



Importance of Network Security in Deregulated Environment

A presentation sketch (unofficial version)

Dr. Mohammed Yaseen
Member Technical, PTA

unofficial version



Importance of Network Security in Deregulated Environments

Suggested Topics

- Deregulation and rise of competition -- a global perspective
- Regionally specific regulatory concerns
- Network Security Policy Design
- Readily implementable methodologies to remedy network security threats
- Challenges for the operators
- Challenges for the regulators



Deregulation and the rise of competition – *a global perspective*

unofficial version

Introduction: Telecoms Environment

- Markets throughout the region have gradually moved toward market liberalization, noting the role that telecommunications can play in economic advancements.
- Telecom deregulation has been judged successful. Long-distance rates have declined and innovation has dramatically improved service.
- Deregulation in the telecom sector allows a whole new host of businesses to provide basic-to-advanced communications and entertainment services.
- Rights of way and the wires that connect long-distance carriers to homes and businesses have emerged as expensive real estate.
- As long-distance telephone services face increasing competition, access to consumers through these rights of way has become new profit centers.
- This threatens community control over local resources and demonstrates the unexpected risks that may be inherent in the tide towards deregulation.



Introduction: A Regulator's Role

- **Key Factor for a Regulator's Success**
 - The extent to which the regulator is perceived to be independent of political control – and separate from other telecommunication bodies – is a key factor in the confidence that industry and the public have in its decision making and its capacity to attract foreign investment.
 - As introduction of privatization, without at the same time establishing regulation and opening markets to competition, may not be productive toward telecoms expansion, a regulator's role is critical in ensuring that coherent and manageable policy design is put in place.

Introduction: A Regulator's Role (contd.)

- **Key Factor for a Regulator's Success**
 - Regulator's role inducing early establishment of independent regulation increases investor confidence, as has been witnessed in Pakistan.



Deregulation in Asian Countries

- Many Asian governments deregulated their telecommunications sectors in the 1990s, which led to the sectors' rapid growth and development, allowing some countries to catch up with the west in the most advanced telecommunications technology within a short period of time.
- With more competition in the market after deregulation and the poor performance of the global telecommunications sector in recent years, the Asian telecom companies had to reassess their strategies and adopt different business models.
- The market potential of wireless technology and broadband as well as e-business is still favorable both in the developing and mature markets of Asia, although telecom operators are cautious about the implementation of the 3G spectrum.

Implications of Deregulations and Competition

- Deregulation has resulted in enhanced connectivity
- Subsequent rise in competition has resulted in the creation of advanced services and technologies to meeting growing user demands
- Operators have been forced to develop new business models to assure revenue-generation
- Investments in telecom network expansion have been deemed by some operators as a necessity
- Some operators believe employing new “disruptive” technologies to enhanced their network capabilities
- **Security threats** have arisen
- **Fraudulent activities** and network manipulations have materialized



Regional Telecom Concerns

unofficial version



Regional Telecom Concerns

- **Threats to Reliable Service**
- **Industry Standards**
- **Reliability of Service**
- **Service Provider / Operators Liabilities**
- **Customer's/Subscriber's Expectations**
- **Industry Protection Measures**



Threats to Reliable Service

- **Physical disturbance resulting from human error are the most common cause of service interruptions.**
- **Cyber attacks are the greatest threat to service reliability within the telecommunication sector.**



Industry Standards

- Numerous Industry standards exist within Industry for maintaining reliable service.
- However, some standards that exist through legislation and through various trade associations may not be at acceptable levels to dictate their operations.



Reliability of Service

- **There are currently many service providers that can provide their customers with higher levels of reliability but with additional cost**
- **The acceptable cost is dependent on the level of service required to meet customer demands.**
- **This high cost high quality is a trend which is expected to continue.**
- **The burden for reliable service falls on the customer**



Service Provider Liabilities

- Liabilities associated with service interruptions are not generally perceived to be an issue of concern within the industry unless there were a case of gross negligence
- Most service providers and operators have negotiated contracts with major customers that specifically address the liabilities associated with service interruptions
- Liabilities are not as large a concern as the severe damage that unreliable service can do to a company's brand.



