3. Chapter 3

3.1 Indian software services providers – examining information security practices followed and service quality gaps

3.1.1 Preamble

In this Section, 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” as part of Section 1. Through this exploratory study an understanding of the current state of information security practices being followed at the service providers end can be understood. This understanding helps towards identifying specific areas that need further analysis and study.

This section covers the first two research objectives, which are:

1. To examine information security practices followed in the Indian software services industry using a holistic, scalable, theory based, business oriented model for information security

2. To examine select dimensions of service quality to understand if it leads to any perceived service quality gap in the security services from the Indian software services providers’ perspective within the Indian software companies?

The schematic view of the work done for these two research objectives is depicted in figure 11 and a paper has been published [Bahl et al. 2011] on this section from where most of the text is taken:
3.1.2 Introduction

Today the most important strategic asset for organizations is data or information and hence it needs to be protected. This strategic asset is the foundation of the digital or knowledge economy. Due to the various benefits of ICT for businesses, organizations for their economic success and competitive advantages embark on offshore outsourcing of services where the organization specific business processes and related data or information is also accessible to and in the hands of the service provider. The customers trust the service provider to protect this data or information and also bind the service provider and themselves through legal contracts to reduce the risk of opportunistic behavior. This requires the service providers to protect the information on behalf of their customers.

In today’s digital or knowledge economy, services (including Information Technology services) are taking a centre stage as they are crucial and critical for maintaining competitive advantage. As per the World Investment Report [UNCTAD 2004], it is possible to break down information-intensive services into their constituent parts and trade them in the same way as possible with goods. Hence, this services trade enables the production of services to be distributed globally in locations offshore from the firms’ home countries. Various transnational companies are taking
advantage of this trend and expanding their supply chain to include places where they can get skilled workforce at lower wages through outsourcing arrangements, which is well documented in prior research and it has become an established practice across many companies [Lacity et al. 1996]. Prior research has also documented the fact that outsourcing is a management practice, consolidated within the area of Information Systems and is currently going through an unstoppable growth stage [Gonzalez et al. 2009]. Offshore outsourcing of software services is one of the dominant strategies followed by majority of corporations in the developed states to achieve competitive edge.

According to Forester [Forrester Report 2002] over the next 15 years, 3.3 million U.S. services jobs and $136 billion in wages will move offshore. Of this total, 473,000 will be Information Technology (IT)-related jobs, representing 8% of all current IT jobs in the US and most of the outsourcing is expected in the area of software development and customer service and call centers. This benefits the Indian software services providers as India tops the global IT outsourcing supply chain world ranking.

While there are numerous benefits, there are also perceived risks of IT outsourcing to India and information security is one of them. As the Indian software service providers are an integral part of the global supply chain it is pertinent to understand the impact on the Indian software services export trade if risks are perceived and gaps identified with respect to information security in service design and service delivery at the Indian software service providers end. Security (practices, data and application software) is an area that the Indian software service providers need to be focused on so as to establish India as a trusted global hub for professional services. In view of this growing need for managing security in a software services outsourcing context towards a sustainable relationship, the security processes of vendor organizations in India have evolved alongside the maturity of these organizations. How do Indian software service vendors provide service delivery to their customers with respect to security as an integral part of their services, which is critical from a trust, relationship building and business sustainability? This section attempts to examine security gaps, if any, in software services outsourcing from a vendor perspective.
3.1.3 Theory

