Role of Corporate in National Cyber Security

By
Naavi
July 14, 2009
@ CISS 2009,
Trident Hotel, Mumbai

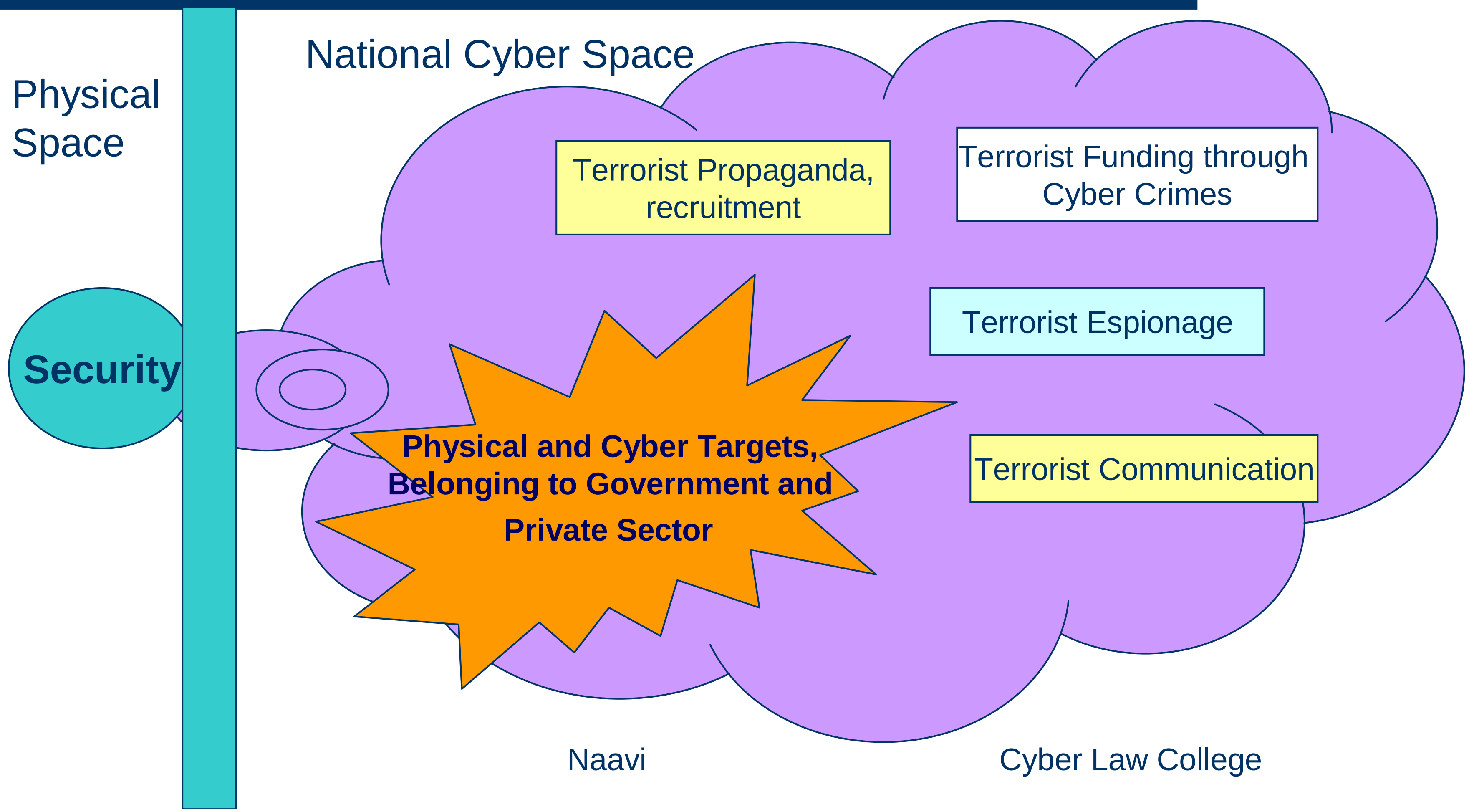
We are talking of National Cyber Space..

Most of us are non Cyber Space security professionals…

How Is Physical Space Security related to ..

….National Cyber Space.. Is our first question..

Security in Physical Space is dependent on Cyber Space security



National Cyber Space
Physical Space
Security
Terrorist Propaganda, recruitment
Terrorist Funding through Cyber Crimes
Terrorist Espionage
Physical and Cyber Targets, Belonging to Government and Private Sector
Terrorist Communication

