1. Chapter 1

1.1 Introduction

1.11 Preamble

Data continues its very fascinating journey in time, that of explosive exponential growth from the year 20,000 BC of counting abstract objects to the year 15,000 BC when the first narrative stories were recorded as cave paintings to the earliest written record in the year 3000 BC when a systematic way to record and transmit knowledge was developed and till date in the digital world. It is estimated that by the year 2020 information would double every 73 days [Bernheim and De Souza 2003]. In the era of digital revolution, data is playing a crucial role by permeating into every industry and business function due to the growth and use of information and communication technologies (ICT) which is helping digitize industries, society and Nations.

Today the modern and globalized business and society has grown to be dependent on the global nature of cyberspace (a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical ICT devices and connected networks) due to the dynamic and novel use of ICT. The successful innovative exploitation of cyberspace and mature use of ICT by technologically advanced Nations is helping them and their society to prosper in the digital economy also known as the knowledge economy, information economy, wired economy or Internet economy.

It is clear that there are three outstanding features that make this digital revolution unique, namely cyberspace, digital economy and the speed with which it has transformed industrial economy into a digital economy. The word digital or information or knowledge or wired or internet economy involves interactive machine learning as well as commerce using ICT infrastructures.

As the cyberspace continues to expand at a rapid pace, it is increasingly being recognized that the same network connectivity has also increased the vulnerability of businesses, society,
individuals and Nations at large. The attack surface has increased and there are multiple points of access vulnerable to attack making it difficult to separate or secure any particular area within the overall system. Individuals empowered with tools and information in cyberspace can wreak havoc in ways never before imagined thereby causing issues for national security, bring reputational damage to businesses, cheat individuals, violate human rights or damage the culture of the society. In short, compromising the confidentiality or integrity or availability of data, has the potential to threaten international peace or the security of global systems (businesses or society).

As a consequence users are looking for end to end trust assurance in ICT. Trust is the basis of human existence, is used intuitively and helps in making context dependent assessments [Touré 2011]. Thus securing the data or information security has become an important priority as it cuts across businesses, individuals, society and Nations.

The remarkable increase and dependency on ICTs by businesses to achieve efficiency, collaboration, improved effectiveness and competitiveness has also led to an increasing demand for software services, which can be broken down into their constituent parts and traded [UNCTAD 2004]. This increased demand has led to and is fuelling the unstoppable growth of IT outsourcing business [Gonzalez et al. 2009] and outsourcing is making the world a better place by the redistribution of wealth [Conboy 2013]. As offshore outsourcing service providers and customers continue to innovate and devise new services for outsourcing there is also an increasing challenge for service providers to ensure that they provide assurance and compliance against information security breaches including service failures. “India is the most competitive and popular IT-outsourcing destination in the world and tops the ranking of The Global Outsourcing Report” [Davis 2005]. While there have been many cases across the globe related to data breaches and their consequences, a decade of select outsourcing related cases from India are listed here:

2. November 2002: Cisco admitted that they were investigating a source code theft allegedly stolen by former employees based in India and was being offered for a price of US$240,000 [Online article 320 – 2005]

3. January 2004: Wipro Spectramind, a New Delhi based subcontractor for Capital One Financial Services, apparently lost its contract to an organized crime, after an audit discovered that Wipro employees were, among other things, offered fake discounts and free gifts to customers. The audit characterized the problem as “unacceptable practices” [Lum 2004].

4. August 2004: Jolly Technologies, a division of U.S. Company Jolly Inc., reported Wednesday that an insider stole portions of the source code and confidential design documents relating to one of its key products, at its research and development center in Mumbai, India. The impact was that Jolly Technologies reportedly shut down its R&D center immediately to assess and contain the damage [Online articles 320, 322, 323 – 2005, 2004, 2009].


8. August 2007: A prominent Vadodara based firm (Doshi Accounting and Services Private Ltd) involved in business process outsourcing and knowledge process outsourcing filed an offence against 10 of its former employees for allegedly stealing data and softwares of clients from UK, Columbia, Australia, etc related to payroll operations, book keeping, quality control and other tasks [Online article 328 – 2007].

