Cyber Security Practices and Future Plan: Real Scenario in ISPs

Cyber Security

The Service Providers Perspective

By: Samit Jana , ISPAN

30th Jan 2019

.

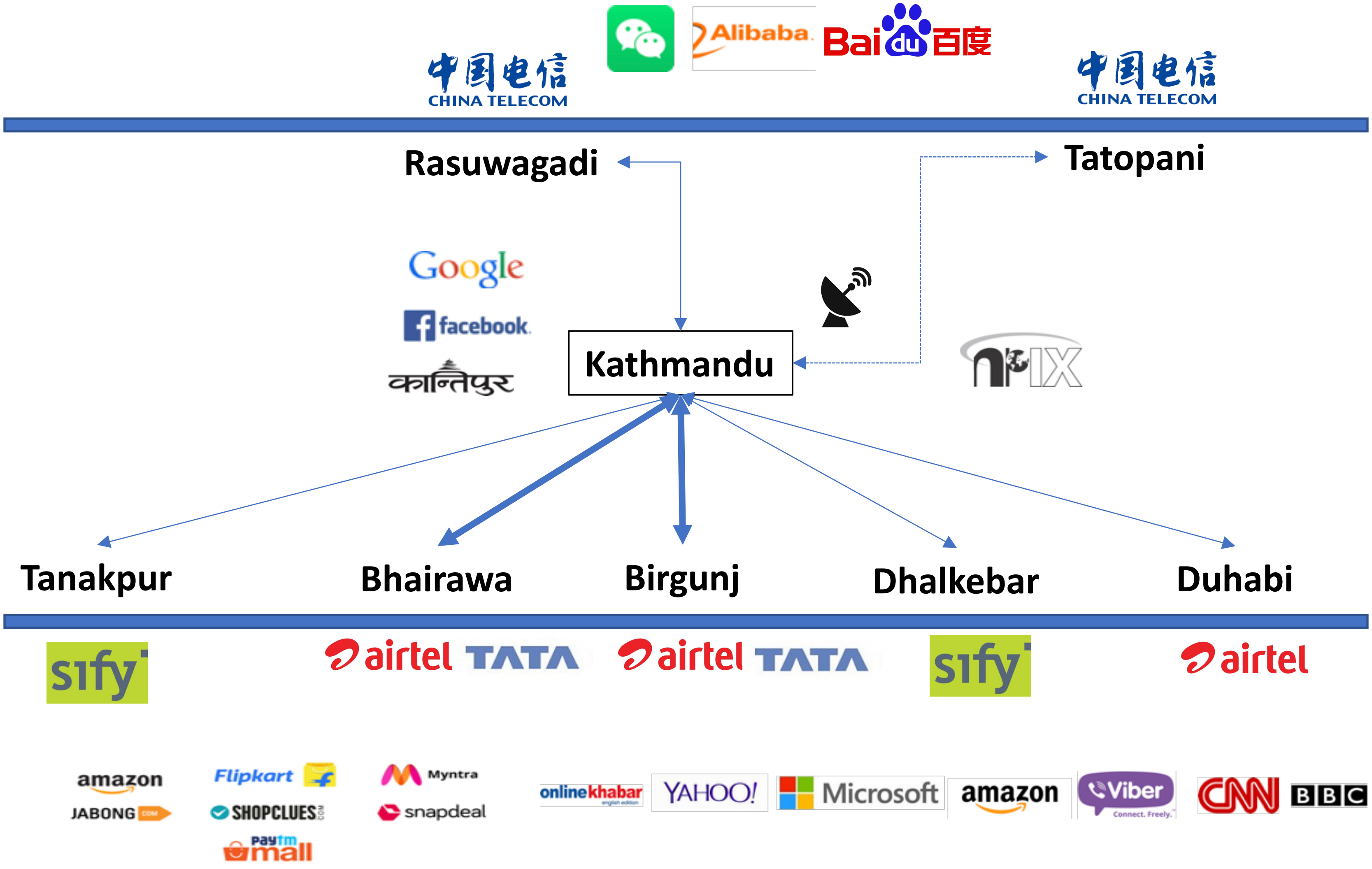
ISPAN: An Introduction

- Internet Service Provider Associations of Nepal, Established in 1998
- Mission to Develop and Provide Affordable Internet for everyone in Nepal
- Promote and Protect interest of ISP and ICT industry as whole
- Works closely with NTA, MOIC, NEA, NDCL, CAN, NPIX and various other agencies in ICT for the development of Internet in Nepal
- 15 officially Members Organization , 100+ unofficially

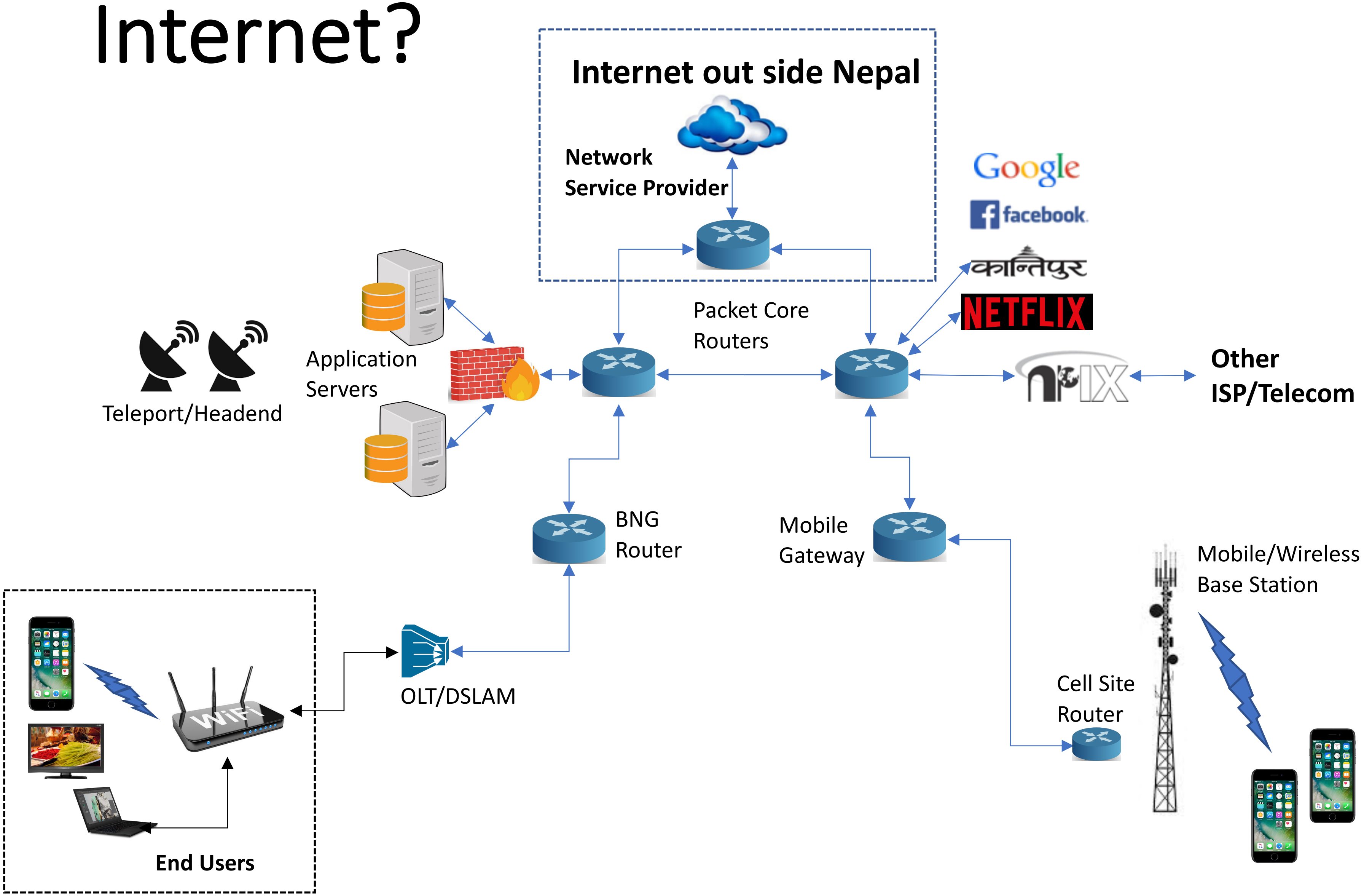
Telecom Sector Statistics:

- 122 registered ISPs ~30 active
- 6 Licensed Mobile Operators 3 active
- 6 Commercial Datacenters in operations
- 38 Millions Mobile Subscribers
- 1Million Fixed Broadband Connections
- 700,000 FTTH connections
- 210,000 ADSL connections
- 55,000 Fixed Wireless connections
- 50,000 Cable DOCSIS
- 2.5 Million Digital TV
- 300,000 IPTV
- Fastest Fixed Broadband and Growth in the Region
- One of the Cheapest Fixed Broadband in the World
- Google & Facebook makes 70% of the Internet Traffic

Our Internet Connectivity to the outside World:



How we are connected to the Internet?



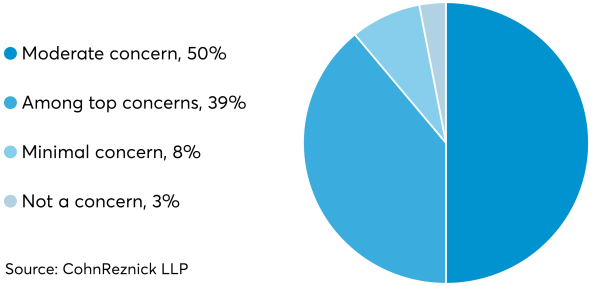
Primary Focus of Service Providers:

- Build Infrastructure for enabling connectivity
- Focus more on accessibility and affordablity
- Increase Service Relialbility

Why are we concerned about Cyber Security today?

Worried, but not worried enough

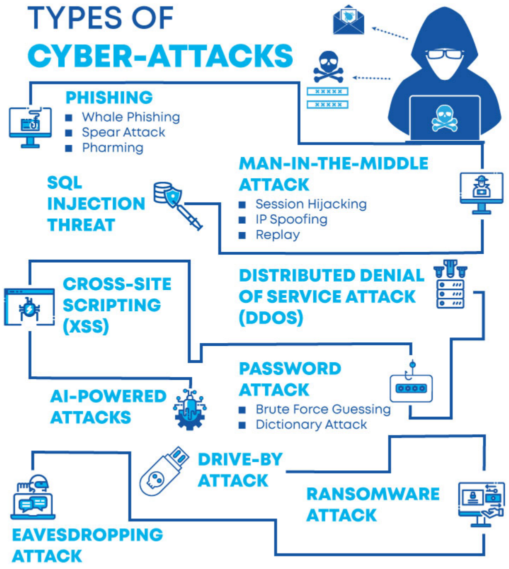
How significant a concern is cybersecurity at your organization?



Source: CohnReznick LLP

- We are Late
- Internet Protocal was not designed for open nature network
- TCP/IP developed by ARPANET for Military Communciation in **Secured** environment
- Basic design criteria: stablity **not** security
- Took almost 20yrs to become Public and Open
  - Unimaginable growth
  - Speed, Reach, Affordablity Triumped Security..!

What does Service Providers do?



- **Own Infrastructure:**
  - Implements Best Common Security Practices (BCP)
  - Analyze Traffic and Flows to detect and mitigate DDOS
  - Manages Firewall/UTM
- **For Government:**
  - Stores Subscribers Internet Lots: AAA, CGNAT, DNS & Web for digital forensic
  - Few Enable v6 – Helpful for forensic but v6 security still remains a concern
  - Block Domain Name and IP address upon request
- **For End Users:**
  - Some provides per DNS based security services in the Internet and Email Security
  - Provides Router, Firewall, IDS, IPS to Enterprise as managed service
  - Awareness programs

Service Providers Dilemma:

- Build Infrastructure focusing on enabling connectivity or security ?
- Focus more on network accessibility and service affordablity or security ?
- How to Store and Analyze the massive amount logs and graphs data with minimal invesment?
- Are we responsible to sniff and analyze user's traffic ?
- Can we do content filtering?
- Traffic Survelliance and Security may degrade network performance?
- Most of the ISPs are already struggling due to high infrastructure capex/opex but low ARPU and stiff competition , can I afford to spend more on security now?

What can Service Providers do ?

- **Collaborate and Facilitate :**
  - Government on Cyber Security Act and Policy formulation
  - Cyber Security Awareness Programs
  - Implement and recommend security BCP for end users and organizations
  - Sharing operational knowledge and Threat Analysis
  - In Digital Forensic helping law enforcement agencies , CERT or SoC
  - Becoming major stakeholders to strengthen National Cyber Security situation
  - To find the right balance between:
    - Security vs Ease of Use
    - Security Cost vs Network/Application Performance

Cyber Security is Best Effort.
It is everyone’s responsibility !

-From Internet