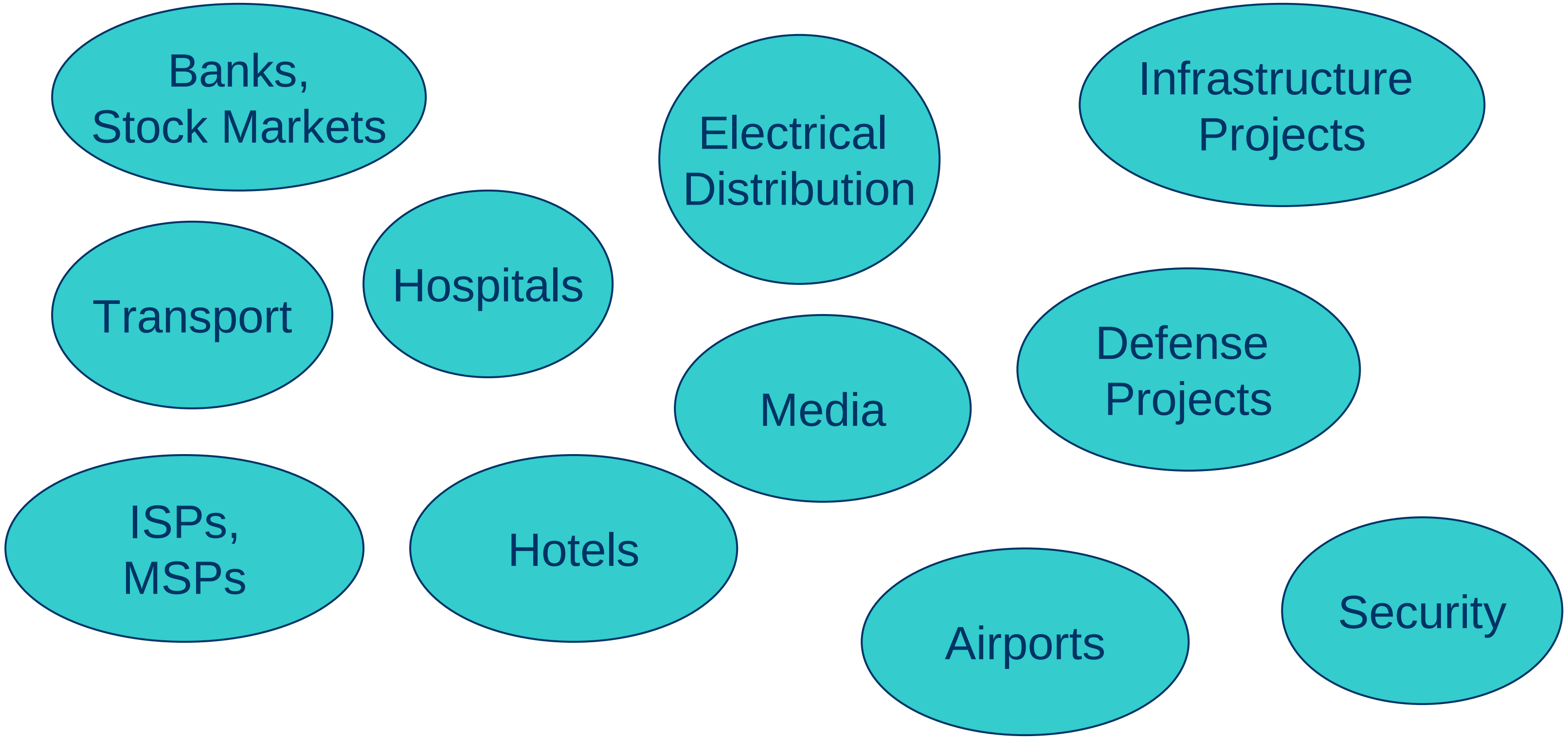
Naavi

Cyber Law College

What is the role of Private Sector..

In National Cyber Security?..is our next question..

Private Companies control critical national activities



Banks, Stock Markets

Electrical Distribution

Infrastructure Projects

Transport

Hospitals

Media

Defense Projects

ISPs, MSPs

Hotels

Airports

Security

Peaceful running of our country..

..is substantially in private sector’s hands..

What Companies need to do?

.. To contribute to National Cyber Security

Four Dimensions to Corporate Role

Ensuring Self Security

Developing Security Culture within

Collaborating with Government in security functions

Contributing to the development Security Culture Development in the society

The Golden Rules for Corporates

- If each one of us is secure, the nation is secure
- Security is not effective when it is imposed. Developing a voluntary adoption of security culture within each one of our organization is required
- Private-Public collaboration holds the key for national security even in cyber space. Let’s do our bit
- We owe it to the society to put resources for developing the cyber security culture in the society

The First Step

Let's ask some questions to ourselves..

Have we recognized the value of Information assets in our hands?

- Today our corporate assets are as much in the form of "Information Wealth" as in the form of "Physical Assets".
- We know what is the value of our land, building, machinery
  - Do we know how much is our information worth?
    - The Tractor Manufacturer's experience

Value of our Information Asset

- If we don't know its value
  - How can we decide how much to invest on information security?
  - How can we insure our assets?
- Let’s first put a value to our information asset
  - Let us bring it to the balance sheet
    - As a contra entry?
    - At a notional value?
    - At a risk assessment value?
      - Cost of creation? Replacement Value? Contingent liability value?
        - E.g.: Satyam Unpaid incident?

The Second Step

Define an appropriate security objective

What are we securing?

