation’s ERM practices can limit its ability to prevent risks from occurring and minimising their impact when they do. An organisation must seek to establish a framework for managing risk. The framework can be created by the organisation itself or be based on one of the publicly available methodologies. The organisation will find it challenging to manage its risk without developing an underlying framework and ensuring that management has been adequately prepared, trained and empowered to manage all risk. Making adjustments to ERM practices when outsourcing
will allow the organisation to combat the risks associated with outsourcing, ensuring that their risk-management practices are adapted to the new and changing landscape provided by the adoption of an outsourcing model. ERM practices should be adjusted to incorporate risk assessments into management decision-making methods, establishing control units and aligning risk-taking activities with the organisation’s risk appetite. Mitigation of risks needs to be sufficient to treat the risk but also to ensure the ongoing tracking and management of residual risk, minimising the exposure to risks that can only be partially mitigated. ERM considerations and thorough risk analysis must be factored into offshore location decisions to ensure that the nation and conditions selected have been well understood and the level of risk is palatable for the organisation.

**8.3.9 Realisation**

Although outsourcing of combat resources has been carried out by many militaries in history, the Romans clearly did not realise the potential detrimental effects on their empire of utilising significant numbers of mercenary troops.

> How the ‘Roman’ army came to be composed of barbarian troops of an often renegade nature is in many ways the story of Rome’s fall. It is the story of a people who seemingly lost confidence in themselves, a government that lost control of its army, and an army that lost control of its soldiers. (Frye, 2007)

When outsourcing to external organisations today, it is possible for an enterprise to lose control of its operations. But could Rome’s downfall have been its failure to realise the threat that barbarian mercenary troops posed? As the empire progressed, Rome continued to recruit foreign mercenaries in greater numbers.

> Whereas Italy still supplied 65 percent of legionary troops during the reigns of Augustus, Tiberius, and Caligula, by the mid-second century the contribution of the Italian heartland had dwindled to less than 1 percent. Rome had begun recruiting its soldiers from the least civilized areas of the empire—a policy that would remain in place in late Roman times. Recruiters seem to have believed
that the best soldiers, the real fighting men, could only be found outside the cities. (Frye, 2007)

Towards the end of the late Roman Empire, foreign mercenaries served in record numbers; this was no doubt a contributing factor in Rome’s eventual end.

The primary trait that indicates an enterprise of today could be suffering from barbarian syndrome is the failure to realise that the outsourcing engagement is placing the organisation at significant risk. The Roman Empire continued to recruit mercenaries in greater numbers, failing to realise that the increasing inclusion of these outsourced soldiers could be contributing to the demise of the empire. The key to mitigation lies in organisations building awareness among their management teams to ensure the aforementioned risks have been addressed. Building an awareness of the potential impacts associated with these risks will aid the organisation in identifying the risks before they occur. Linking ERM practices with procurement processes will allow the enterprise to address the risks as part of the outsourcing vendor-selection process, ensuring that risk management is at the forefront of any outsourcing venture. The longer the affliction is permitted to progress the greater the potential jeopardy the organisation is placed in. Allowing risks to progress unmanaged and allowing the enterprise to continue to establish unmitigated outsourcing engagements could see the organisation follow the same fate as the Roman Empire.

8.4 Sentience or Luck?

Developing sentience – that is, an ability to sense or feel potential threats – could be the key to a firm maintaining agility whilst not ignoring the risks that could unfold. Yet organisations will not develop a capacity for sentience on their own. A formal risk-management canonical is required – that is, thoroughly documented risk-management methods, procedures and guidelines that the organisation is committed to enforcing. This will ensure that the organisation is able to improve the risk-management processes and risk awareness required to navigate the volatile commercial landscape. But as this research has discovered, there are organisations that do not have in place the
frameworks that formulate an effective safeguard against risk. These enterprises do not follow best practices to keep abreast of the potential challenges and therefore subsist by operating under the guise of a stable, safe environment, their lack of being impacted by risk to date providing their stakeholders with a false sense of security. But it’s more than possible that the trajectory of a firm could be completely down to luck. Failing to have adequate respect for the potential impact of threats can have dire consequences; yet this will only be discovered by the organisation if the risk actually eventuates.

