Telecom industry has gone through significant expansion phase and industry is committed to remain on growth path exploring new avenues.

Data services have become one of growth driver for the industry with increasing internet penetration and broadband adoption. At the same time, m-Commerce is been considered a great opportunity to expand business beyond just voice & data services.

Telecom industry has evolved significantly over the last five years and during this period there has been increased requirements to have robust information security environment. Also, with the industry having stringent legal and regulatory information security requirement, there is an enhanced focus on the subject across telecom operators.

This report explores on various areas that are relevant for telecom operators from information security perspective in the current context. Also, it focuses on the need to have robust security framework for meeting up with newer requirements that shall emerge with newer and more advanced technologies.
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Network Security</td>
<td>5</td>
</tr>
<tr>
<td>Customer Privacy</td>
<td>9</td>
</tr>
<tr>
<td>Internal Organization Security</td>
<td>13</td>
</tr>
<tr>
<td>Third Party Security</td>
<td>17</td>
</tr>
<tr>
<td>Changing face of Technology</td>
<td>21</td>
</tr>
<tr>
<td>Footnote</td>
<td>23</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>24</td>
</tr>
</tbody>
</table>
Introduction

Telecom services has been one of the key growth sectors in India. The sector has recorded a growth of 12 percent during 2010-11 as compared to 7 percent during 2009-10. The revenue during 2010-11 is INR 119845 cr\(^1\). The sector has revolutionized the way of communication in country, including providing additional services options to subscribers (VAS, mCommerce, High speed internet, etc). The revenue is expected to grow further during 2011-12 when the 3G services are rolled out in more towns. With the increased range and scale of services, the sector is exposed to multiple forms of information security and data privacy related risks.

\(^1\) http://www.indiatelecomonline.com/tag/telecom-revenue-growth-2011/
Stakeholders inclusive of the regulators for this sector are in the process of evolving effective control mechanism to overcome the new risk introduced in the environment. These include the amendments to UASL agreement, Draft NTP 2011 policy, IT (Amendment) Act 2008, etc.

Control Environment in Telecom Ecosystem

Telecom operators are governed by the regulations laid down by regulatory bodies such as Telecom Regulatory Authority of India (TRAI), Department of Telecom (DoT), Telecom Dispute Settlement Appellate Tribunal (TDSAT), Group on Telecom & IT (GOTIT), Wireless Planning Commission (WPC) and Telecom commission which also include information security requirements. Further, the recent Unified Access Service License (UASL) amendment extends information security to the telecom networks and also to the third parties of the operators.

Adherence to evolving regulatory requirements can be achieved by having a collaborative and holistic approach whereby various stakeholders need to work together including telecom operators, equipment manufacturers/suppliers and third party service providers.

Effective implementation measures should include an Information security governance framework that spans across the organization. While most of the telecom operators in their current operations have been able to formalize an Information security governance framework in the Information Security (IS)/IT function, it would be imperative to have this extended to the telecom networks.

Information Security Landscape

Information security has been an evolving process for telecom operators which has been driven by:

- Security incidents
- Increased size & complexity of operations
- Changing technology and complexity of services
- Regulatory environment.

While all the telecom operators carry some level of information security risks, the degree of risk and the ability to mitigate these depends upon the maturity of the organization.

Two major drivers for information security initiatives are:

- Legal and regulatory requirements
- Internal controls environment

Major information security focus area:

- Comprehensive information security risk assessment covering the entire organization
- Understanding and addressing legal & regulatory requirements
- Focus on information security in holistic manner covering telecom network, equipments and IT systems
- Strengthening internal organization security with changing threats and operational requirements of business
- Third party security being part of the Information Security Framework
- Defining an operations control framework for maintaining privacy of sensitive information
- Continuous assessment of risks emerging from new technologies and defining controls to mitigate them.

Legal & regulatory requirements hold the telecom operator directly accountable for ensuring effective information security environment. Whereas, mature telecom operators’, by means of their internal controls, extend these responsibilities to third parties as they are integral part of their information lifecycle.

Considering the operating model adopted by most of the telecom operators in India, ensuring information security at third parties is essential to ensure complete coverage of information security landscape.
Compliance to legal and regulatory requirements is extremely critical for an operator to sustain its operations.