As ICT continues to transform the way businesses operate [ICAEW IT Faculty 2011], information has become the lifeblood of an organization [Susanto et al. 2011; Morton 1996]. This data or information is a strategic corporate asset not only acting as a business enabler to grow revenues or cut costs but also providing competitive advantage and helping create innovative customer value [Von Solms et al. 2011; ICAEW IT Faculty 2011; Koskosas et al. 2011]. Similarly for the digital economy and information society, data or information is the most valuable asset [Koskosas et al. 2011]. Organizations adopt a risk management strategy to protect their assets and since data or information is a strategic corporate asset it needs to be protected, by utilizing information security good practices, in terms of its integrity, confidentiality, authenticity and availability with the objective to “maximize assets protection at minimal protection costs” [Kovacich and Halibozek 2003; Koskosas et al. 2011]. Security “was not thought of as a business process” and hence was not viewed “as an integral part of business” but “more of a detached afterthought” as there were no ways to measure defined benefits or how it could add value to the enterprise [Kovacich and Halibozek 2003]. However, in todays globalized world, “if this information is compromised, an organization may not only lose its competitive advantage, but its very existence” [Von Solms et al. 2011].

Organizations are embarking on offshore outsourcing of their vertical business as well as horizontal processes cutting across functions or units not just for achieving substantial cost savings but as a key corporate strategy for increasing productivity, draw upon specialist skills, improve services and as an essential means to continue being competitive [Corbett 2004]. Academic articles on offshore outsourcing started in the early 1990’s and researchers had bracketed “India as the par excellence provider of IT offshore services” [Online articles Gonzalez et al. 2013] India has been called an offshore powerhouse as it dominates the offshore outsourcing global market, has built up a considerable export oriented IT service sector and is also on top of the A. T. Kearney’s Global Services Location Index for IT services for organizations wanting to offshore work to an external supplier to provide services [Cattaneo et al. 2010; McCue 2008].
Vargo and Lusch [2004] have provided a broad and all-encompassing definition of services “as the application of specialized competences (knowledge and skills) through deeds, processes, and performances for the benefit of another entity or the entity itself”. The services trade - offshore outsourcing of software by customers to their software service providers – as part of the global supply chain requires a strong commitment and close relationship among trading partners in order to attain lowest cost and maximizing service [Stank et al. 2001]. Indian software service providers have developed and then honed and capitalized on the competencies for offshore outsourcing of services by focusing on processes to achieve performance for the benefit of their customers. In this inter organization (between the Indian software service provider and the customer) asymmetric partnership (since the expertise, resources and knowledge differ among the partners) the role of trust is crucial to reduce cost and improve the partnership through constructive and cooperative behavior between the partners so as to reduce the risks [Blomqvist and Ståhle 2000] of opportunistic behavior and questions raised regarding the service quality and security violations offshore [Davis 2005; Jorek et al. 2009; Kaka and Sinha 2005; Randeree et al. 2007] since the strategic data or information and proprietary business processes of the customers are either with the external service provider or the external service provider has access of most of it which is stored in the Information Systems of the customer [Gulla and Gupta 2006].

Security is an important pillar of trust and trust is an important factor in initial and continuing outsourcing [Luor et al. 2008]. Based on the details in literature review section [Saitta and Fjermestad 2005; Gonzalez et al. 2009; Tafti 2005], security determinants of trusted software services in the outsourcing perspective are governance (including laws and regulations), culture, policy, people, process (including audits and controls) and technology (including infrastructure and operations). Thus the Indian software service providers need to (1) provide superior service quality, as well as (2) ensure the security of the customer data or information offshore by following reasonable and good information security practices within the organization.

Service quality theory has been covered in section 2.17 “Total Quality Management and Service Quality” as part of section 2, where the service quality gaps model to understand customers perceived and expected service gap has been discussed. The customer service gap comprises of the summation of the four gaps namely knowledge gap, service design gap, service performance gap and communication gap [Parasuraman et al. 1985]. It is important to understand these
service gaps in detail with respect to security, as these gaps reside at the software service provider's side. This understanding is also necessary since the agency theory, where the customer delegates the work to the service provider, highlights two issues namely difficulty of client in verifying appropriate behavior of the service provider and that the customer and service provider may prefer different actions because of the different risk preferences that each of them have [Tiwana and Bush 2007].