Customer's/Subscriber's Expectations

- Customer's/Subscriber's expectations and needs for reliable service vary widely
- Subscribers demand that some minimum level of service be offered to everyone and that "seamless" service be available.
- This is an issue of greater concern in the deregulated environment given that certain rural residential customers are already experiencing service problems.
- A fear exists that companies will focus on the areas where higher premiums are generated.



Industry Protection Measures

- **General consensus within the industry is that “uninterruptible service,” taken literally, is not possible.**
- **The service with uninterruptibility involves high costs.**
- **Service providers/Operators offer network redundancies and anti-hacking firewalls to protect themselves and minimize service interruptions.**
- **Major customers subscribe to multiple services as a backup plan.**
- **Illegal manipulation of networks is on the rise, with each year bringing in more revenue loss**



Network Security Policy Design

unofficial version

Introduction: The Industry's Security Needs

- Better awareness of security threats and impact
- Telecom industry is the main body of national information industry.
- Its network and information security concerns national infrastructure security, therefore, telecom industry's awareness to information system security is comparatively early and mature.
- Along with its stricter requirement to network management, telecom industry also requires:
 - A higher standard of the solution provider's professional security services
 - There has been a drastic need for professional network security service and solution providers.



Risks in Telecom Networks

- At present telecom industry's network is a super large-scale network that includes interconnections of various equipments and systems.
- Professionally it can be subdivided into
 - Basic network,
 - Fixed telephone switch network,
 - Digital data network,
 - Public computer interconnection network,
 - Telecom management network,
 - Information token network etc.
- It also includes many value-added business networks, providing various business.
- The telecom network faces all kinds of risks including
 - Bound risks,
 - DoS risks, system risks,
 - Applied system risks, etc.

Telecom Industry's Main Security Demands

- The necessity of integral security management.
- For telecom enterprises, network and data's security and reliability are the foundations of procedure optimization and management improvement.
- Network applicability or data reliability also requires to be ensured through the implementation of professional network security services and security solutions.
- Policies (and products) that aid network security mechanisms
- For telecom network administrators, the task of providing superior telecom network security is very tough.
- As telecom networks begin to move from TDM systems to a hybrid of legacy systems and VoIP technology, telecom network security can be compromised by a multitude of new telephony-related
- Security is further complicated by the difficult nature of managing a hybrid voice network. For the tools to efficiently and effectively ensure greater telecom network security.



Readily Implementable Methodologies to remedy Network Security Threats

unofficial version



Steps to Reduce Security Threat Levels

- Hacking, cracking, and cyber crimes are hot topics these days and will continue to be for the foreseeable future.
- However, there are steps that can be taken to reduce an organization's threat level.
 - The first step is to understand — *through active industry dialogue and regulatory participation* — what risks, threats, and vulnerabilities currently exist in your environment.
 - The second step is to formulate a solid response system.
 - The third step is to intelligently deploy selected countermeasures (including security audit solutions and fraud-detection solutions) and safeguards to erect protections around your most mission-critical assets.

Risks Associated with New Telephony Technology

- While Voice over Internet Protocol (VoIP) is gaining popularity due to its impressive cost savings, there are certain risks associated with this new telephone technology.
- Businesses that are considering switching to VoIP services, or already using VoIP, should be aware of these risks and prepare to deal with them through the use of call accounting software.
- Because VoIP uses packet switching, the same technology that drives the Internet, it faces the same threats, such as denial of service (DoS), hackers and spam.

Risks Associated with New Telephony Technology

- Fraud is another problem, with hackers patching into a telephone system and using the company's telecom resources to make long distance calls, which may end up costing the enterprise thousands of dollars a month.
- While this possibility also exists with more traditional PBX systems, VoIP systems are more prone to this type of crime, because the techniques of Internet hacking are much more widely known.
- Even so, with proper precautions, VoIP systems can work well and provide an excellent return on investment.



Challenges for the Regulators

unofficial version



Challenges for the Regulators

- **Networks have become the "backbone" of the economy, thus security stakes have been raised**
- **The telecom industry realizes the need to implement strong security measures, but general awareness level is comparatively low**
- **Some private companies/groups were granted licenses to provide telecom services**
- **Where market is growing, operators also started offering different services**
- **The rise in tele-density is a good thing, but challenges for the regulator have dramatically heightened**
- **There are not enough arrangements to keep a network secure**
- **National security concerns arising from enhanced connectivity**