An operator’s focus to build internal organization security should increase in order to have a robust business and operations environment.

Tighter control on internal organization security enables telecom operators to mitigate security risks (existing and emerging) arising from various external and internal sources.

Telecom operators continuously need to evaluate, monitor and mitigate the security risks emerging out of new technologies which they adopt to diversify their services, such as mCommerce.

Telecom operator need to extend their information security framework to third party organizations, to mitigate and prevent risks arising from extended organization boundaries.

Customer privacy can act as a competitive advantage in current scenario where customers are becoming more aware and demanding better privacy.
The National Telecom Policy Draft - 2011

The Draft National Telecom Policy – 2011 (NTP-2011), released on 10 October, 2011 directionally sets the groundwork for the next round of transformation in the Indian telecommunications sector. Although details on key issues, such as license renewal, spectrum pricing, spectrum re-farming and consolidation guidelines, are still awaited; the policy framework demonstrates a directionally mature and optimistic approach. One of the key focus areas of Draft NTP – 2011 is security, which is in many way aligned to the requirements emerging from regulator and UASL agreement.

This report provides an overview of the key information security risks and the suggested framework/ steps that telecom operators should adopt. This report covers key aspects of information security i.e.:

- Network Security
- Customer Privacy
- Internal Organization Security
- Third Party Security
- New Technologies & Services
Network Security

Telecom operators have a complex network, which comprise of network elements belonging to different vendors which are mostly proprietary applications, operating systems, and protocols, which remains an unknown for telecom operators. The scenario is more complex for telecom operators that have network elements from different OEMs. Further, with outsourcing of network management, contract with multiple network vendors adds to the complexity.
Network security has been key aspect of the addition to legal & regulatory requirements through amendment introduced by DoT, on 31 May 2011, to the telecom operator’s license terms and conditions (UASL agreement) which refers to enhancing security in telecom operator environment. This amendment has provided an opportunity to operators to have a more comprehensive view on overall information security and risks across the organization, covering telecom network which is an integral part of the operations.

**Key implications of the amendment include:**

- Network security responsibility is with Telecom Service Provider (TSP)
- Operators to audit their network (internal/external) once a year
- Pre-Certification for vendor network equipment /IT systems prior to insertion into the network
- Only Indian nationals shall be leading key positions in technology function, covering CTO,CISO and nodal executives in-charge of GSMC, MSC, Soft switch, Central database and system administrators
- Mandated to keep records like software details, updates and changes; operation & maintenance procedure manuals and command logs; supply chain of products
- Operators to monitor all intrusions, attacks and frauds and report the same to licensor and to CERT-IN
- Right to vendor audit (i.e. service providers to TSP) with DoT (or designated agency) and expenses to be borne by vendor
- Financial penalty of INR 50 crore per security breach
- Continuous assessment of risks emerging from new technologies and defining controls to mitigate them.

**Key Timelines/ Milestones**

- License terms updated
- Network security and security management policies and procedures to be shared with Licensor
- Network audit – Year 1
- SoC to be set up within 12 months and periodic reporting to CERT-IN/ DoT

31 May 2011 | 30 June 2011 | 1 till 31 May 2012 and thereafter once every year
Challenges in meeting Network Security requirements

**CHALLENGES**

- Vast Spread of telecom network
- Ever changing technology and business architecture
- Third party management of network
- High cost of Implementation
- Operational sustenance of security landscape within the organization

- Telecom network comprising of equipments from various vendors and spread across the country (operating circles)
- Ever expanding network
- Lack of clear visibility on equipments deployed and thus there security implications

- Newer business requirements and new services.
- Increased network architecture complexity

- Different services providers across zones
- Network equipment deployed by vendors mostly proprietary in nature
- Unaware of all vulnerabilities due to uniqueness of these equipments

- Cost associated with security audit of all the network equipments
- Cost for assessments across networks due to non standardization across equipments
- Cost of maintaining records of all calls & data for 12 months

- Need for specialized skills & experience for critical activities
- Employ only Indian nationals for critical positions/roles
- April 1, 2013, the certification shall be got done only from authorized & certified agencies/labs in India.