The threats to information (including customer information to which the service provider has access or which resides in the service provider's ICT systems) keep evolving and it is necessary for organizations to manage this evolving risk by understanding the business impact of the threat, likelihood of the threat and efforts involved or the cost to mitigate the threats [Bojanc 2012]. Predictive threat modeling is an approach that helps towards doing a continuous and systematic analysis of the threat to the organization. It helps in determining the most likely courses of action that could be taken by a threat and provides pointers towards areas where appropriate responses need to be developed thereby identifying areas of weakness. Predictive threat model captures structural and dynamic properties of systems with emphasis on measurement and prediction [Yearworth et al. 2006]. Such a model typically represents processes of various business entities which respond to events occurring at particular rates and with particular probability [Yearworth et al. 2006]. To mitigate the threats to information, the service provider must have in place robust information security practices with the goal to safeguard its integrity, confidentiality, authenticity and availability [Kovacich and Halibozek 2003; Koskosas et al. 2011].

Researchers have proposed various information security models [Maconachy et al. 2001; Skopik et al. 2012; Workman et al. 2008; McLean 1990; McCumber 1991; Lindström and Hägerfors 2009; Gustavsson et al. 2005] which have either been technical or economic or integrated in their approach and have adopted a reactive style to the various threats, breaches or risks that organizations face or to the various legislations and cultural issues that may arise depending on the country of operation of the organization [ISACA 2010] thus not being aligned to the business requirements or being understood completely by decision makers in the organization. Thus there is a need for a model that should be holistic and scalable, can address the common (technical and business) language for information security and business management, is dynamic in nature as opposed to reactive and can empirically provide a possible visual view of how do service
providers align their security practices within the organization with respect to service delivery. The Business Model for Information Security from ISACA [2009, 2010] as depicted in figure 12, takes a business oriented approach to managing information security has been considered in the study.

As per ISACA [2009]: “This model has been conceptualized on the foundational concepts developed by the University of Southern California (USA) Marshall School of Business Institute for Critical Information Infrastructure Protection utilizing systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections in this model are comprehensive and are over and above the security determinants identified in literature review thereby adding richness to the service design and service performance areas. The way to view the model is like a flexible, three-dimensional, pyramid-shaped structure made up of four elements (Organization inclusive of Organization Design and Strategy; People; Process; and Technology) linked together by six dynamic interconnections (Governing; Culture; Enabling and support; Emergence; Human Factors; and Architecture). The elements and dynamic interactions constantly exert a push / pull force depending upon changes in the enterprise, while they interact with each other and allow the model to adapt as appropriate. The equilibrium of the model is disturbed if any one part of the model is changed, not addressed or managed inappropriately. Further these elements and dynamic interconnections can be depicted in terms of their relative size and thickness to each other, thereby providing a visual view of the state of equilibrium or disturbance of the Business Model for Information Security. The model utilizes concepts of systems thinking which stems from Systems Theory, to help understand how systems interact and how complex relationships within the enterprise work”. This model also reflects the characteristics of complexity theory, which focuses on how patterns emerge. Complexity theory has grown out of systems theory and chaos theory [Dann and Barclay 2006] and attempts to “demonstrate why the whole universe is greater than the sum of the parts and how all its components come together to produce overarching patterns as the system learns, evolves and adapts” and thus helps to more effectively manage security. Dann and Barclay [2006] state that systems behave in a non-linear fashion and that small changes in initial conditions can have a large impact on outcomes – also known as the butterfly effect.
The business model for information security in figure 12 shows a balanced model where the elements are of equal size and the dynamic interconnections are of equal thickness exerting an equal amount of push / pull force thus keeping the model in equilibrium. This model is not just a theoretical model but a practical implementable model which is holistic, scalable, theory based, business oriented and provides visual view capability.

### 3.1.4 Hypotheses

Since the Indian software service providers need to provide acceptable service quality to their customers in the light of various existing and emerging threats to their customers strategic data or information by adopting reasonable and good information security practices within the organization else there would be a perceived gap by the customer in the service delivery of the service provider. Hence there is a relationship between information security practices followed
within the service providers' organization and the service quality gaps model. The motivation in this study is to use existing models by leveraging prior disjointed research in the areas of information security and service quality by bringing them together and providing a coherent linkage between theoretical approach, the framework conceptualization and practical implementation by utilizing a combination of the existing theories.