9. December 2007: A former engineer with a Pune-based software solutions company, 3DPLM Software Solutions, was charged by the company of cyber theft worth US$12 million for allegedly leaking confidential information of her employer and source code, via email to her husband and others [Online article 329 – 2007].
10. April 2012: On receiving a complaint from Autocad software training firm located in Hyderabad alleging that their customised software training module was tampered with, stolen and put on sale by unidentified offenders, the Crime Investigation Department arrested a Mumbai-based civil engineer for the source code theft [Online article 330 – 2012].

11. May 2013: Breach of information security at two payment card processing firms (ElectraCard Services and EnStage) in India where a gang of cyber criminals stole nearly US$45 million from two Middle Eastern banks (National Bank of Ras Al Khaimah and Bank of Muscat) [Online articles 331, 332 – 2013, 2013].

The impact of these cases can be summarized in six points as follows:

1. Damage to the country’s reputation and impact on Gross Domestic Product (GDP) growth. Thereby impacting trust and also eroding the GDP. It is estimated that the Group of Twenty (G20) economies have lost 2.5 million jobs to a wide range of nefarious cyber activities including counterfeiting, piracy and cybercrime, and that governments and consumers lose US$125 billion annually, including losses in tax revenue [Online article 333 – 2013].

2. Loss of Foreign Direct Investment (FDI) thereby impacting trade.

3. Unethical or unacceptable security and privacy business practices thereby questioning the governance of organizations.

4. Criminal breach of trust which impacts service quality and customer trust. In the digital economy service delivery is fundamental to economic exchange, which includes customer relationships, the process of exchange of intangibles such as information and specialized competence such as knowledge and skills [Vargo and Lusch 2004].

5. Billions of outsourcing Dollars at stake for the Indian IT Industry thereby resulting in loss of business and hence impacting the performance of the organization.

6. Objections to outsourcing due to high security risks.
In India, the major reason for these breaches is attributed to human errors and system problems together accounting for 74 percent [Ponemon Institute 2013].

These six points highlight, trust, GDP impact, information security, trade, governance, service quality, performance and risk, thus providing the basic themes to explore in this research from an Indian context while examining the globalization of services sector which has given rise to offshoring – the cross border sourcing of ICT enabled business support services.

In the pursuit of healthier globalization, six direct points has been proposed [Kohler 2004]:

1. Increasing interdependence and the need for multilateral cooperation
2. The need for good governance and National self-responsibility
3. Need for an international regulatory framework
4. Giving more consideration to social dimension of globalization
5. Respecting different cultures and human diversity
6. Achieving sustainable value creation, profitability and competitiveness while being globally ethical

Adhering to these points proposed by Kohler could possibly have avoided or minimized the impact of the select outsourcing cases summarized earlier. To achieve what Kohler has proposed for a healthier globalization, building of trust along with accountability among nations, among organizations and among individuals is most critical so as to undertake collaborative and innovative actions by way of continuous improvement and learning.

