Telecom Security

Vijay Madan

Chief Mentor Tata Teleservices

15th December 2015

Questions we may ask in India?

- What kind of protection is needed and against what threats?
- What are the distinct types of network equipment and facility groupings that need to be protected?
- What are the distinct types of network activities that need to be protected?
- Whether approach based on best practices works?
- Whether approach so far adequate for assuring compliance to National regulatory security guidelines and at the same time addresses business as well as customer needs ?
- Whether the security practices in India are maturing?
- Are the businesses , individuals , corporate, small and medium enterprise still casual or serious about the subject?
- Are the stakeholders aware that they are compromised to various extents and are too worried for ROI and shall wake up when some thing serious happens? Shall it be disastrous ?

Questions that we need to ponder upon?

- Is there adequate built in security architecture and additional overlaying security solutions (actually practiced) and does it address the essential issues?
- Are these strong enough to proactively mitigate known and unknown threats as well as for evolving security threat canvas Are the current measures would result in a reduced cyber incidents impact outcome?
- Do we have a flexible , adaptable security wall, to monitor and address fast evolving end to end threats canvas
- Thus: Do we have robust security ecosystem which addresses the essential issues?
- All the above needs to be examined , considering Telecom as and important and critical infrastructure for the country

Current happenings in India Telecom

- Shift towards Data similar to world
- High tele- density in metros (100% +), approaching 80% in towns, rural 70+ , majorly wireless
- Digital India, quick broadband, Bharatnet, last mile wireless
- 4G roll out, IP based networks, OTTs, VNOs, WiFi hotspots, carrier grade WiFi, steps forward to SDN / SON / NFV
- Large Variety of feature phones, smart phones, grey market, users change phones , not much awareness about security
- Service providers offering solutions along with BW to Government, Corporate, SMEs, HVCs, mobility customers
- Develop ,build, organize , operate, solutions and services
- Great push to M2M, IoT, V6, Cloud, VoLTE….Vitrual world
- eEverything, m-all, many fold increase in upload, whattsapp, FB, Twitter, social, governance , free wifi,……

Security Threats to Telecom Systems

- Telecom infra – though well protected at enterprise levels but a long way to go
- IT enablement – extensive – following best practices but still to go into DNA and culture
- Devices a great fear and the related users
- Down loads without knowledge of rogue sites
- I accept mindset to connect to the world
- Migration to IP, cloud
- Attacks not reported most times
- Sector CERTs still taking shape
- RoI not understood well even by corporate
- Shortage of skilled manpower on security
- Government concerned and acting in PPP mode but a long way to go

Action Points in India

- To protect data, to put security / cyber security systems , many proposed.
- TSPs and ISPs mandated to enhance security by license amendments
- Constantly monitored by the licensor and related agencies.
- Strong Network /IT security policy, safe to connect H/W – S/W, mandatory audits and vulnerability assessment, hardening of network and applications, firewalls and intrusion detection / protection systems, information sharing and analysis systems, internet monitoring systems, secured remote access systems, test labs, equipment certification for security & testing
- SoPs for nodal officers , for both LEAs and service providers; effective and competent CISOs
- IT Act and it's have very strong and good functional clauses

Efforts in India

- **JWGs between industry and the Government with the following guiding principles and objectives that would underpin the public-private partnership (PPP) in cyber security:**
- Given the diverse stakeholders in cyber security, institutional mechanisms should be set up to promote convergence of efforts both in public and private domains;
- Use existing institutions , organizations in both private sector & government, create new institutions where required to enhance cyber security;
- Set up a permanent mechanism for private public partnership;
- Identify bodies that can play a wider role in funding and implementation in the public and private sector;
- Both private and public sector can build capacities for cyber security;
- Put in place appropriate policy and legal frameworks to ensure compliance with cyber security efforts