- Our assets?
  - Building or Machinery?
  - People?
    - Business ?
- Should our security goal be the asset? or
  - the asset owner?
    - In the Information Security scenario, is it enough if we have a Disaster Recovery Plan (DRP) and the Business Continuity Plan (BCP)?
    - Should we try to upgrade it to Defensive Legal Protection (DLP) and Offensive Legal Remedy?
      - Concept of Techno legal information security

The Third Step

Implementation

Have we made a Risk Assessment?

- Can an external person intrude into our systems?
  - If so where and how?
  - Do we have a good Firewall? Intrusion Detection System?
- Can any of our employees send out sensitive information in the form of an e-mail from within the organization?
  - If so, how to prevent this internal threat?
    - As much relevant in a textile company as a software company
- Does our hardware and software contain any malicious agents which is stealing our data or taking control of our systems?

Have we conducted an Information Security Audit?

- ISO 27001 (in addition to quality audits)
  - As much relevant to textile or steel companies as much to software development or BPOs

Have we conducted an ITA 2008 Risk Audit?

- May be we have not even recognized the need !!
- Have we recognized that ITA 2008 has mandated?
  - Due Diligence
    - Data Retention norms
    - Traffic data archival
    - Security Incident breach reporting norms
      - Failure of which can put our CEO (and the security chief) in jail?

Security audits will tell you what are the gaps

We need to seek solutions and implement them

Implementation Examples

- If we maintain electronic documents year on year and consider them as our assets
    - We need to audit them from time to time and ensure that the documents have not been unauthorized changed.
        - Have we thought about any means of checking millions of documents which we keep in our e-document store for data integrity year after year?
            - Look out for e-audit specialists using “Ujvala-Bellur e-audit tool”
- If we use electronic communication, we need to use Digital Signatures for authentication
    - P.S: You can download a free e book on Digital Signatures from www.naavi.org
- If law requires archiving of data, we need to put required systems in place to archive required data, get it properly certified when required..etc
    - Look at the Indian Information Security Framework developed by Cyber Law College
        - IISF 309.. Refer for details at www.naavi.org

Once we secure our information space..

We can think of other things that are required for securing the national cyber space

Why My Security is relevant for National Security

- Unlike a physical space, there is no defined border for Indian Cyber Space which can be guarded by a National Army or a Border Security Force.
- The enemy can enter the Indian Cyber Space through any Computer connected to Cyber Space.
  - Every Internet ready device (Computer or Mobile) is a potential gateway for our enemies to enter.

Cyber Patrolling is an intelligence necessity.

- Cyber space is the tool of communication for conventional attackers also
  - E.g.: Parliament attack case
- Patrolling Cyber Space is an absolute necessity for security
  - At the ISP level
  - At the Cyber Café level
  - At the individual desktop level
  - At the corporate level
- Cyber patrolling cannot be undertaken without the total cooperation of the private sector

Corporate Role in Cyber Patrolling

- Collaborate with the relevant agencies engaged in Cyber Patrolling
  - Avoid Criminals taking shelter under excuses such as “Privacy” or “Freedom of Speech”
    - These are rights to protect the law abiding community and not the law breaking community
      - E.g.: Google/Yahoo proxies
      - Blocking of an objectionable site
- Invest in Cyber Patrolling Projects
  - Developing a network of Cyber Law Compliant Cyber Cafes
- Support and Promote Cyber Patrolling Projects of the Government

Developing a security culture within our organization

- Make “Due Diligence” a voluntary compliance Programme for every employee
- Before you hire an employee, ask him
    - “I know you are a Cyber Professional. Are you a Certified Ethical Cyber Professional?”
        - Ensure that every employee of your organization is Cyber Law Aware
        - Engage in Cyber Ethics training and certification across the enterprise
- When your IS Manager asks for top management support, accord it the right priority
    - Remember
        - IS is as important as Marketing or Finance or HR.
        - IS is not a burden to be tolerated but an essential ingredient of management policy

Assisting the Government in its security functions

- Private-Public collaboration holds the key for national security even in cyber space
  - Encourage the State Government to set up a State level Cyber Security Advisory Committee
    - And participate in its activities wholeheartedly
    - Lend your brains and resources to help Government agencies and Voluntary Organizations to work for Cyber Security in the interest of the nation.

Contributing to the development of Cyber Security culture in the Country

- For the Government,
  - it is a duty to protect the Country and therefore the Cyber Space
- For certain voluntary organizations
  - It is a passion
- Corporates owe it to the society
  - Help establish
    - “Cyber Security Research”
    - “Cyber Forensic Centers” of International excellence
    - Academic institutions which focus on “Techno Legal Information Security education”
    - “Cyber Crime Insurance” in India
    - “National Cyber Security Guard”
      - ..and

Contributing to the development of Cyber Security culture in the Country

- Remember that
  - **"Cyber Security" is a great investment opportunity for Companies who have a vision of leadership for the future.**
    - **It is the infrastructure for the Digital World.**
    - **If it is good for Entrepreneurs to invest in Steel, Cement, Construction, it is also good to invest in a Cyber Security Company**

Thank You

naavi@vsnl.com

www.naavi.org

www.cyberlawcollege.com

+9343554943