Ensuring effective implementation

Strong and focussed network security controls can be achieved by:

- Carrying out a comprehensive and holistic information security risk assessment to identify high risk areas that need to be focussed
- Establishing an advanced network security function with the operator organization
- Collaborate with specialized, skilled and experienced professionals to ensure robust security controls
- Setting up a mechanism for continuous two way communication between the operator network security function and the vendor/service provider
- Continuous evolution of security function and adoption of technology solutions to meet network security requirements
- Ongoing monitoring of the security regulatory environment to determine the various threats and initiatives required to be carried out.
Customer Privacy

With increasing customer awareness about the sensitivity of their personal information, customer privacy has become an important focus area for the operators. However, the initiatives for implementing customer privacy controls are in nascent stage.
Telecom operator’s deal with the end customers at all times through web, third party agents and their own employees. This makes it imperative to have customer privacy maintained at all levels. Government of India through IT (Amendment) Act, 2008 and other regulatory requirements is making sure that customer privacy is maintained. Compromise of customer information can have financial as well as legal implications. Further, with many telecom operators venturing out of India, data privacy laws applicable in other countries also become applicable for operators supporting services in those geographies.

**IT Act 2008 amendments Applicability to Telecom**

Regulatory requirements such as IT (Amendment) Act, 2008 also become applicable to telecom operators from the perspective of ‘intermediary’ and ‘body corporate’.

| Section 43 A : Compensation for failure to protect data |
| Section 66 C: Punishment for identity theft |
| Section 72 A: Punishment for disclosure of information |
| Section 84 A: Liability of Intermediary |

- A body corporate shall be liable to pay compensation if it is negligent in implementing “reasonable security precautions” with respect to “sensitive personal data”
- Any person shall be liable to punishment for fraudulent or dishonest use of any unique identification feature of any other person
- Any intermediary shall be liable for punishment in case of wrongful gain or disclosure of any material containing information of another person in breach of lawful contract
- The central government may, for secure use of electronic medium and for promotion of eGovernance and eCommerce, prescribe the modes or methods for encryption.

*This is not a comprehensive list and just identifies some of the clauses, part of ITAA 2008, applicable to telecom operators*
Various forces associated with Customer Privacy

In India’s macro environment, there are various forces that drives the need for controls to be put in place to ensure customer privacy. In Indian macro environment, ensuring customer privacy has Social & Economic factors associated with it which is a challenge to overcome. At the same time, Regulatory & Technological forces also play an important role in creating a need for customer privacy.

Customer Privacy – Varying Viewpoints

Privacy needs to reflect on from three stakeholder’s perspective:
- business,
- customer and
- regulator.

All stakeholders requirements needs to be satisfied by striking a balance between their need to collect/share customer personal information and need to secure customer personal information.

Where, customer personal information might be required for identifying business opportunities, providing better services and verifications purpose. At the same time, there is a need to secure customer personal information to prevent misuse of this information.
Customer Privacy as a competitive advantage

The telecom sector in India is growing at a staggering pace and the key to attract new customers is by establishing a brand image, which is reliable and sensitive to the customers. In the age of Mobile Number Portability (MNP), customer confidence and loyalty remain the only barriers to switching from one operator to another. Privacy of customer information can act as one of the key differentiating factor and can help increase customer loyalty.

To achieve this, telecom operators need to understand the key drivers and controls to establish an effective customer privacy program. Operators need to look not only within their operating environment but also at their third parties to ensure that customer personal information is handled securely. Having a robust control framework and implementing it throughout the organization and the third parties can help the telecom operators ensure adequate customer privacy.

Establishing Customer Privacy

Customer privacy needs to be ensured throughout the lifecycle of customer information which can be done by having a holistic framework which includes:

- Identifying the right set of information to be captured and the purpose for the same
- Having a complete and exhaustive inventory of the customer personal information
- Identifying the right level of access to the information basis the classification
- Privacy principles related to (collection, notice, disclosure of information ) being integral part of the business processes
- Extending the customer privacy across third parties
- Improving the sensitization towards customer privacy requirements across business functions.
In light of the fast-paced scale up at various telecom operators, internal organization is emerging as a focus area for information security. Lack of employee seriousness towards information security, vast geographical spread and lack of uniformity of controls are the key challenges in ensuring effective internal organization security. Further, there exists a need for establishing an Information Security Organization Structure that includes both IT and network function.
Internal organization security initiatives are driven by an organization’s risk appetite. However, there are regulatory requirements such as the IT (Amendment) Act, 2008, TRAI and UASL requirements, which cover the aspect of Internal Organization Security. The section 43A on body corporate in IT (Amendment) Act, 2008 lays down requirement for implementing and maintaining reasonable security practices and procedures on companies possessing, dealing or handling any sensitive personal data or information in a computer resource owned by them. Companies can be held liable to pay damages by way of compensation to person affected by breach of the requirement.