Can being lucky enough to not be severely impacted by risks in the past really be an adequate reason not to start mitigating risks today? Suppose one was to cross the road blindfolded without being struck by a vehicle, does this make it a good idea? The threat still exists, and the probability of being struck only increases with the number of attempts to cross the road that are made. In much the same way, a firm that has not managed its risk and has remained relatively unscathed cannot continue to test the laws of probability without eventually becoming unstuck. In these organisations, a catalyst is needed to encourage the organisation to change its ways. This could be a viceroy who chooses to drive organisational change or a significant, near-apocalyptic event that makes the enterprise realise the error of its ways. One just hopes the eye-opening event does not destroy the enterprise altogether.

**8.5 ERM and Strategic Alignment**

Aligning ERM practices and the risk-management framework to the organisation’s strategy is the only way to ensure that risks are managed within the context of the organisation’s strategic direction. If organisations have the intention of outsourcing critical parts of their enterprise, the risk associated with the venture should be analysed to ensure the enterprise is not at risk of developing barbarian syndrome, competitive mitosis or any other detrimental affliction. Continuing to operate in an environment where systems outsourced put the organisation’s strategy at risk, but the organisation’s senior management have little understanding of how the organisation plans to address risk, is a recipe for disaster. Enterprises that proactively seek to align their practices
with their strategy will be in a position to pre-emptively address these threats. Greater alignment with their strategy can be achieved through establishing the required roles and responsibilities to drive engagement and developing a risk-audit function within the enterprise with the primary purpose of ensuring risk avoidance is on the organisation’s agenda.

8.6 Roles and Responsibilities to Drive Engagement

Governance can aid in driving an organisation to establish a successful ERM practice. A key prerequisite involves the development and implementation of the roles and structure in order to establish the right governance framework. Communicating roles and responsibilities to the employees of the organisation is critical if the enterprise wants to see the risk framework successfully embedded into practice. All employees within the organisation should be involved in risk-management initiatives. Yet thirty-eight (38) per cent of participants of this research claimed to not even know what risk-management methodology is in place in their organisation, and twenty-five (25) per cent advised that their organisation did not always actively mitigate risks. This suggests that organisations within Australia and New Zealand are not receiving adequate communication on and involvement with ERM practices in order to drive successful engagement. Hubbard (2009, p29) advises that mitigation requires “organisational structures or roles defining clear responsibilities for and authority over certain types of risks”. An enterprise should invest time and effort in capturing and communicating the roles and responsibilities that relate to their risk-management practices in an effort to gain engagement across the business at all the required levels. Gaining executive and senior management support to improve risk-management practices can be critical in ensuring risk management remains on the corporate agenda as a priority. Obtaining executive support will allow ERM practices to be aligned with strategic-planning processes, management activities and procurement processes – thereby providing governance in the formulation of outsourcing strategies. Tight executive alignment will ensure the organisation’s risk position is at the forefront of operational management and new initiatives. Marchetti (2011, p23) supports this approach:
Corporate governance is critical to the initial development and long-term maintenance of a successful ERM program. The board of directors and management should be actively and consistently involved in the risk management initiative.

Organisations seeking to implement a solid ERM practice can use published methodologies and frameworks such as COSO (Moeller, 2011) to generate the required organisational structure, roles and responsibilities. Moeller suggests that, based on the COSO framework:

A key component of an effective ERM function is the need for enterprise leadership that is responsible for the overall risk management process. Enterprise risk management is usually the responsibility of a CRO (Chief Risk Officer), a designated senior enterprise officer responsible for administering and monitoring the overall enterprise ERM function. (Moeller, 2011, p91)

It is important that organisations assign the role of the CRO to one of their senior executives to assist in driving ERM.

The major responsibility of the CRO is to manage the process of assessing risks throughout the enterprise, to implement appropriate corrective actions, and to communicate risk issues and events to all levels of the enterprise. (Moeller, 2011, p92)

It is self-evident that having a senior manager acting as the catalyst to drive ERM efficiency throughout the organisation would help establish ERM as a priority, but Marchetti (2011, p20) suggests that roles and responsibilities also need to be addressed more broadly:

Every individual within the organisation has some responsibility for ERM. This includes members of the board of directors, management, risk officers, internal auditors, and each employee. Management should ensure that each employee has an understanding of his or her role in the company risk management process.
8.7 Risk Management Reporting

Getting ERM on the corporate agenda at executive level can assist an enterprise in maintaining a risk-based focus towards formulating strategies. Risk reporting can play an important part in communicating risk to the enterprise. Yet many organisations, as pointed out by Lam, do not do this well:

One of the key requirements of risk management is that it should produce timely and relevant risk reporting for the senior management and board of directors ... however, this is frequently not the case. In a silo framework, either no one takes responsibility for overall risk reporting, or every risk-related unit supplies inconsistent and sometimes contradictory reports. (Lam, 2003, p46)

Reporting on the status of risks across the enterprise will assist in identifying cross-functional risks that impact on multiple business areas. This will ensure that risk treatment addresses the impact across all the likely impacted areas of the organisation.