1.12 Background

Data longevity through civilizations in various forms is extremely fascinating and one of the most stable factor which provides actual facts regarding people, society, organizations, generations, nations and civilizations since the year 20,000 BC when the counting of abstract objects started to the digital world of today. Data has played an extremely important role through
civilizations and digital data or information is expected to play an increasingly crucial role in the future of humanity. Based on the work done by Schumpeter on development of the Kondratieff long wave curve (referred to as Schumpeterian Shifts and also as creative destruction for the Continuity and Discontinuity in innovations) and the work done by Kaku in adapting the Kardashev scale to classify civilizations of the future based on harnessing and consumption of energy, the trend forecasted is moving from the past industrial revolution to the present information evolution to the future planetary civilization progression which is Type 1 (we are currently not at Type 1) and the current digital revolution comprising of cyberspace along with ICT fueling a digital economy are the foundation to progress towards Type 1 civilization (harnesses sustainable energy from the entire planet) [McCraw 2006; Hausknost and Haas 2013; Kaku 1994, 2012; Online article 334 – 1999]. The evolution of the internet to a semantic web is traced from the days of connecting information to connecting people (the social web of today) and now evolving to connecting knowledge and to connecting intelligence or behavior [Davis 2008; Breslin et al. 2010]. This requires usage and storage of vast amount of data or information from the past and present. It clearly is a long way for information to have moved from cerebral storage and being etched on stone tablets or papyrus to filing cabinets, punch cards, floppy, compact disks and now to the cloud and quantum storage. Each of the stages of data storage has had and will have their own set of challenges for its access, sharing, extraction, exploitation and preservation. As the internet evolves and the information on it continues to explode it is crucial that all the data or information available in the cyber space is secure and can be trusted as the future of humanity would be dependent on this information. Trust is at the core of social order and economic prosperity as it is the basis for economic transactions and inter-human communication [Tonkiss 2009; Reina and Reina 2007; RISEPTIS 2009]. To address this issue of trust in the Semantic web, a five layered approach has been proposed and adopted which addresses security and privacy along with secure information integration based on standards so as to achieve trust management which is the highest layer [Thuraisingham 2005]. Nations policy makers are beginning to realize that by embracing digitization while addressing security and privacy concerns of citizens and businesses, allows for increased access, sharing and integration of information using hyperconnectivity thereby encouraging citizens and businesses towards improving economic, political and social participation which in turn accelerates the Nation’s economic growth and global integration to achieve planetary civilization where the
socioeconomic path and ICT are deeply linked [World Economic Forum and INSEAD 2012; Clift and Mandeville 2012].

The remarkable increase and dependency on ICT by businesses to achieve efficiency, collaboration, improved effectiveness and competitiveness has also led to an increasing demand for software services. A new wave of globalization not previously witnessed has international trade, investments and technology connected inseparably within global supply chains [Milberg and Schöller 2008]. The globalization of knowledge jobs and their outsourcing since 1990’s has benefitted India [Clift and Mandeville 2012]. India has been able to effectively trade globally, information-intensive services by breaking it down into its constituent parts and trading them in the same way as possible with goods [UNCTAD 2004], by providing a skilled workforce at lower wages.

The Indian software services industry has contributed to India’s increase in GDP (1.2 per cent in Financial Year (FY) 1998 to an estimated 7.5 per cent in FY2012), employment (additional 230,000 jobs in FY2012), exports (19% growth of IT Services in FY2012) and the growth in global outsourcing share (55% in FY2010 to 58% in FY2012) [Barg et al. 2012; Online article 341 – Nasscom; Department of Electronics and Information Technology 2012-13]. India is the largest exporter of ICT services in the world [OECD 2012]. The United States (60%) followed by the United Kingdom (18%) have been the largest offshorers to India and the mature banking and financial services industry the biggest segment (40%) [Nasscom 2012].

Successful outsourcing is ultimately dependent on business maturity and trust between the two parties and trust is a key issue in all kinds of business relationships, including inter-company relationships [Fink 1994; Nguyen et al. 2006; Oza et al. 2006]. Long term contracts help in relationship and trust building [Arora et al. 2001; Barg et al. 2012]. While offshore outsourcing provides various benefits such as cost, growth, competitiveness, improved service levels, there are also perceived risks. Concerns have also been raised over the risks of outsourcing financial services to Indian companies after the May 2013 reported breach of information security at two payment card processing firms mentioned earlier. The risks of outsourcing offshore that need to be managed, by both - the customer and service provider, are service quality, culture, information or data security, intellectual property, disaster recovery and operational efficiency as seen in Chart 1 [Lewin 2005].
As per prior literature, issues related to information security are impacting the software and services sector due to the regulatory trends seen across countries [Nguyen et al. 2006; Oza et al. 2006]. Preceding literature also establishes the importance of information security as a determinant of trusted software services in the outsourcing perspective [Yalaho 2007; Agarwal et al. 2005; Tafti 2005]. More than 60% of the cases investigated for information security breaches were linked with outsourcing partners who were thought to have been responsible as a direct result of deficiencies within their system which could be exploited by hackers [Trustwave 2013]. Information security and privacy breaches have a network impact, a single breach can break down organizational reputation and two breaches could act as a catalyst for loss of business [Patterson et al. 2007]. The average cost (inclusive of detection, escalation, notification, incident response, legal, investigation, outbound communication, the economic impact of lost customer trust and confidence as measured by customer turnover or churn, all using the activity-based
costing model) of a single compromised record (the average number of breached records was 23,647) in the United States was US$188 in the year 2012, while third party / outsourcing service provider errors increased the cost per compromised record by US$19 and having a strong security posture at the outsourcing service provider end reduced the cost of the breach by US$15 [Ponemon Institute 2013]. This effectively translates to a saving of US$ 34 for a single compromised record (or US$ 803,998 for the average number of breached records) for a customer in the United States if their outsourcing service provider has a strong information security posture at its end.