**Challenges towards Internal Organization Security**

In the initial years of operations, the organizations tend to focus more on regulatory requirements and external risk factors. Further, vast spread of operation & services, large employee strength, involvement of third parties, complex infrastructure and short turnaround time makes ensuring internal organization security a big challenge.

However, as the organizations mature, their security posture also matures to the extent that internal information security becomes a basic hygiene for carrying out business operations.

Some of the challenges to the Internal Organization Security are depicted below:

---

Source: KPMG in India Analysis - Information Security in Telecom Sector

© 2011 KPMG, an Indian Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
Establishing a culture for information security

While internal information security can be enforced by establishing technology controls and performing periodic audits, the success of such initiatives would largely depend upon the acceptance level of the employees. Telecom operators need to look at establishing a culture where information security becomes part of the DNA of the organizations and thus there employees.

In most of the organizations, Information Security focuses on IT and does not include core telecom network. There is a need for a holistic Information Security Organization Structure that integrates security in IT and core telecom network. Further, the effectiveness of Information Security can be ensured by involving business functions in security initiatives.

Establishing Internal Organization Security

Internal information security can be achieved by imbibing security as part of work life and implementing controls to enforce information security. Adoption of the below steps can facilitate in bringing about this change:

- Establish a robust framework (such as ISO 27001) along with Information Security Management Office for driving security across organization
- Establish a consolidated framework driving synergies from various information security initiatives within the organization
- Develop a structured program of making employees/vendors aware of their information security responsibilities across geographical locations and business functions
- Make the employees accountable for information security by having security as part of their employment contract or job description
- Implement security solutions such as Digital Rights Management (DRM), Information Leakage Prevention (ILP) for enforcing security at the end user level
- Constant monitoring and learning to be included in the organization wide framework.
Most telecom operators work on an outsourcing model involving various third parties, which significantly challenges operators’ information security posture. In such an environment, the success of ensuring information security depends on the ability of an organization to effectively extend their security framework to its third parties.
Telecom operators regard outsourcing as a strategic option that brings agility in business, saves cost and provides bandwidth to focus on core competencies. This multi party involvement to deliver services to end customers involves sharing of information between the third party service provider and the telecom operators, which exposes them to a different set of information security risks.

**Challenges in implementing secured third party environment**

Managing information security at third parties such as infrastructure provider, system integrator, software vendor, retailers & distributors, VAS provider, bill printing agency etc. is a challenging task due to limited control over the third party environment. Because of the increasing number of third parties and the risks associated with outsourcing, including security controls as part of the contract has become a norm. However, ensuring adherence to the controls and establishing the accountability for the same becomes challenging in today’s environment.

**Operating as one big family**

Each business function at telecom operator has outsourced some or all parts of its operations to various third parties and it is critical for organizations to manage third parties in an efficient manner. These third parties are like extended arms of the operators without which the operators would not be able to function.

While the process for identification of and contracting of these third parties has been centralized at majority of the operators, business functions still need to interact with the third parties independently for their day to day operations. Hence, it is essential that each function understands the importance of security and imbibes it in its relationship with their third parties.

Telecom operators have adopted various means to achieve information security at third parties. However, the steps adopted vary from operator to operator depending upon the maturity and complexity of the third party environment, services provided and relationship with the third parties.

**Key challenges towards establishing and strengthening security at third parties:**

- Establishing security governance;
- Classification of third parties for relevant security controls being applicable
- Identifying of Key Performance Indicators (KPIs) for information security
- Aligning the security policy of the third parties with the operators security requirements
- Enforcement of security requirements through contracts/ SLAs
- Cost for periodic assessments of third parties
- Extending the business continuity beyond organizational boundaries to third parties.
Steps for Third Party Security

- Define detailed security process for selection of third party to ensure baseline information security measures
- Design contracts with third parties containing information security requirements and KPIs/SLAs
- Implement a structured periodic risk assessment process with third parties
- Identify a Information Security SPOC (preferably dedicated) from third party service provider
- Formalize controls considering third parties as extended boundaries of organization.