The assumption is that the various security determinants as identified in literature and in the business model for information security can be mapped to the service design and service performance in the service quality gaps model. The research model for the conceptual relationship between service quality gaps model and business model for information security is shown in figure 13.

Figure 13: Conceptual framework of the modified service quality gaps model with information security considerations using business model for information security

[Source: Results undertaken by Author]
The hypothesis is that this research model would help to:

1. Examine the information security practices followed by the Indian software services industry, and
2. Identify, including visually, areas of weakness, if any, in the select dimensions of service design gaps and service performance gaps of the service quality gaps model which could lead to perceived service quality gaps in the delivery of security services from the Indian software services providers’ perspective.

3.1.5 Methodology

Since this is more of an exploratory study it employs theory, methodological and data triangulation to enhance confidence in the conclusions from the primary and secondary data collection and its findings. The approach comprised of (1) literature review to identify determinants of security for trusted software services, as covered above (2) identification of research models where these determinants could be used and which could help understand the service design and service performance from a security perspective in more depth and detail, as covered above (3) using triangulation to arrive at conclusions from the selected models and analyzing the outcome for discussion and findings.

Theory triangulation was applied during literature review and identification of research models, wherein different perspectives were reviewed.

Literature review perspectives reviewed were:

(1) trade, economics and social sciences
(2) outsourcing, offshore software development and supply chain
(3) risk management and security with respect to management, legal and technical aspects.

The research models were studied with a perspective of:

(1) service quality
(2) predictive threats
(3) information security from a business perspective covering systems theory and complexity theory.

On the selected research models, in this study methodological and data triangulation [Creswell and Miller 2000; Gable 1994] has been used. This included using multiple methods of data collection and data analysis to enhance confidence in the resulting findings. Methodological triangulation has been used as more than one method for gathering data was adopted:

- field survey based on focus group discussions,
- secondary data, and
- face to face interviews.

For the data triangulation:

- data at different times has been collected for the field work as well as for the secondary data;
- it covered different people, and
- different social situations.

The triangulation approach was followed for the following reasons:

1) Security surveys and breach statistics can be unreliable because many organizations are unwilling to report security breaches for fear of attracting adverse publicity and fear of incurring financial loss.
2) Much of the available data becomes historical fast and, in a dynamic environment where threat capability and motivation can change overnight, it may not have much predictive validity.
3) By following triangulation it helps to reduce the overall bias in data and in enhancing the verification of findings and derived conclusions.

3.1.6 Data Collection

Methodological and data triangulation carried out as part of this study, are explained as follows:
1) Carrying out two field surveys covering 14 organizations each time in an interval separated by almost ten months in the year 2009 and 2010 based on prior focus group discussions to arrive at the questionnaire for the field survey (Appendix 1). The participants in the focus group discussions were the security chiefs of the respective organizations and these discussions were held twice for a period of four hours each to arrive at the final questionnaire. The objective was to arrive at a structured approach to study and understand the threats that mattered to the organizations the most and where the organizations would deploy their limited resources to mitigate these threats. The data was collected using different means - physical printouts as well as web email.

2) To validate the field survey findings, the available survey literature or secondary data was studied (3 different credible surveys were studied in detail all pertaining to India:
- one surveyed 150 organizations of which 51 were IT / ITeS organizations [DSCI and KPMG 2009];
- the second surveyed 140 organizations of which 45 were IT / ITeS [CERT-In, PwC and FICCI 2007-2008];
- and the third surveyed 35 organizations at Capability Maturity Model Level 4 and Level 5 within the Software / Outsourcing verticals [AMI-Partners 2010].

These surveys covered the years 2007-2008, 2009 and 2010.