An enterprise risk function can prioritize the level and context of risk reporting that should go to senior management and the board: an enterprise-wide perspective on aggregate losses, policy exceptions, risk incidents, key exposures, and early warning indicators. (Lam, 2003, p46)

Communicating the organisation’s risk position will assist in providing transparency and maintaining visibility of risks across the organisation to ensure they are understood and addressed at all levels of the enterprise. The visibility obtained through risk reporting can be used by the organisation to support decision-making throughout the enterprise, allowing all levels of management to make informed decisions in their day-to-day functions. Improved decision-making will ensure that threats are front-of-mind when any critical or strategy-affecting paths are taken and, most importantly, risk is addressed when outsourcing business functions, assessing offshore locations and selecting outsourced service providers to partner with.
It is disturbing that a large proportion of the people surveyed indicated that they were unaware of the risk-management methodology or framework employed by their organisation and how their organisation managed its risk. Risk reporting must form a central part of the organisation’s risk-management regime if these organisations would like to generate a risk-conscious culture that is tightly aligned with the enterprise’s risk appetite.

8.8 Establishing a Risk Audit Function

Organisations may be able to circumvent some of the challenges associated with outsourcing by developing an internal risk-audit function within their organisations. Marchetti (2011, p23) advises that the internal-audit function may vary from one organisation to another but will assist in ensuring a continuous maintenance of objectivity and independence within the group:

The existence of an internal audit function can strengthen risk management capabilities within an organisation. This group, in performing its overall responsibilities, possesses significant amount of key information that can assist and support management with strategic planning, objective setting, and the management of strategic risk.

Building risk-audit capabilities into the organisation will assist the enterprise in ensuring that risks receive the appropriate treatment, in-line with the organisation’s strategic direction. Developing such a capability within the organisation will enable an entity to own, manage and influence the risks associated with outsourcing. This function can assist with communications. It can embed the most effective organisational framework for the enterprise to manage its risk and overall integration with the organisation’s business and procurement processes related to third-party engagements. Without such a function, the employees that indicated they do not actually know what methodology their organisation utilises to manage its risk will continue to be ill-informed and misaligned, potentially resulting in real risks remaining unmanaged.
8.9 Achieving Separation

It is critical for an enterprise with an engagement that presents with the symptoms of barbarian syndrome to ensure the threat is not just treated, but abolished altogether. It is vital that the organisation establishes its best footing, accepting the short-term pain to ensure the enterprise is not impacted long term. This may be challenging due to the quarterly reporting of financial results by public companies and the potential for the organisation to be impacted financially in the short term in order to free itself from the burden of the outsourcing arrangement. There are a number of ways that separation can be achieved without transitioning the function back in-house. The organisation can:

- end the engagement early by reviewing legal options
- establish a new engagement and transition services to a new partner with improved contractual arrangements
- revise the scope of the existing engagement, removing critical business functions
- adopt a new model such as automation, nearshoring or internal offshoring

This may in fact be the most difficult aspect of mitigating barbarian syndrome – that is, realising the potential for harm and separating from the outsourcer prior to any substantial loss of IP. Because of the nature of the affliction, dependence has likely developed, and convincing all management in the enterprise to cease the engagement even though a dependency exists (or a perceived dependency exists) is an exercise for the board of executives. Without the support of the board, it is likely the ties will not be easily severed and resistance, both internal and external, will be encountered. Breaking the paradigm may be difficult, but given what is at stake the effort will be worthwhile. Had the Romans attempted to rid themselves of the stronghold of the barbarians it’s extremely likely there would have been some resistance, yet in the aftermath of the fall of Rome this seems inconsequential. The organisation needs to determine whether pursuing with a troublesome engagement is the right decision or
ending the engagement (potentially earlier than planned) is the only way to break the
cycle and protect the organisation’s strategic interests.