In India

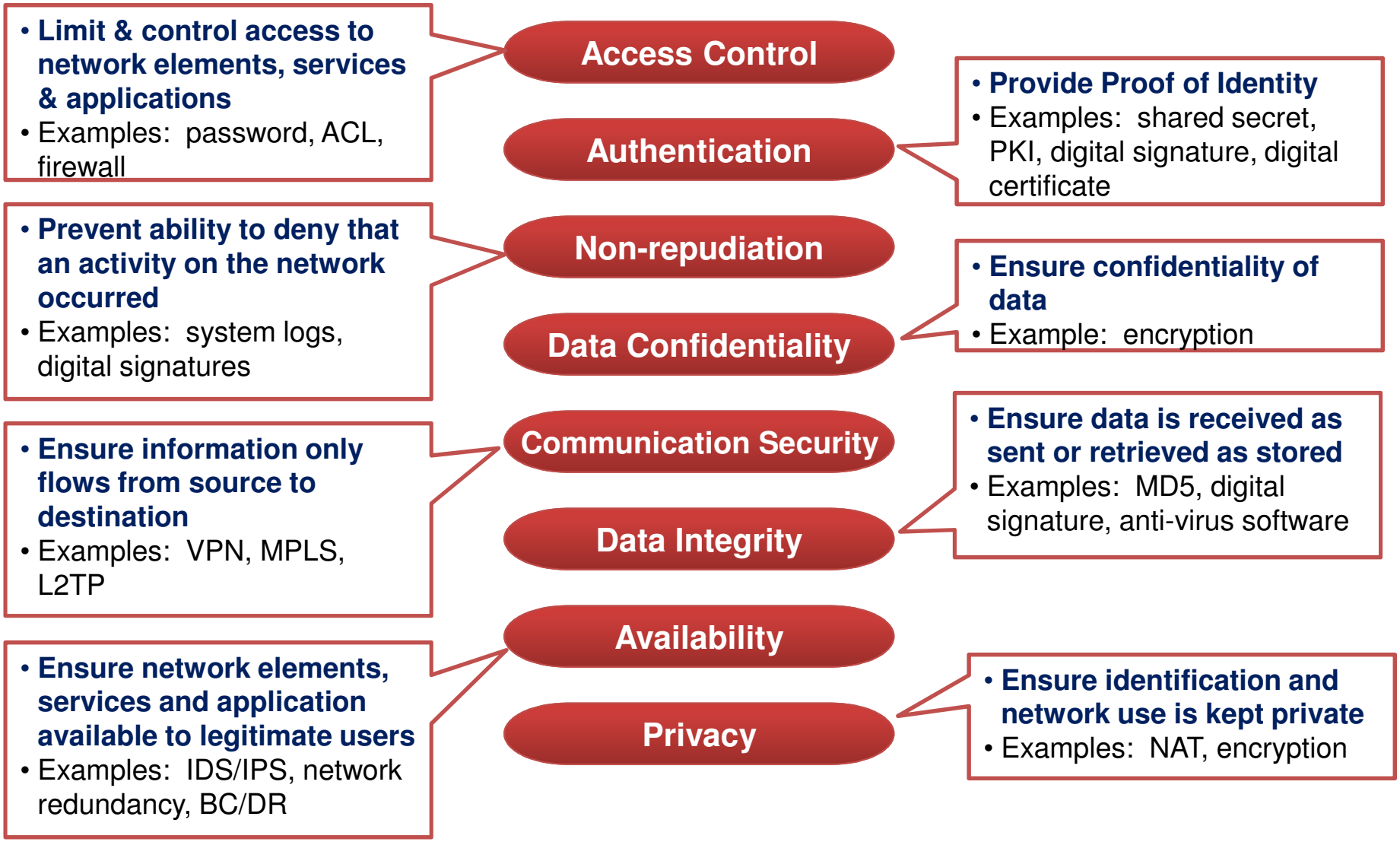
- **Some of other proposed measures include (besides many) policies and methodologies to:**
- Creation of National Structure for Cyber security
- Competency framework for Cyber Security Work force
- Maintain an Inventory of Critical information infrastructure
- Establish Centres of excellence for best practices in Cyber Security and Research
- Set up Labs for accreditation of IT and Telecom products
- Establish a Cyber command within Indian Defence
- Establish a National threat Intelligence Center
- Build capacity of the Law enforcement Agencies

Security Vision

Vision:

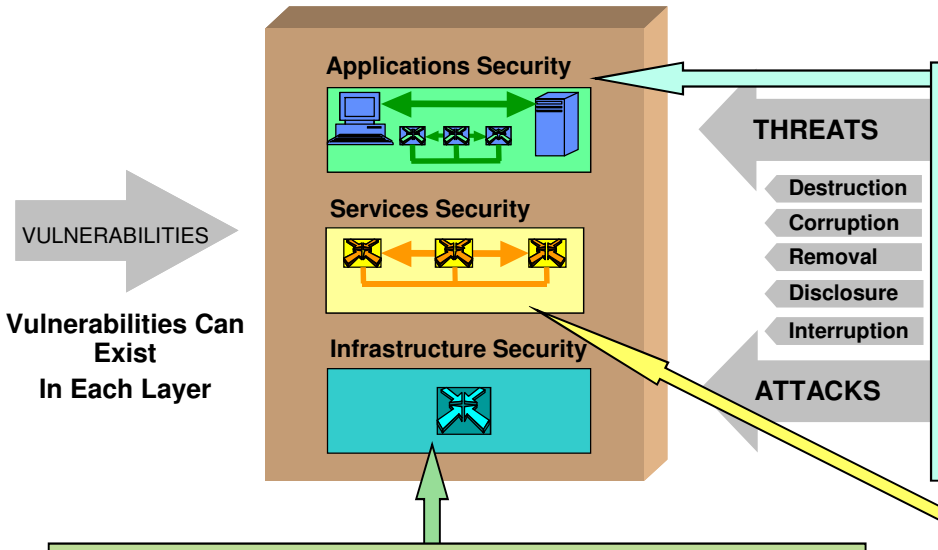
“To implement a Security Management System that protects the Confidentiality, Integrity, Availability and Privacy of the network, information of the company, customers, business partners and other stakeholders complying with all regulatory and legal requirements”.

Eight Security Dimensions Address the Breadth of Network Vulnerabilities



Eight Security Dimensions applied to each Security Perspective (layer and plane)

Three Security Layers



3 - Applications Security Layer:

- Network-based applications accessed by end-users
- Examples:
  - Web browsing
  - Directory assistance
  - Email
  - E-commerce

1 - Infrastructure Security Layer:

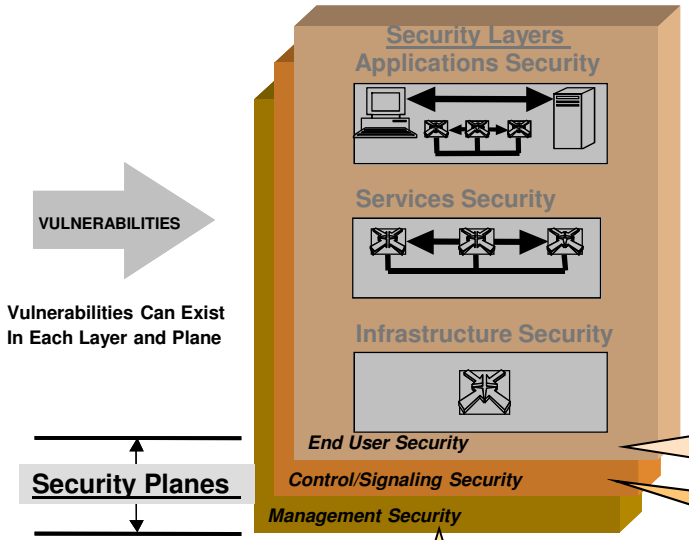
- Fundamental building blocks of networks services and applications
- Examples:
  - Individual routers, switches, servers
  - Point-to-point WAN links
  - Ethernet links

2 - Services Security Layer:

- Services Provided to End-Users
- Examples:
  - Frame Relay, ATM, IP
  - Cellular, Wi-Fi,
  - VoIP, QoS, IM, Location services
  - Toll free call services

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

Three Security Planes



1 - End-User Security Plane:

- Access and use of the network by the customers for various purposes:
  - Basic connectivity/transport
  - Value-added services (VPN, VoIP, etc.)
  - Access to network-based applications (e.g., email)

3 - Management Security Plane:

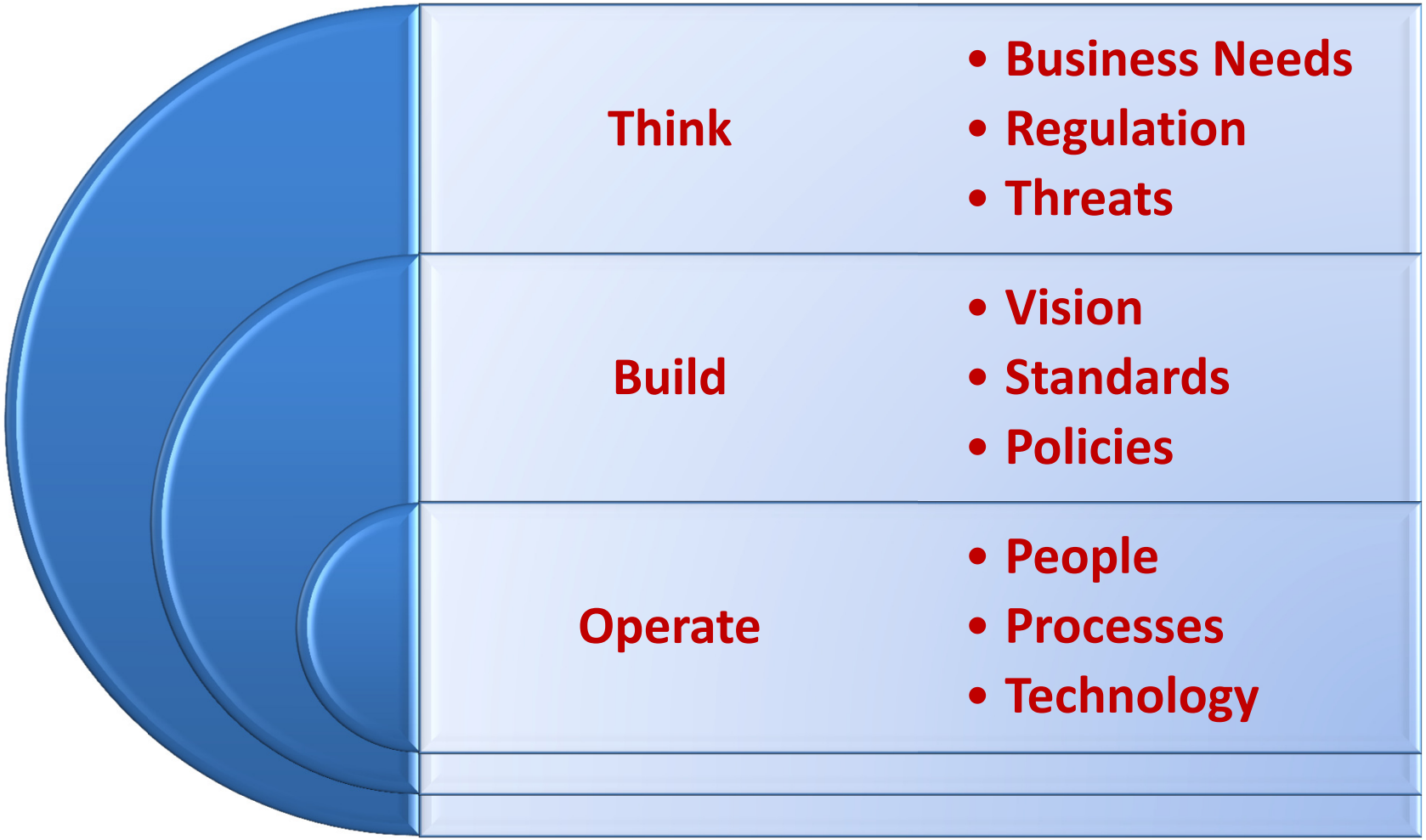
- The management and provisioning of network elements, services and applications
- Support of the FCAPS functions

2 - Control/Signaling Security Plane:

- Activities that enable efficient functioning of the network
- Machine-to-machine communications

- **Security Planes represent the types of activities that occur on a network.**
- **Each Security Plane is applied to every Security Layer to yield nine security Perspectives (3 x 3)**
- **Each security perspective has unique vulnerabilities and threats**

Security Framework



Key Security Concerns

Securing the Business

Are **regulatory** driven security requirements adequately addressed and effectively enforced?

Is **governance** through security policies and processes adequate and working as desired?

Is **the technical infrastructure** securely designed and configured. Does it have exploitable security weaknesses?

Are the **vendor operations** secure? Are they increasing security risk?

Risk Governance

Manage Risk | **Achieve Compliance** | **Protect**

Reputation

Security Governance Risk & Compliance

- **ISO Security /3GPP/ISO 15408/IETF/ ITU & Other Standards**

- **Information Security Policies, Procedures, Guidelines**

- **Known Risk Management Document**

- **Information Security Index**

Processes & Technology

Protect what matters!