3) To further validate the understanding from the field survey and secondary data, face to face interviews with nine of the prominent Chief Security Officers in the Indian IT industry were conducted. Each face to face interview was carried out over a period of approximately half hour.

3.1.7 Data analysis
The data collected was analyzed separately for secondary data based model and for the field work based model. Since there is no established and recommended measurement model for the business model for information security to arrive at its equilibrium state or disturbed state, the measurement approach followed in the study was to tabulate the findings using a frequency distribution method and then map them on to the business model for information security. The summation of the frequency distribution from the findings of the three secondary data / surveys were used to increase or decrease the size of the elements and dynamic interconnections. A value of 1 was considered as 1 unit, a positive remark provided a positive value and a negative remark provided a negative value to arrive at the overall value or unit, so as to represent the elements and dynamic interconnections visually and see the push / pull forces on the equilibrium of the model (figure 14) on a relative scale.

Figure 14: Business model for information security based on the secondary data (The four elements are of different sizes and the six dynamic interconnections are of different thickness)

[Source: Results undertaken by Author]

During both the field surveys focus group discussions were held to identify and list the various information security threats that were perceived as critical by the focus group. The group
produced a list of twenty five threats. From this list, fifteen threats were identified based on frequency distribution which the focus group felt were relevant for handling, were manageable from a practical perspective and would also cover the remaining left out threats in their view. These fifteen threats (see Appendix 2 for the list of threats) were then sent to 14 participant organizations to be rated across three dimensions - business impact of the threat; likelihood of the threat; and efforts involved / cost to mitigate the threat, on a scale of 1 to 5 where: 5=Strongly Agree, 4=Agree, 3=Neither, 2=Disagree, 1=Strongly disagree (this scale is useful in research and practice [Zheng et al. 2002]).

Based on the inputs received, the arithmetic mean scores were calculated for each of the fifteen threats against each of the factors for the three dimensions. These were then ranked to arrive at predictive threats – those that required immediate attention or focus, those that required active management, those requiring a business contingency plan and those that could be delayed for implementation as the risk was considered low (Appendix 3).

Each of the predictive threats was mapped to the elements or to the dynamic interconnections of the business model for information security.

For the face to face interviews thematic analysis was carried out wherein

- the interviews were converted to a transcript,
- coherent thoughts were identified,
- grouping was carried out on these coherent thoughts and
- then the themes were identified.

Each of the themes was mapped to the elements or to the dynamic interconnections of the business model for information security.

The summation of the frequency distribution from both, the predictive threat model field survey findings and face to face interviews findings were used to increase or decrease the size of the elements and dynamic interconnections. A value of 1 was considered as 1 unit, so as to represent them visually and see the push / pull forces on the equilibrium of the model (figure 15) on a relative scale.
Figure 15: Business model for information security based on the field work (The four elements are of different sizes and the six dynamic interconnections are of different thickness)

As a final step, the two business models for information security namely secondary data based model and field work based model, that emerged were combined together to provide a single view of the business model for information security (figure 16) so as to understand its equilibrium and the service quality gaps, if any, to arrive at the findings. The final result of the research model is depicted in figure 17.
Figure 16: Business model for information security based on the secondary data and field work combined (The four elements are of different sizes and the six dynamic interconnections are of different thickness)

Figure 17: View of the Service Design Gaps and Service Delivery Gaps with respect to information security using the business model for information security along with the service quality gaps model
The business model for information security was also looked at from the trust perspective. Using the Trust bibliography [Arnott 2009] comprising of 655 research articles, the topics were mapped to the four elements and six dynamic interconnections and are tabulated in table 5:

Table 5: Mapping of Trust bibliography research articles to elements and dynamic interconnections of the Business Model for Information Security