1.13 Motivation

The world is transitioning through difficult economic times and information systems outsourcing and offshoring is expected to stay and flourish by continuing to be a key strategic instrument for increased competitiveness by providing effective cost reduction, source for specialist skills and superior services.

In the growth of the digital or knowledge economy to be more globally and better integrated, trust is a key perception in inter organisational relationships for economic growth. The Indian software services companies have steadily developed and nurtured inter organisational relationships and built trust which has helped them in enhancing business performance and outcomes.

Today, information is increasingly handled, processed, transported or stored in ICT systems across the business. Businesses perceive an increased risk which has arisen due to the increased attack surface due to the dependence and complex hyperconnectivity with its supply chain and customers. Their critical asset, information, is at risk and needs to be safeguarded and protected. Outsourcing customers need trust and assurance with respect to security of their information from the outsourcing and offshoring service provider for continuation of outsourcing and offshoring. The outsourcing and offshoring service providers need to continue their economic growth and thereby the Nation’s economic growth by showing improved organizational performance while addressing to the satisfaction of the outsourcing customers their concerns
regarding perceived risks around information security to their critical asset – information, so as to continue on the journey of integrating the socioeconomic path and ICT for the Type 1 civilization.

This study intends to contribute towards the larger goal for civilization in a small way by exploring themes namely trust, GDP impact, information security, trade, governance, service quality, performance and risk, in the context of globalization of offshore outsourcing services sector.

1.14 Outline of this Research

Based on the themes identified above, this study carries out a literature review across these identified theme areas. It covers literature review of areas such as globalization, the role of FDI in globalization, how India has fared in the context of globalization. Since India tops the global IT outsourcing supply chain world ranking this study covers literature in areas such as offshore outsourcing of IT services in terms of why these services are being traded and how trust and information or data security assurance level has emerged as an essential parameter when selecting an outsourcing partner. Why security is an important pillar of trust and why trust is essential for outsourcing. It also touches upon the fact that the IT sector in India was quick to spot the growth trend of intermediate services and the need for providing specialization in services which has contributed towards inclusive economic growth and development. Offshore outsourcing of IT services is a strategic and dominant management practice followed by a majority of business enterprises in the developed nations to achieve cost advantage, superior service quality and hence a competitive edge on a global scale. The literature on competitiveness highlights the need for valuing reliability and trustworthiness as part of the culture for wealth creation and that globalization encourages trust by increasing competition. While trust is main topic of this study, so it is covered across the literature in all areas, but a specific section in literature review is also dedicated to trust. It primarily highlights that trust is a process and in the era of information revolution it is multi-dimensional and extremely complex as there is a need to address it from the perspective of industrial era as well as the information or ICT era. To address
trust in a converged way (industrial and information era), it needs to be viewed as a governance instrument. From the literature on governance it is clear that corporate governance impacts the performance and competitiveness of organizations. Since IT is transforming organizations in the information revolution, it has become a major contributor and part of corporate governance. Similarly there is a need for information security governance to now be an integral part of corporate governance since the growth of data continues to explode and would need to have strategies and oversight in place for its protection and safeguard. Since reliable and consistent superior quality is an important dimension in terms of perceived value for customers trust and satisfaction it is also a part of corporate governance. One of the roles of corporate governance is to manage risks for all the stakeholders, including quality risks. Literature clearly establishes that security is a quality area which can be decomposed into sub factors and security is a dimension of information quality with its roots traced to Total Quality Management (TQM). Thus TQM is an integral part of corporate governance. To deliver superior service quality to their customers, service providers need to achieve operational excellence by focusing on their internal processes and controls. Hence service quality is an ongoing commitment at a strategic, tactical and operational level in an organization which leads to increased trust between the service provider and the customer, improves customer satisfaction and hence customer loyalty leading to better organization profitability or performance. Delving into the literature on performance clearly highlights that information security breaches can be the grounds for continued losses thus impacting the organizations performance while an escalation in customer loyalty in a service industry can lift profits significantly.