IP, business data, privacy...

Operations Security

Enable Secured Setup

Network Security
(Firewall, VPN, Access Control, IPS/IDS, Websense, SOC, Watch Dog)

Applications Security
(Hardening Checklist, VA / PT, IDM)

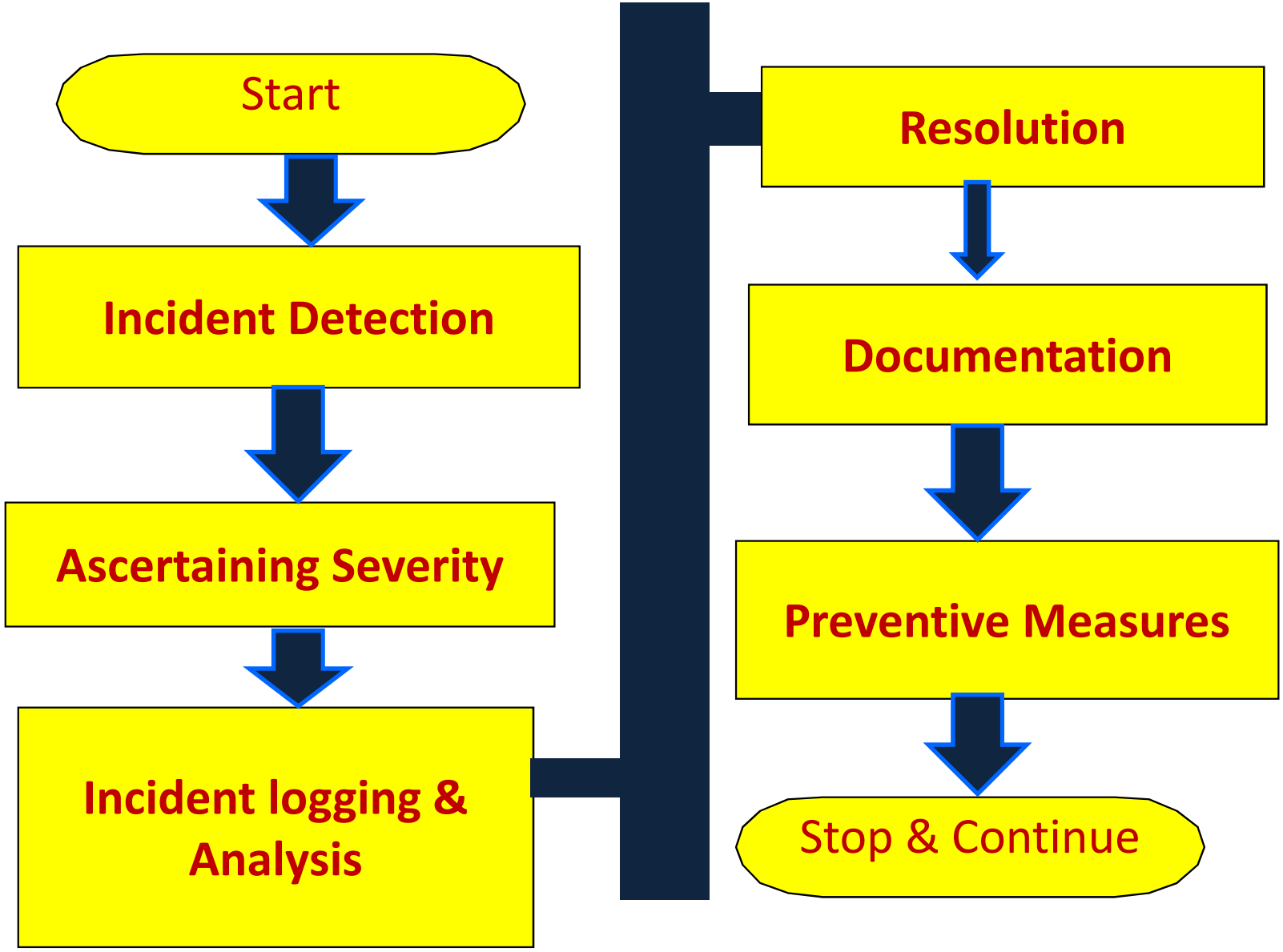
End Point Security
(Antivirus, Antimalware, Network Threat Protection, User authentications, subscriber management, SNAC)