8.10 A Barbarian-Free Culture

Barbarian syndrome may well be ingrained in an organisation’s DNA, making complete
eradication a challenging feat for the best of organisations. At the end of the day, the
key is to develop an organisational culture that is conscious of outsiders and proceeds
with caution in opening up their enterprise. Outsourcing is inevitable in today’s world,
and the offshoring nations of India, China and others have immense benefits to
provide an organisation. Organisations should seek to develop a risk-averse culture –
that is, a culture that mitigates risk wherever possible and understands how risks can
affect the organisation’s strategy at all levels of management. The overall objective is to
remember that the barbarians in essence were just non-Greeks and non-Romans, and
therefore had non-Greek and non-Roman interests; this is no different from the
outsourcing firms of today which regularly operate with their own interests at heart.
Hillson and Murray-Webster (2007, p82) describe how a strategic audit can assist in
driving such a significant change:

A strategic audit of corporate risk attitude can be undertaken to diagnose the
presence and strength of various drivers of risk culture ... defining routes to
improvement and development as part of an overall change programme.

Executives need to influence the culture of the organisation to ensure they can obtain
the benefits of outsourcing without placing their enterprise at immense risk. Through
instilling risk-conscious qualities within its employees the organisation will be able to
solidify its initiatives to minimise long-term risk. As we’ve seen in the past, the risks
can have detrimental consequences, and if left unmanaged can have major implications.
Most importantly, the Romans outsourced military forces to these outsiders in what
they thought were the best interests of the empire; yet a failure to realise the long-term
effects such an engagement could have is the trait that makes barbarian syndrome so
dangerous for the enterprises of today.
8.11 Barbarian Syndrome – A Modern Example

The now defunct airline Swissair, the Switzerland-based airline, depicted many of the traits of barbarian syndrome. Swissair outsourced strategic decision-making to consulting firm McKinsey, which led to a loss of strategic control prior to its collapse in 2002.

The overall effect of this outsourcing of strategic control – with McKinsey at times almost bulldozing the organisation into following its advice – was that, bit by bit, Swissair lost its own internal ability to carry out strategic thinking. (Hamilton & Micklethwait, 2006, p119)

Exposing a critical function (such as strategy), losing control over the enterprise and a loss of strategic influence are all traits that resonate with barbarian syndrome. Furthermore, another trait – flaws in ERM – also contributed to the former airline’s downfall. According to the OECD (2014, p72):

The most prominent risk management failure has been Swissair, but several of the other large Swiss corporates have also had to strengthen their governance following prominent risk management failures.

Building a dependency on the outsourcing firm, and allowing the firm to expand the scope of the outsourcing engagement are also traits that Swissair demonstrated.

One of Swissair’s fundamental errors was effectively to delegate its strategic decision-making to McKinsey. Unsurprisingly, the strategy devised was one that ensured Swissair’s continued reliance on McKinsey through the ensuing series of acquisitions of minority stakes, so much so that the McKinsey consultants became almost indispensable to Swissair and a de facto part of the operations. In parallel, Swissair’s own internal capacity for strategic thinking diminished to the extent that McKinsey’s proposals, assumptions and predictions were rarely questioned or challenged, by either management or the board. (Hamilton & Micklethwait, 2006, p130)
It is easy to identify the traits of barbarian syndrome as part of a post-mortem of a collapsed corporation, yet the key to mitigation is to develop the ability to identify the potential for the syndrome prior to commencing the outsourcing engagement.
9. The Death of Outsourcing

9.1 The Future of Outsourcing

The risks associated with outsourcing and offshoring, along with the potential for detrimental impacts to an enterprise, have been detailed extensively in previous sections; yet we have also seen through the surveying of IT professionals that many of the organisations actively outsourcing do not take action to mitigate the risks. As organisations become more aware of the risks and their impact, will they continue to pursue such offshore engagements? I believe as the industry evolves and awareness of the dangers increases, there will be a fundamental shift towards investigating alternatives rather than persevering down the traditional outsourcing and offshoring path. Yet some of the alternatives to traditional outsourcing already exist today and should be considered by enterprises when formulating their mitigation strategies. Nearshoring, offshore insourcing and automation may all offer viable alternatives, and the impact that they have on traditional outsourcing in the future could be immense.

9.2 Nearshoring

Outsourcing and offshoring have long been the solution for organisations that are seeking to reduce operating costs and overheads. Rai (2014) highlights the potential for costs in India to increase due to many years of stagnant growth in the salaries of IT professionals:

Entry-level salaries have been static for many years. Industry-wide entry-level compensation for engineering graduates has not gone up in the past five to six years. Entry-level salaries for engineers have barely risen from the 250,000 rupees–350,000 rupees ($4,200–$5,900) annual levels of a few years ago.

But as the cost of offshoring to nations like India increases, it’s inevitable that enterprises will begin to seek cheaper, more sustainable and lower-risk alternatives. It is possible that new and emerging strategies threaten the long-term affluence of
offshoring countries and at the very least dampen the perceived effectiveness of offshoring as a whole.