Based on this literature review, gaps have been identified and issues which are relevant for this study are highlighted. The study then goes on to provide the overall design of the study in terms of the research question, the research objectives, the issues addressed, the scope of the study, the research methodology followed, the research models identified, the instrument design carried out, the survey sample identified, how data collection has been carried out and how the model testing and construct validity has been achieved.

The overall study can be viewed as a three step process to arrive at answering the research question. The first step primarily helps in identifying the information security practices followed by the Indian software services industry by utilizing the business model for information security
and the service quality gap model, and pinpointing areas of weakness in the select dimensions of service design and service performance of the service quality gap model. In this step methodological and data triangulation has been used which includes using multiple methods of data collection and data analysis to enhance confidence in the resulting findings. Triangulation has been used to help reduce the overall bias in data and in enhancing the verification of findings and derived conclusions. In this step it emerges that the service providers have been able to govern the customer data adequately to provide acceptable service quality to customers and in turn continue to improve their organization and industry performance while having gaps at the governance layer as information security culture is not an integral part of the organization fabric and information security architecture is not aligned to overall corporate security strategy and business goals. This leads one to explore the relationship between governance, service quality and performance further as the next step.

The second step uses survey methodology to gather the data to explore governance, service quality and performance from the Indian software service providers perspective. It provides an empirical analysis using Partial Least Square (PLS), a Structural Equation Modelling (SEM) technique which has been used for modeling to validate the relationship between information security governance as part of corporate governance and information security service quality and that between information security service quality and organization performance. The data was collected from survey respondents from across Indian cities namely Bangalore, Chennai, Hyderabad, Delhi, Noida, Gurgaon, Lucknow, Bhubaneswar, Mumbai, Pune, giving an all India perspective where the outsourcing software services vendors are situated. The individual items of the survey instrument were tested for convergent validity or unidimensionality and their loading values. For the overall model, composite reliability and convergent and discriminate validity tests were carried out. After this the coefficient of determination, effect size, path relationships and predictive relevance were calculated for the model.

The third step utilizes the survey instrument and data gathered in step 2 for mapping the security governance and security service quality items to individual trust items and to the key trust dimensions. This step triangulates the above two steps in a qualitative and quantitative manner to conclude that trust leads to corporate sustainability and growth and can be depicted in the form of a maturity framework while answering the research question.
The study finally culminates with the synthesis of the three steps to arrive at the overall conclusions, findings, recommendations, implications, contributions, limitations and suggestions for future research.

1.15 Organization of the chapters

Chapter 1 or Section 1 provides an Introduction and Motivation for this study along with the outline of the research.

Section 2 delves into the literature review across the various themes identified, identifies gaps in extant literature and provides the overall study design including the research question and research objectives.

In Section 3 the information security practices followed by the Indian software services industry have been studied, and areas of weakness in the select dimensions of service design gaps and service performance gaps of the service quality gaps model have been identified. This has been referred to as step one in the section “Outline of the research” above.

This leads to an empirical study of the governance of information security services in Indian outsourcing organizations providing software services, the information security service quality provided and overall organization performance in Section 4, using existing dimensions, frameworks and instruments from extant literature. This has been referred to as step two in the section “Outline of the research” above.

Building upon the dimensions and findings in Section 4, Section 5 maps the individual information security items to individual trust items and to the key trust dimensions so as to develop and arrive at a trust capability maturity competency framework. This has been referred to as step three in the section “Outline of the research” above.

Section 6 provides the overall synthesis of this study in terms of overall conclusions, findings, recommendations, implications, contributions, limitations and suggestions for future research.
Three research papers covering Section 3 and Section 4 have been published / accepted for publication [Bahl et al. 2011, Bahl and Wali 2013, Bahl and Wali appearing 2014].