<table>
<thead>
<tr>
<th>Disciplines - Elements and Dynamic interconnections</th>
<th>Number of research articles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Design and Strategy</td>
<td>67</td>
</tr>
<tr>
<td>People</td>
<td>32</td>
</tr>
<tr>
<td>Process</td>
<td>196</td>
</tr>
<tr>
<td>Technology</td>
<td>44</td>
</tr>
<tr>
<td>Culture</td>
<td>20</td>
</tr>
<tr>
<td>Architecture</td>
<td>63</td>
</tr>
<tr>
<td>Governing</td>
<td>143</td>
</tr>
<tr>
<td>Emergence</td>
<td>41</td>
</tr>
<tr>
<td>Enabling and support</td>
<td>28</td>
</tr>
<tr>
<td>Human factors</td>
<td>21</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>655</strong></td>
</tr>
</tbody>
</table>

[Source: Arnott 2009 and Results tabulation undertaken by Author]

3.1.8 Findings and results

The key points that emerged from the secondary data and field work were consolidated under the elements and dynamic interconnections of the business model for information security to gauge the equilibrium of the model.

From the secondary data it is observed that the Indian Software Services Providers are laying focus on governing, people, technology and enabling and support for providing information security practices to their customers. The challenge identified by the Indian Software Services Providers is in human factors, architecture and culture. These are clear when we look at results in
the secondary data for architecture such as compromised user accounts, data leakage, non-encrypted emails and for human factors such as insider threats and account permissions. One of the major factors identified for challenges in implementing robust information security practices is employee non-seriousness. This is a culture challenge. Since culture in the literature review [ISACA 2009] is defined as a pattern of behavior, beliefs, assumptions, attitudes, and ways of doing things in an organization by the people. This secondary data finding may well indicate that security is not deeply ingrained as part of the organization design and strategy. Hence it is a corporate governance issue.

It is also noticed from secondary data that there are emerging concerns among the Indian Software Services Providers around application security, privacy and access to personally identifiable information by employees. It was also observed from the secondary data that application security was not yet a critical deciding factor for award of contracts to Indian Software Service Providers. The Capability Maturity Model (CMM) level 5 companies were focusing to build application software as part of their process (meaning they were trying to be proactive) while the CMM level 4 companies were following a client centric approach (meaning that they were reactive and would do what the customer required as per the contract between the parties).

Since there is focus on governance and a gap regarding architecture, it is evident that there is no synchronization between the overall security strategy and overall security architecture. This means that the business goals and objectives cannot be shown linked to the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth [Ilie and Parikh 2004]. This is critical because it is here that one can describe how the different security controls are placed and their relation to the overall IT architecture which is aligned to the business goals of the enterprise.

Based on the visual thickness of the different dynamic interconnections, it is evident that the model can snap due to weak dynamic interactions of architecture, issues around human factors and culture. This shows that the organizations should be focusing towards these areas by either putting more effort and resources in these areas or reducing from other areas where it is much more so as to create a balance.
Establishing on the field work carried out which involved the predictive threat model and face to face interviews, it was observed that the Chief Security Officers were concerned with the threats falling in human factors, technology, governing and emergence areas. They addressed architecture to an extent but did not consider culture. The model can snap due to weak dynamic interactions of human factors, emergence and culture due to governing. Since culture flows from corporate governance in the organization this is an area which needs to be addressed and this is what the field survey results are depicting in terms of weakness in governing.

Building on the combined view (secondary data and field work) of the business model for information security it indicates that there is a gap in the Service Design and Service Delivery with respect to security since the model is not balanced due to the different size and thickness of the elements and dynamic interconnections. Clearly the weak links in the final model emerge as culture, architecture and human factors which are creating an unbalance.

These findings above are similar to the ones found by the Ponemon Institute [2013] in their study of organizations across industries globally as shown in chart 9. It shows that not focusing on human factors, culture or architecture can lead to errors, breaches, theft or failures which compromise the confidentiality or integrity or availability of data.