Nearshoring has emerged as a potential alternative to offshoring. By adopting a nearshoring model an enterprise is able to obtain the benefits of outsourcing whilst mitigating some of the risks. By outsourcing to a closer location, organisations can benefit from reduced risk of location-based threats such as crime and political or social issues. Cultural issues may also be lessened, as the outsourcer will be located in the same region and share similarities with the organisation. The closer proximity of the nearshore location to the customer organisation could be of enormous benefit to operations. The closer distance may assist with reducing travel costs and overall amalgamation and synergy between partnering organisations. Exposure to time-zone differences could also be significantly reduced in comparison to offshoring to outsourcing firms in different regions. It’s understandable that nearshoring will grow as a consideration for enterprises seeking to outsource; however, there may be some potential burdens. Nearshore countries may have less favourable exchange rates, and in regions like Europe the currency and exchange rate may be the same for the customer and outsourcer (i.e. the euro). Considering offshoring involves migrating services offshore to take advantage of cheaper markets, organisations may be reluctant to take the plunge in offshoring if the financial benefits are diminished.

9.3 Offshore Insourcing

As the outsourcing market has matured and the industry has developed, the benefits of offshoring have been well publicised. Yet could it be possible to obtain the benefits of offshoring without exposing your organisation to the risks of outsourcing? Heath (2014) suggests that the drive to send jobs offshore has in part been fuelled by low labour costs relative to Western countries. In India, entry-level salaries for engineers are falling between $4,200 and $5,900. With such significant cost-saving potential, it makes sense to consider such cheap resources. Yet the advantages of offshoring don’t necessarily require an enterprise to utilise a third-party outsourcing firm. Many
organisations have begun to focus on insourcing – that is, the transitioning of services offshore internally, without engaging a third-party firm.

Offshore insourcing is particularly popular with companies that wish to retain or maintain control over their offshore operations. (Burgess & Connell, 2006, p21)

When offshore insourcing, many of the location-based risks may still apply as the enterprise has still expanded its operations to another location. For an enterprise, the primary difference between offshore insourcing and traditional offshoring will be the ability to maintain control. The firm will have full control over selecting the location, thereby allowing the enterprise to avoid exposure to any risks associated with locations that are not aligned with the organisation’s risk appetite. Most importantly, the risks associated with outsourcing firms further subcontracting, the potential loss of intellectual property and the risk of the enterprise becoming dependent on an outsourcing firm will not apply if the organisation adopts an offshore insourcing model. By insourcing, the organisation is able to save costs by utilising more cost-effective resources that are available offshore without actually relinquishing control of their environment to a third-party supplier. This model can assist an enterprise in mitigating many of the human resource and IP risks associated with outsourcing to a vendor; therefore it is no wonder it’s becoming more appealing to risk-averse businesses in the quest to improve their bottom line.

With all the appeal of insourcing, there are some very clear limitations. Opting for an insourcing model could be seen as preventing an organisation from achieving some of the most basic of benefits that outsourcing delivers. Most notably, offshoring without outsourcing does not allow an enterprise to take advantage of economies of scale. Skills, expertise and efficiencies not readily available to an organisation can be accessed through an outsourcing venture, and the capabilities of much larger vendors are leveraged to achieve outcomes more efficiently and at a significantly cheaper cost. These costs include setup costs, maintenance, infrastructure and operational costs, not just cheaper employee salaries. Ultimately, it would be challenging to argue that
adoption of an insourced model is any more likely to impact on an organisation’s risk-management practices in comparison to a traditional outsourcing approach, as the selection criteria is so vastly different from enterprise to enterprise and risk appetites can vary. But it is imperative to bear in mind that this model negates some of the most basic of benefits and still exposes an organisation to location-based risks. Notwithstanding this, future research over the coming years would be beneficial in determining whether uptake of this model has been successful in practice.

9.4 Automation

Ford (2009, p8) advises that:

… while offshoring seems to get most of the attention at the moment, we also know that automation – the complete replacement of human jobs by machines – continues to go on in a variety of industries.

Automation is growing as an option for organisations looking to reduce costs and minimise the overhead of simple repetitive tasks. Ford (2009, p114) paints a grim picture on the future of outsourcing:

The danger – together with the fact that the benefits from offshoring in the third world are likely to be only transitory since automation will follow – really calls into question the overall wisdom of this practice. This is true even for the developing nations that are currently benefiting from offshoring because, as we will see later, the consequences of such a severe and long lasting economic downturn in the West would almost certainly wipe out and reverse any temporary gains these countries may have obtained from offshoring.