Information security could be ensured at larger third party vendors by means of contracts and adherence report, since they have the resources required to build controls and ensure compliance. However, more focused approach is required for small sized third parties, where telecom operators educate their personnel on information security and conduct periodic risk assessment.

Consequently, operators are now looking at taking more and more control into their hands. One good example of this is the management of infrastructure for the call centres. Earlier call centres were required to manage the infrastructure for servicing the operators; this model is now witnessing transition wherein the operators are taking over the management of call centre infrastructure in a co-hosted environment.
Mobile telecommunication technologies and Internet are setting contours of further technological progress. Majority of the Indian telecom operators are adopting leading industry practices to ensure that they are prepared against possible security threats from emerging new technologies.
The need for efficient, sustainable, cost effective and profitable way for business is the driver for innovation and emergence of new technologies & services. The advent of technologies such as 3G, New Generation Networks (NGN), Wi-Max and use of services such as M-Commerce, Cloud-computing services etc will benefit everyone by supporting the proliferation of information, enabling citizens to access vital communication services and promoting the development of technology advancements. However, these technological advancements expose telecom operators to new set of security threats and vulnerabilities.

**Factors contributing in adoption of New Technology & Services**

The Indian Mobile subscribers are looking for more than voice services from the telecom operator. The most recent initiative aims at convergence of voice and data received from multiple sources, both web based and real time video streams, in mobile handheld devices.

Services such as m-Commerce, enables users to perform commercial transaction as well as official communication wherever they go. However, these technological advancements pose a challenge to overall information security landscape with in a telecom operator.

While users download and install Mobile Apps on their devices, the basic security measures such as firewall & encryption needs to be ensured. At the same time, sharing of subscriber’s financial and personal information through these applications on the mobile devices demands a high level of security that will increase customer trust and reduction in possibilities of fraud & leakage.

Moreover, depending on the network technology used for transmission, the bandwidth capacity varies and influences the decision of the end user of kind of services that he would like to avail.

**Outsmarting Technology**

Technology advancements can provide efficient and effective service. There is a need for a strong, multilayered security which will help in protecting networks, not just in 3G world, but also in the future with newer technologies. Few measures like firewalls, VPN, Data encryption and other such security products can help operators survive imminent threats posed by rapid technological advancements. Indian telecom operators can leverage from experience of their global partners who have successfully rolled out new technologies in other geographies.
Telecom Industry in India is going through a dynamic phase triggered by the intense competition, increasingly stringent regulatory requirements and evolving new technologies. In order to stay competitive within the industry, telecom operators are evolving their service delivery model and service offerings to provide new and innovative services to customers in a cost effective environment. This has resulted in a complex security environment for telecom operators which extend beyond organizational boundaries. Telecom operators are focusing to build a sustainable, self evolving, flexible and extendible security framework for meeting the evolving security requirements. Some of these initiatives will include:

- Closely working with the regulatory bodies and third parties to understand and implement regulatory requirements
- Strengthening internal organization security by increasing employees awareness and management commitment for information security
- Defining a collaborative approach with third parties to strengthen the information security in an outsourced environment
- Developing business and operational environment with focus on protecting customer personal information
- Identifying and mitigating the potential impact of emerging technology on the information security landscape.
Acknowledgements

- Akhilesh Tuteja, Partner – Management Consulting;
- Romal Shetty, Partner and Head -Telecommunications;
- Navin Agrawal, Partner – Management Consulting;
- Atul Gupta, Director - Management Consulting;
- Nitin Shah, Associate Director – Management Consulting;
- Vidur Gupta, Associate Director – Management Consulting;
- Deepak Agarwal, Assistant Manager - Management Consulting;
- Nayab Kohli, Assistant Manager - Management Consulting;
- Shubham Singhal, Assistant Manager - Management Consulting
Contact us

**Atul Gupta**
Director - Management Consulting
KPMG in India
T: +91 124 3074 134
E: atulgupta@kpmg.com

[www.kpmg.com/in](http://www.kpmg.com/in)