Chart 9: Common threats ranked in terms of economic impact

[Source: Ponemon Institute 2013]
Probably the Indian software service providers understand the impact of data breaches on their brand as well as on the industry and country as a whole and that is why the Indian software service providers are focusing strongly on areas such as governing, people, technology and process so that they address the common threats and deliver undisrupted IT services and operations to their customers for a long term partnership based on trust. The study by Luor et al. [2008] indicates that security is the most important belief impacting trust and that trust is an important outsourcing factor. Trust is used to solve specific risk problems [Luhmann 1988]. It is also documented in literature that trust, security and business maturity between the outsourcer and outsourcing service provider define the success of outsourcing [Fink 1994; Khan et al. 2003; Lee et al. 2008]. Further, Luhmann [1988] mentions that if a dreadful end result would make one repentant then trust is required and the attribution of a bad decision is then internal and not external. Interpreting this in the context of outsourcing means that if the relationship fails or turns ugly due to a security breach then, though both the parties would suffer dreadful business losses, the internal decision to outsource to the specific outsourcing service provider would be under scrutiny. The table 5 shows that trust has been studied in various disciplines. These disciplines work together in complex relationships within the organization including in the context of information security. This makes trust an extremely complex, multi-dimensional and dynamic concept just as information security. It also probably explains that trust is the binding glue within the organization for all the four elements and six dynamic interconnections. The intraorganizational trust has an impact on the interorganizational trust and reliability [Sydow 1998].

Both the hypothesis are validated since one is able to examine the information security practices followed by the Indian software services industry, and also identify, including visually, areas of weakness in the select dimensions of service design gaps and service performance gaps of the service quality gaps model.

Despite the model not being in an equilibrium state and there being a gap in the service design and service performance thereby impacting service delivery, it does not create a customer gap. The reason is that this is still better than what customers seem to have at their own end and hence the customer tolerance limits are not breached by the Indian software service vendors. This is also indicated by [CERT-In, PwC and FICCI 2007-2008], which clearly states that based on
global benchmarks, Indian organizations are ahead, better and focused when it comes to security practices being followed.

The analysis of this study is the following:

1) Though the equilibrium of the Business model for information security is disturbed as per the findings, it is seen that there has not been any change in the overall Indian software exports percentage and the overall software export figures have continued to grow.

2) The Business model for information security clearly highlights that there are service design gaps and service performance gaps as part of the Service Quality Gaps Model thus creating a gap between expected service and perceived service or the customer gap.

3) Since the service design and service delivery in the Service Quality Gaps Model is primarily customer driven and as has been concluded here that the equilibrium of the Business model for information security is disturbed, it can be inferred that the equilibrium of the Business model for information security at the customer end probably is also disturbed.

4) A disturbed equilibrium of the Business model for information security will not impact software exports growth adversely since it qualifies as an acceptable service quality as long as the customer gap remains within tolerance limits, as defined and perceived by the customer.

3.1.9 Conclusion, limitation and suggestions

Apart from the above four main analysis, it is evident that to safeguard the customer data or information Indian software service providers are putting strong emphasis on people, technology, process, emergence and enabling and support. There seems to be gaps at the organization, culture, architecture and human factors. There is a strong focus on governing but there are also serious gaps as in culture and architecture which stem from corporate governance. These gaps are contributing to service design gaps and service performance gaps as part of the Service Quality Gaps Model thus creating a gap between expected service and perceived service or the
customer gap. However despite the customer gap, the overall Indian software exports percentage and the overall software export figures have continued to grow as the customers perceive that their data or information is safe at the service provider’s end. This helps towards trust building with the customer. 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. This leads one to explore this relationship between governance, service quality and performance further which is taken up in the next section.

Due to a lack of an established measurement method for the business model for information security it is suggested that future research be directed towards this area. Future research should compare the business models for information security at the vendor and customer side to study the alignment and differences that may emerge.

To improve the overall information security practices in a supply chain, the acceptable service quality as defined and perceived by the customer needs to be raised to a higher level both within their own organization and at the service provider end. The service providers in the supply chain should explore the process of self-attestation wherein they lay out the information security practices and the required information security activities to claim they have a balanced business model for information security thereby helping create more secure outcomes transparently.