With this in mind, should an enterprise be seeking to automate rather than transition services offshore? Through automation, an organisation could eliminate the need for simple and repetitive tasks to be performed by a human being altogether, therefore reducing employee numbers and hence offering a permanent cost saving. In comparison, an enterprise outsourcing a business function continues to accumulate
costs through contract expenses and maintenance and as a result of an outsourcing engagement. Although less expenditure may be required compared with employing local or in-house resources, utilising an outsourcing provider costs money. Automation, on the other hand, while it may require some initial capital investment, negates the requirement for ongoing expenditure, meaning that the return on investment can be considerably higher and the breakeven point can be reached much sooner. Therefore it is quite conceivable that an organisation may opt to remove the requirement to perform the task altogether rather than just moving the task offshore to be completed at a lower cost.

In addition to the potential for substantial reduction in operating costs, automation provides a vast number of benefits over traditional outsourcing and offshoring for a business. Most significantly, automation minimises human-resources-related issues. There is potential for a reduction in human error, which can continue to impact on an organisation in an outsourced model. With automation an organisation will no longer be at risk of losing IP, not to mention the risks associated with offshoring such as natural disasters, crime and the like. These threats are not just mitigated by adopting automation over offshoring, they can be completely eliminated, reducing the need to address ERM practices altogether.

9.5 Predicting the Future

From ancient times many scholars have highlighted the challenges faced in attempting to predict the future.

The key factor underlying the difficulty in predicting the future is the existence of uncertainty. As Plato (427–347 BC) realised, ‘the problem with the future is that more things might happen than will happen.’ With an infinite number of possibilities ahead it is hardly surprising that the task of selecting the one which eventually materialises is problematic. (Hillson & Murray-Webster, 2007, p3)
Machiavelli advises that:

Wise men say, and not without reason, that whoever wishes to foresee the future must consult the past; for all the human events, at any time, have their equivalent in the ancient times. (Cesa, 2014, p45)

Since a mechanism to foresee the future is not available, mistakes of the past can assist with predicting the future. At the very least we should attempt to learn from the mistakes of others. We have seen how natural disasters and other location-based threats can disrupt a business. We have seen IP issues arise as a result of joint ventures between organisations. Just as Philip of Macedon took away the liberty of the Thebans when he was granted too much power, outsourcing can lead to an enterprise being locked in and at the mercy of a third party. Just as outsourcing to the barbarians led to the fall of Rome, an organisation could potentially fall due to outsourcing a critical function. An enterprise needs to understand the state it is currently in, identify which threats pose a risk to it, and implement measures to avoid and mitigate these risks wherever possible.
10. Conclusion

10.1 Aim of the Thesis
The primary objective of the research was to determine the impact that outsourcing has on ERM practices. The research process proved effective in utilising information on current practices to identify gaps in organisational practices. In relation to the sub-questions, which sought to determine whether organisations adjust their ERM practices to protect against the risks inherent from outsourcing and offshoring, a large proportion of the enterprises studied indicated that they did not actively address all risk. Furthermore the research aimed to identify the extent to which organisations implement measures to protect against IP risks, considering there have been many public cases of IP theft impacting an enterprise. The research was also aimed at exposing the lack of overall consideration for ERM in the outsourcing and offshoring process.

Upon critical reflection, although these risk-management practices are now understood and the purpose of the research was achieved, the findings generate more cause for concern as Australian organisations have proved much less risk-averse than originally thought. Moreover, many of the heavily documented risks associated with outsourcing and offshoring such as natural disasters, which have been proven to have dire consequences, are not concerning organisations in practice. A number of the risks raised in the literature do not appear to be causing concern to the enterprises that are outsourcing, which could be placing their organisations at risk. Concerns for the risks brought about by third-world and developing nations were also not as common as originally anticipated. Through the study of research participants, insight into the concerns and practices of real enterprises allowed for an understanding of how misunderstood and neglected the threats associated with outsourcing and offshoring actually are.
10.2 Findings

The research sought to determine what practices are in place in organisations and as a result discovered a number of new concepts. The four fluctuations, entailing the four key areas within which the changes to offshore conditions occur, provide organisations with context for the ongoing assessment and monitoring of their offshoring activities. The potential threat that popular outsourcing locations pose to organisations was demonstrated and, through the survey, it was discovered which locations are most outsourced to by Australian firms, something that was not previously quantified. Through this, we were able to discover that the most outsourced-to locations pose a significantly greater risk in a number of areas than Australia, according to the indicators developed as part of this research. This led to the development of the offshore strategic pillars, a model consisting of 15 key areas that govern a successful offshore-location assessment, identified through risk-management literature and the analysis of survey findings from Australian IT professionals. The Location Assessment Tool, a new instrument to aid in the selection of the most suitable and risk-palatable offshore location, was developed for organisations to utilise as part of selecting the safest offshore location to outsource to.