Regulatory Compliance

Security Governance, Risk & Regulatory Compliance

16

Security Incident Management Process



Continual Improvement & Way Forward

- Compliance reporting to Senior Management
- Compliance to policies, processes , practices, procedures, guidelines & checklists
- Self compliance reporting & auto repository, efforts to integrate NW into IT SOC
- Security compliance audits
- Strengthening internal & Stakeholders awareness and placing Formal Security Organization Structure

Implementation Challenges

- Techno-economic feasibility
- Enhanced awareness amongst all stakeholders
- Structured information on applicable security standards
- Availability of tools, Testing facilities of Devices under test and Context aware Testing
- Multiple Government agencies issuing policies , Guidelines, Advisory bodies and related confusion and overlap at times
- Thin line between privacy, legal interception and related operating processes and procedures
- Huge funding requirements
- Local expertise on Cyber Security
- Indigenous research and develop programs on security
- Global Cooperation

Network Security Processes

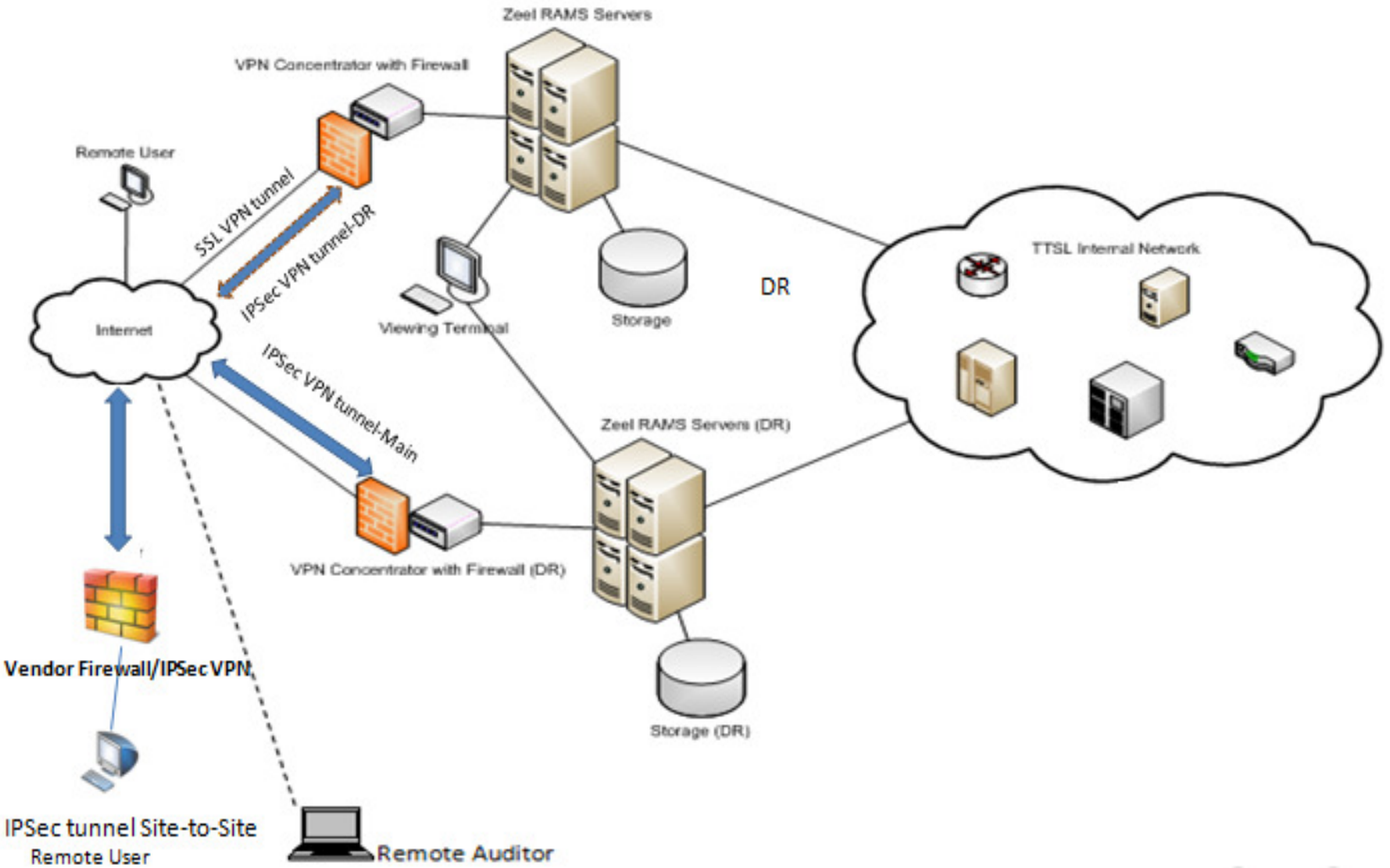
.

- **Network Access (Logical) Management Process**
  - Management of user and access control of network elements, access related logs.
  - Best Practices based Identity and Access management solution as a centralized security solution - CNOC and Network Security teams
- **Remote Access Management Process**
  - Management of remote access user using VPN Virtual Private Network, management of access logs.
- **Password Management Process**
  - Tool based management of passwords and privileges across the Nodes

Log Management

- Keeping records of Operation and Maintenance command Logs of Network Elements at Centralized Server for a period of 12 months.
- For next 24 months, Logs available in Archive mode in external Tape Drive.
- Regular backups taken

Remote Access Network Architecture



The Multi-Layered Approach
New technologies

- Getting the IP network design right
- Protecting the IP traffic in transit
- Enforcing controls in the Gateway
- Ensuring UE and HeNBs are secure
- Monitoring and Response
- Testing

Unified/Consolidated Gateway

- The “Gateway” enforcing some very important controls:
- Anti-spoofing
- Encapsulation protection
- Device to device Routing
- Billing and charging of users

IP Routing

- Architecture design and routing in the core is complex
- Getting it right is critical to security
- We see issues with this
- Needs extensive testing before production deployment

IPSec - the battle between Essential and Optional

- Difficult choice (encryptions / PKIs / DPIs) latency
- If correctly implemented will provide Confidentiality and Integrity protection
- Can also provide authentication between components
- Keeping the keys secure is not trivial and not tested
- Embedded, centralized & security servers, firewalls positioning, amongst e/h nodeBs, to / from MMEs and Gateways
- Issues of UEs, VoLTEs, Other Devices

Testing for Security

- Captive facilities
- Key protective controls for test within LTE and HetNets environment as also fail safe fallbacks
- Safe to connect and Safe to transact
- Policies and rules in the Unified/Consolidated Gateway , Protocol tests
- The implementation of IPSec or mixed others between all back-end components
- A back-end IP network as also non-IP , with well-designed routing and filtering

We sincerely believe

- Despite fears from the use of IP in 4G and beyond (security by design) , will improve security if implemented correctly
- Key controls must be correctly implemented
- Testing must be completed for validation
- Continued scrutiny is required
- Legacy systems may still be the weakest links

Looking ahead

- More air interface extensive testing is needed
- Will need co-operation from vendors/operators
- Global Cooperation. Cyber Issues.
- Private Sector the first line of defence. Enterprise and National Interests both
- Context Aware testing Vs Device testing
- “Open” testing tools will need further significant development effort
- Still lower hanging fruit, if support for legacy wireless standards remain

Some known Standards to us so far

3GPP Security Specifications 4G+ Security

- 33.401: System Architecture Evolution (SAE); Security architecture
- 33.402: System Architecture Evolution (SAE); Security aspects of non-3GPP ++

Lawful Interception

- 33.106: Lawful interception requirements
- 33.107: Lawful interception architecture and functions
- 33.108: Handover interface for Lawful Interception

Key Derivation Function

- 33.220: GAA: Generic Bootstrapping Architecture (GBA)

CONTD

Some known Standards to us so far

Backhaul Security

- 33.310: Network Domain Security (NDS); Authentication Framework (AF)

Relay Node Security

- 33.816: Feasibility study on LTE relay node security (also 33.401)

Home (e) Node B Security

- 33.320: Home (evolved) Node B Security

Areas of Submission to Regulator and Audit

Network & IT security policy implementation

Internal and external NW & IT audit reports

NW and IT hardening reports

Security authentication reports

VA & PT security tests, logs

Security Certificates reports vendors tests

Vendor agreement & Vendor Inspection

Data retention, O&M logs , software updates, change management

RAS, C-RAS – Status and compliance

LBS status

CDRs

Audit reports

Regulator may visit and inspect & for further engagement

Tools used, used, methodology, PoCs