SAUDI LAW CONFERENCE
المؤتمر السعودي للقانون

UNDER THE THEME OF: **REINFORCING A SUSTAINABLE AND INCLUSIVE BUSINESS ENVIRONMENT**

LEGAL FRAMEWORK FOR CYBER SPACE & CLOUD SECURITY IN SAUDI ARABIA
POLICY AND ITS CHALLENGES

By
Misbah Saboohi
Law college; Prince sultan university

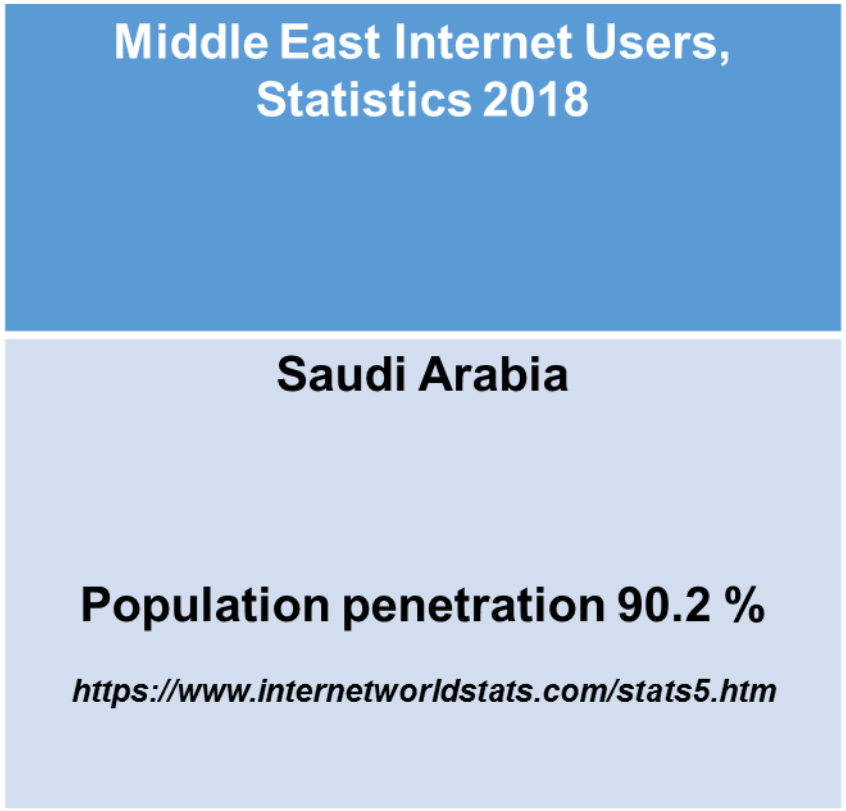
Some data

Year	Internet Penetration In Business Sector
2007	52%
2009	65%

Year	Percentage
2009 (individuals)	Laptops: 76%. Desktop Computers 66%
2009 (business establishments)	Total : 82% Medium enterprise :91% large establishments : 93%

Internet growth in KSA

Year	Percentage
2007	19.5
2009	27
2010	38.1
2012	49.0%



- **The trend shows the adoption of machines and gadgets now which have mobility advantage i.e. “on-the move connectivity”. Hence cyber space connectivity and internet services are of importance as lifestyle for Saudi Arabia now**

Cloud opportunity in KSA

Year	Total Saudi market capacity	Budget allocation for cloud computing	Current Saudi usage of 'hybrid' cloud computing	Saudi cloud market	Outsourcing services expansion	Application management services market
2015	$570.6 million	35% (equal $ 29 billion)	32% of companies	Approx. $77.5 million (53.8 % up from 2014)	Network 22.1% Desktop 18.5 %	Current growth rate: 16.2% (Expected to rise 16.5 %)

Saudi efforts to regulate cyber space

1. The CIT Committee of the Majlis E Shura Council (Parliament) stressed the need of ‘orientation’ of Saudi individuals, government agencies and companies to deal with foreign companies with access to cloud computing services

Challenges To cyber security

1. Absence of centralized information security policies and standards .
2. Little or no consistency in policy or communication across organizations. Each organization has implemented ICT security in their own manner.
3. The national standards and requirements only extend to the organization's connection point and not inside the enterprise ICT infrastructure.
4. Lack of common national framework for Internet Security Risk Assessment and Management (ISRAM), so results from various ministries and organizations cannot be compared on the same scale for senior management decisions

Challenges To cyber security

5.A large need exists for qualified IT, ICT, ICT security and cyber-security practitioners.

6.Absence of centralized control center.

7. the Kingdom's infrastructure elements highly vulnerable and represent a major risk to the Kingdom’s critical ICT infrastructure.

8.Limited emphasis on the importance of business/mission requirements to an ICT architecture, or the implementation of specified **resilience** requirements.

9.No guidelines for disaster recovery planning for Ministry ICT and information systems

Saudi strategy for cyber security

- **Step 1**: Saudi Ministry of Communication and Information Technology (MCIT) adopted the Saudi Cabinet Resolution No 82 for formulating a strategy for the kingdom.
- **step 2:**The Ministry formed a commission called Communications and Information Technology Commission (CITC) to regulate technology and communications services in the Kingdom of Saudi Arabia with the goal of ensuring that these services are ***"universally available, high quality and affordable***
- **Step 3:** The commission adopted 'National Information Security Strategy' (NISS) for the Kingdom in response to a Request for Proposal issued by the Ministry, January 2011

Saudi NISS elements include:

1. Information Security Environment
2. Policy and Regulation
3. Risk Management and Assessment
4. National ICT Infrastructure
5. Human Resource
6. Re-assessment and Audit
7. **National** Cooperation and Sharing for Information Security
8. **International** Cooperation and Sharing for Information Security(Saudi NISS recommended to seek guidance from European or USA policies for securing cyber space)
9. Research and Innovation

Important legislation for cyber security in KSA

- National Information Security Strategy (NISS) of the kingdom of Saudi Arabia intends that all the Laws/acts, policies, regulations and directives related to information and Data security should establish the key direction…**TRUST & PRIVACY**
- **Telecom Act** Issued under the Council of Ministers resolution No. (74) dated 05/03/1422H (corresponding to 27/05/2001) Approved pursuant to the Royal Decree No. (M/12) dated 12/03/1422H (corresponding to 03/06/2001).The **Anti-Cyber Crime Law** of Saudi Arabia (Anti-Cyber Crime Law Royal Decree No. M/17 8 Rabi 1 1428 / 26 March 2007, First Edition 2009) provides a good base for prosecuting those that attack, steal or damage a network or computer. However, this law does not cover prevention, education and collaboration. The **Electronic Transactions Law (ETA)** (Electronic Transactions Law Royal Decree No.)M/8(8 Rabi' I- 1428H – 26 March 2007) provides a good basis for controlling, regulating and providing a legal framework for electronic transactions and signatures

Issues in cloud computing

- No borders,GLOBAL communes
- computers can communicate with one another across a seamless landscape of global networks
- Public sector services like hospitals and hotels,universities etc have only one server provider from any country .

Basic Legal hurdles in cloud protection

- **STATE JURISDICTION**. Server is in one state but cyber activities taking place in multiple states. If a user sends an email from Riyadh to Singapore using a cloud service based in New York, “the question of the email's jurisdiction is better answered by a philosopher than a judge.” (‘*Legislating the Cloud. Information Today ‘ By SCHILLER K.Oct 2011;28(9):1-36*)
- **PRIVACY** .cloud data has multiple users all over the world.
- Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to store and process data in specific jurisdictions only

SAUDI APPROACH

- Saudi Arabia is party to The Arab League Convention to Combat Cyber Crimes. Plus the NISS commission has approved the cyber security legal frameworks of:

1. UK
2. Tunisia
3. GCC States
4. Japan
5. USA
6. Malaysia
7. France

- To overcome jurisdiction issues in legal cases, the first line of action for Saudi Arabia is how the Saudi companies sign the appropriate contracts with the service providers. International treaties are needed for this solution to work
- careful drafting of agreements with cloud service providers to ensure information security and privacy rights

Which company is a good cloud provider

- Compliance level of the service provider for various cyber laws is strong.
- electronic discovery capabilities of the provider
- Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls
- Company ready to Establish clear, exclusive ownership rights over data to the user company
- on-going risk management decisions.

Saudi policy

- Article 3 of the CITC has clear duty to monitor and advise on legislation for information security in cyber space.
- Article 3 of the commission's role as regulator mentions that the licensing for the telecom companies shall be the domain of the Telecom Commission only.
- The information security policies and procedures development is initiated by Government Mandate number (81) – 191430/3/H and all Government Agencies are required to fulfill the minimum security requirements, in line with the relevant information security risk to taht organization's information assets This development framework has been provided to the Government Agencies as a comprehensive set of guidance and tools that can be used by the management in their efforts to comply with the Government Mandate.

- United states’ National Institute of Standards and Technology (NIST) developed a document under the Federal Information Security Management Act (FISMA) in 2002. This is a very important document that Saudi Arabia has kept as one guideline to make its National Policy for Internet security. USA National Security Strategy 2015 has recognized that the cloud computing should be :
- Safe
- Private
- Enabling
- Enduring .

- American policy considers that ‘National Critical Security And Defense Infrastructures And Communications’ need to have effective control over the open computers involved in cloud computing

Recommended contract features for cloud safety

a. Establish Contractual Obligations.	**all contractual requirements are clearly stated in the service agreement, including privacy and security provisions. The cloud user company can save a lot of legal problems if it has a good negotiated agreement with the service provider.**
b. Clear definitions	Privacy regulations should have clear 'definitions' because they may be interpreted differently by an organization's legal and privacy officers than by a cloud provider.
c. A detailed description	description should be present of the service environment, including facility locations and applicable security requirements
d. Specific remedies	remedies to be provided for harm caused or noncompliance by the cloud provider.
e. Data Ownership.	Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; and the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security .
f. Service availability	Contingency Plan in emergency
g. Data backup and recovery	Recovery system

- One solution being discussed is “common repositories by security experts”. It is meant to safeguard privacy through creating and maintaining a trusted system of online identity (like personal emails) that could be used only by cloud users
- “group approach solution”. May be the best solution is to have an international treaty on the pattern of the World Intellectual Property Organization (WIPO) Copyright Treaty.(if a person wants to challenge a URL used by somebody else, WIPO provides a definite, uniform process that whether you're in Germany, the United Kingdom, or the United States) so USA , UK have to be part of these cloud computing international security pacts for their effectiveness because major cloud services are being run from these countries.

Immediate action

- Strict adherence to all current cyber security laws in the kingdom
- Trainings to be conducted for IT officers in all organizations before going into cloud data.

Future action

- cloud security coordination center in the Kingdom. It needs equipping with experts in cyber security and Telecom law experts
- Entering into bilateral treaties for solving legal remedy and jurisdictional issues in case of breaches

THANK YOU