The research addressed the gaps in the literature by discovering what risks associated with outsourcing are of genuine concern to Australian enterprises. As a result, we now have an understanding of what organisations believe are real risks. It is evident that the risks highlighted by authors, although they pose real danger, are not of concern to organisations in practice, demonstrating that most organisations fail to realise the seriousness of these risks. Furthermore, as a result of this research we now understand that even though seventy-seven (77) per cent of individuals believe their enterprise has a low tolerance towards risk, up to sixty-five (65) per cent of individuals believe their organisation should be doing more to mitigate the risks associated with outsourcing.

The research found that there is a link between IP loss and the loss of competitive advantage when outsourcing. This led to the discovery of competitive mitosis, the process by which an enterprise can leak its IP, impacting its competitive advantage and
jeopardising its ability to compete in the marketplace. Supply-chain detriment – the continual increase in risks and reduction in benefits that eventuates as a result of the length of the unmanaged, or unknown supply chain – was also discovered as part of this research. The research was able to demonstrate the negative impact that the supply chain can have on outsourcing, increasing the likelihood that an organisation will succumb to its unmitigated risks, IP loss and competitive mitosis. The research led to identifying barbarian syndrome, a new theory based on similarities between modern outsourcing ventures and the outsourcing practices employed in Ancient Rome, where tax collection and army recruitment were effectively outsourced by the state. Barbarian syndrome is an affliction brought about through outsourcing and the accumulation of unmitigated risks, loss of IP and dependency on the outsourcer, which can erode an enterprise and threaten its very existence.

The initial review of the literature indicated that outsourcing is not a new phenomenon. It has been used for centuries, and the risk of forming a dependency on an outsourcing firm is not a new notion either. Similarities between events in history were discovered and the dire consequences of not mitigating outsourcing risks were demonstrated with support from both modern and ancient examples. They say Rome wasn’t built in a day, but it burned in one. What takes an eternity to build can unravel in a matter of minutes. Not mitigating risk can open an enterprise up to the oppressiveness of opportunistic outsourcing firms, allowing the outsourcer to control the client’s IT estate at its peril. With multiple permutations of risk, it is possible for an enterprise to be impacted in many ways. If organisations truly aim to seek a long-term benefit from outsourcing, further attention to risk mitigation and the establishment of controls are required to minimise risk. Conducting thorough location assessments and establishing measures to protect IP and maintain control over outsourced operations will aid an enterprise in safeguarding itself from the threats inherent from outsourcing. Most notably, it is organisations themselves that are seeking to outsource and offshore, in the pursuit of cost savings; therefore an organisation may find that its biggest threat could be itself.
Organisations that inadequately implement controls to minimise their exposure, run the risk of suffering the same fate as the mighty Roman Empire.

10.3 Significance of the Findings
This research makes a significant contribution to the professional literature by providing insight into the practices of organisations, thus filling a gap in the industry’s literature. Not only do we now have a greater understanding of the risks associated with outsourcing and offshoring, but also the concept that these risks have potential to lead to the collapse of an enterprise has been proven. The findings provide the evidence required for organisations to improve their practices. Furthermore, this research has provided a tool (Location Assessment) to mitigate and manage these real threats. The use of events from history to identify potential risks to the organisations of today is a method that can be applied to any discipline, and could be considered when attempting to think outside the box and shift the paradigms of today on any topic in the literature.

Empirical evidence was used to reveal insights that were not previously available in the literature and, most importantly, the findings indicate that organisations should be doing more to mitigate the risks associated with outsourcing. The clear impacts of these risks, covered at length throughout this thesis, and based on solid evidence, will assist organisations in ensuring that risk management when outsourcing is adequately addressed in their corporate agenda. The research uncovered evidence that frameworks and methodologies for the management of risk are not being used as much as the threats warrant. This has significant implications not just for the organisations that fail to employ the required risk-management rigour, but also for society as a whole. The organisations that are failing to address the risks associated with outsourcing are not just employers; they are energy companies, Internet-service providers, car manufacturers, government departments, and so forth. The impact that the unmitigated risks could pose to society is immense, as we live in a highly digitalised and modern world. The organisations we rely on for a multitude of critical services in first-world
nations could be crippled by an unforeseen event in a third-world nation; and their lack of risk management could have an impact on all people as the consumers that rely on these services.

10.4 Limitations of the Research

The research conducted was limited to Australia and New Zealand. The primary premise of the research involved outsourcing and offshoring, something more prevalent in first-world countries rather than developing nations. The research only covered outsourcing of technology, and the use of outsourcing models in other sectors such as agriculture and manufacturing were not considered. As Sydney is the primary employer of IT professionals in Australia, the majority of participants that took part in this study were located in Sydney. With the adoption of IT outsourcing models being more prevalent in IT and telecommunications companies, the majority of the sample group consisted of participants that work for organisations in these industries. Furthermore, the sample size for the research was limited to one hundred and two (102) participants and, due to the strict requirements surrounding the selection of participants (IT professionals, senior and influential roles), homogenous sampling was necessary.

There was virtually no relevant research available in the literature; therefore there was very little existing (data or earlier studies) for this research to build upon. This resulted in the requirement to conduct the survey to build a foundation of information, followed by an investigation to further design and develop the research outcomes. Large amounts of literature were also difficult to obtain on collapsed and defunct companies. This may be because organisations are reluctant to publicise how and why their enterprise became defunct. Moreover, their lack of existence today makes them extraordinarily difficult to study.

Finally, this research was limited to risks in an organisational context, although utilising history to provide solutions to today’s problems could be applied to any discipline.
10.5 Future Research

There is potential for future research in a number of areas – for example, a longitudinal study to determine whether adopting the measures highlighted in this research would benefit organisations long term. As the international offshoring landscape changes, particularly with the increase in organisations considering countries outside of the traditional offshoring nations such as India and China, there may be allowances to be made for new risks within the Location Assessment Tool. With the recent increase in offshoring to nations located in Africa and Latin America, the risks associated with outsourcing to these regions have not been well proven and understood. How these regions perform over the following decade from a risk perspective will drive further research and knowledge in the area. The quality of outputs for these regions has remained largely not understood and whether the output from these regions is adequate to compete with the experienced offshoring nations is yet to be seen.

Future research on the outsourcing and offshoring practices of nations outside of Australia and New Zealand may prove beneficial in determining whether other developed nations are as susceptible to the increased risks posed by developing nations. A study on the potential impacts of outsourcing and offshoring for industries other than IT may also prove beneficial as industries such as manufacturing and agriculture may share similar risks (as well as introduce new and different risks).

Is there more that can be learned from history? Once, now that awareness in the industry has increased, the threats associated with supply-chain detriment, competitive mitosis and barbarian syndrome are mitigated through improved procurement practices, robust contracts and adjustments to ERM practices, what next? And how will the trends in nearshoring, internal offshoring, and automation influence the ability to eradicate such afflictions?
## 11. Appendix A – Location Assessment Form

<table>
<thead>
<tr>
<th>Selection Criteria</th>
<th>Cost</th>
<th>Economy</th>
<th>Politics</th>
<th>Comms</th>
<th>Location</th>
<th>Crime</th>
<th>Legal</th>
<th>Terrorism</th>
<th>Environment</th>
<th>Infrastructure</th>
<th>Records</th>
<th>Health Care</th>
<th>Quality</th>
<th>Resourcing</th>
<th>Back-out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>0.4</td>
<td>0.5</td>
<td>0.3</td>
<td>0.5</td>
<td>0.6</td>
<td>0.3</td>
<td>0.7</td>
<td>0.5</td>
<td>0.4</td>
<td>0.4</td>
<td>0.6</td>
<td>0.5</td>
<td>0.3</td>
<td>0.2</td>
<td></td>
</tr>
</tbody>
</table>

- **Argentina**
- **Brazil**
- **Bulgaria**
- **Canada**
- **China**
- **Great Britain**
- **Hungary**
- **India**
- **Indonesia**
- **Ireland**
- **Israel**
- **Japan**
- **Malaysia**
- **Mexico**
- **Netherlands**
- **Peru**
- **Philippines**
- **Poland**
- **Russia**
- **Singapore**
- **Thailand**
- **USA**

*Figure 11.1 – Location Assessment Form*
12. References


Numbeo (2015a) Crime Index for Country 2015, Numbeo Doo Inc.: Serbia [online] Available at:


