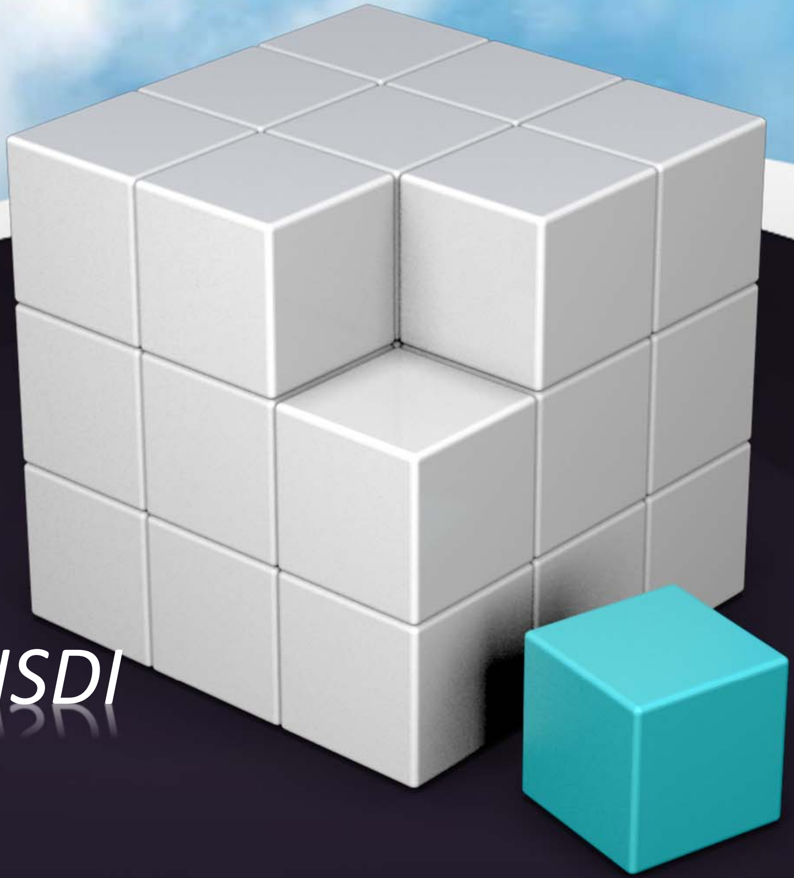
Managing Security in Spatial Data Infrastructure



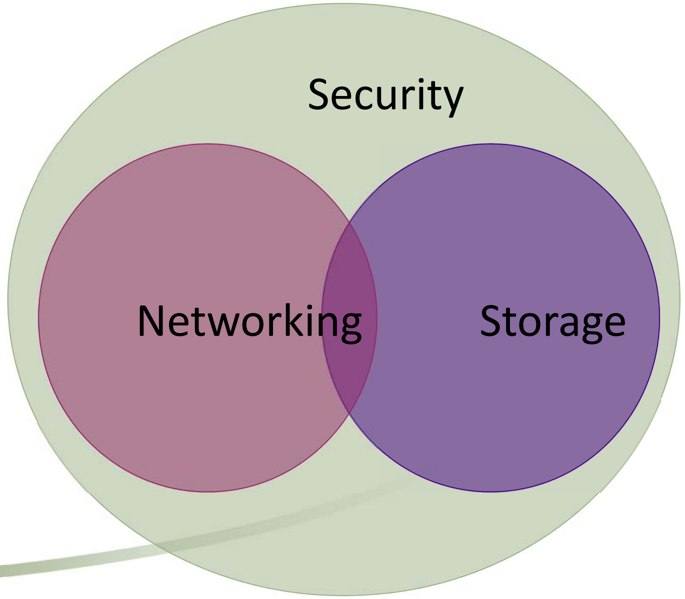
Presented by

R. N. Nanda, SS,NSDI

Dharmendra Singh,SA,NSDI

Information Storage Security

- Application of security principles and practices to storage networking (data storage + networking) technologies
- Focus of storage security: secured access to information
- Storage security begins with building a framework



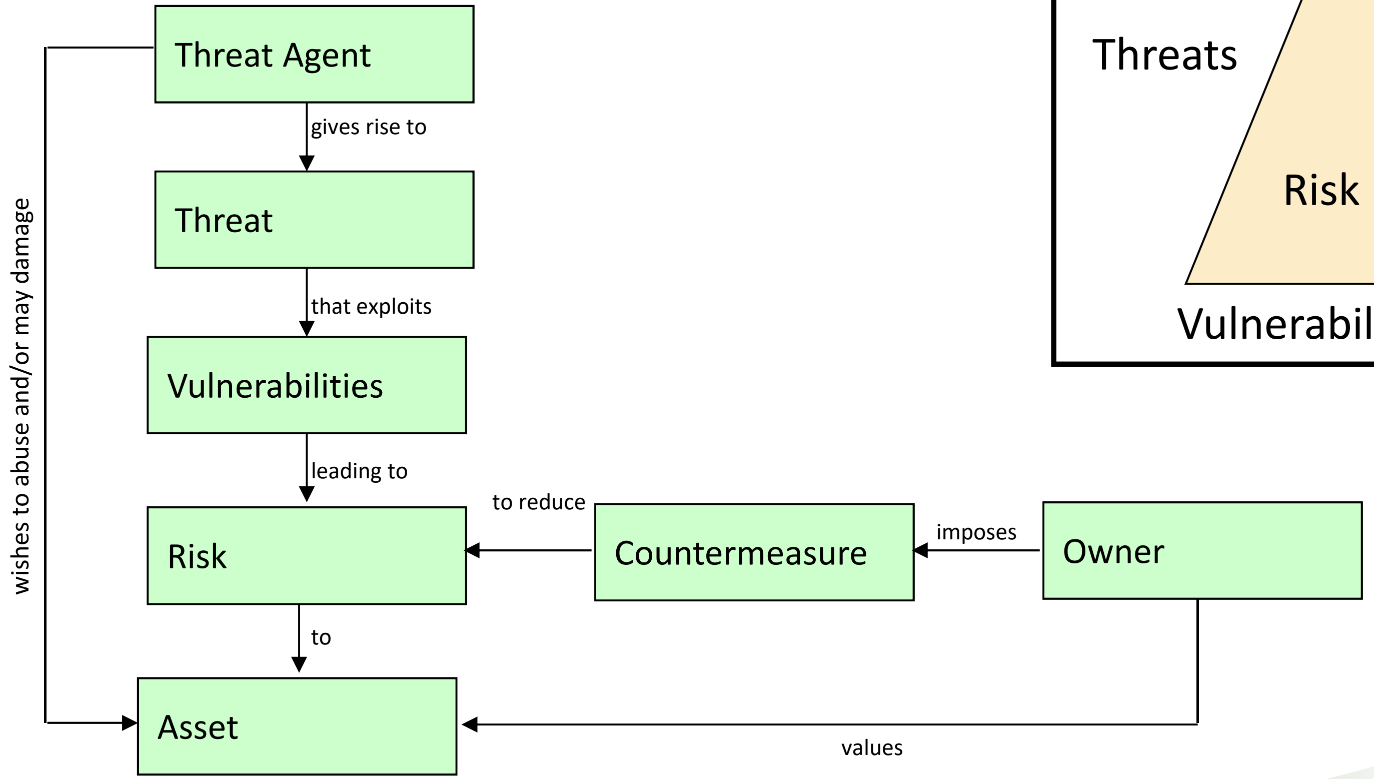
Storage Security Framework

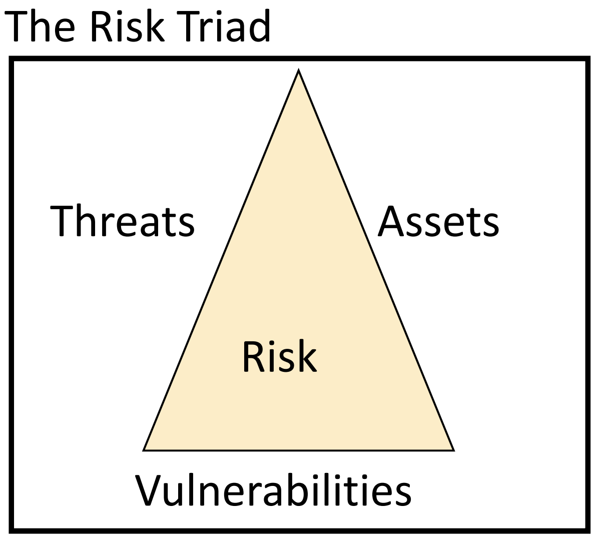
- A systematic way of defining security requirements
- Framework should incorporate:
  - Anticipated security attacks
    - Actions that compromise the security of information
  - Security measures
    - Control designed to protect from these security attacks
- Security framework must ensure:
  - Confidentiality
  - Integrity
  - Availability
  - Accountability

Storage Security Framework: Attribute

- Confidentiality
  - Provides the required secrecy of information
  - Ensures only authorized users have access to data
- Integrity
  - Ensures that the information is unaltered
- Availability
  - Ensures that authorized users have reliable and timely access to data
- Accountability
  - Accounting for all events and operations that takes place in data center infrastructure that can be audited or traced later
  - Helps to uniquely identify the actor that performed an action

Understanding Security Elements





Security Elements: Assets

- "Information" – The most important asset
- Other assets
  - Hardware, software, and network infrastructure
- Protecting assets is the primary concern
- Security mechanism considerations:
  - Must provide easy access to information assets for authorized users
  - Make it very difficult for potential attackers to access and compromise the system
  - Should only cost a small fraction of the value of protected asset
  - Should cost a potential attacker more, in terms of money and time, to compromise the system than the protected data is worth

Security Elements: Threats

- Potential attacks that can be carried out on an IT infrastructure
  - *Passive* attacks
    - Attempts to gain unauthorized access into the system
    - Threats to confidentiality of information
  - *Active* attacks
    - Data modification, Denial of Service (DoS), and repudiation attacks
    - Threats to data integrity and availability

Attack	Confidentiality	Integrity	Availability	Accountability
Access	√			√
Modification	√	√		√
Denial of Service			√	
Repudiation		√		√

Security Elements: Vulnerabilities

- Vulnerabilities can occur anywhere in the system
  - An attacker can bypass controls implemented at a single point in the system
  - Requires “defense in depth” – implementing security controls at each access point of every access path
- Failure anywhere in the system can jeopardize the security of information assets
  - Loss of authentication may jeopardize confidentiality
  - Loss of a device jeopardizes availability

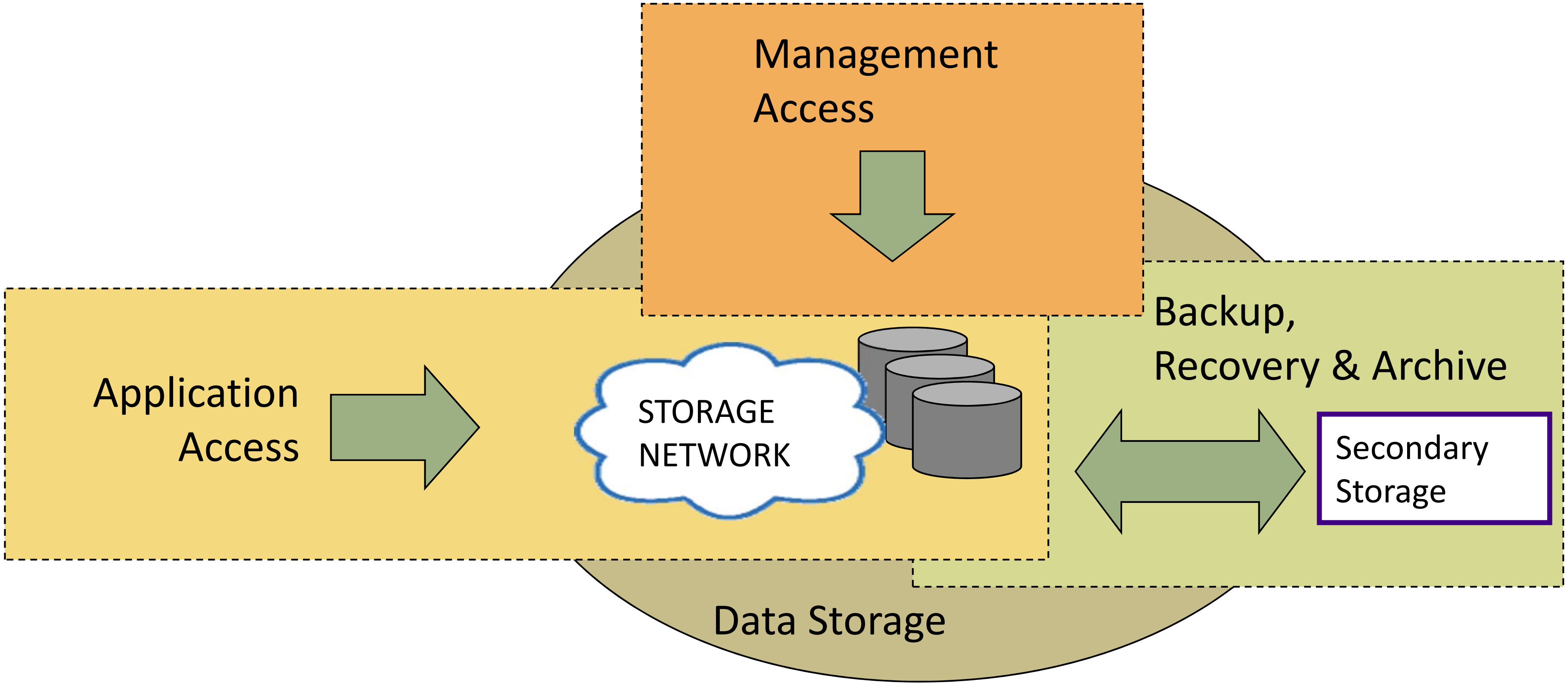
Security Elements: Vulnerabilities (cont.)

- Understanding Vulnerabilities
  - Attack surface
    - Refers to various access points/interfaces that an attacker can use to launch an attack
  - Attack vector
    - A path or means by which an attacker can gain access to a system
  - Work factor
    - Amount of time and effort required to exploit an attack vector
- Solution to protect critical assets:
  - Minimize the attack surface
  - Maximize the work factor
  - Manage vulnerabilities
    - Detect and remove the vulnerabilities, or
    - Install countermeasures to lessen the impact

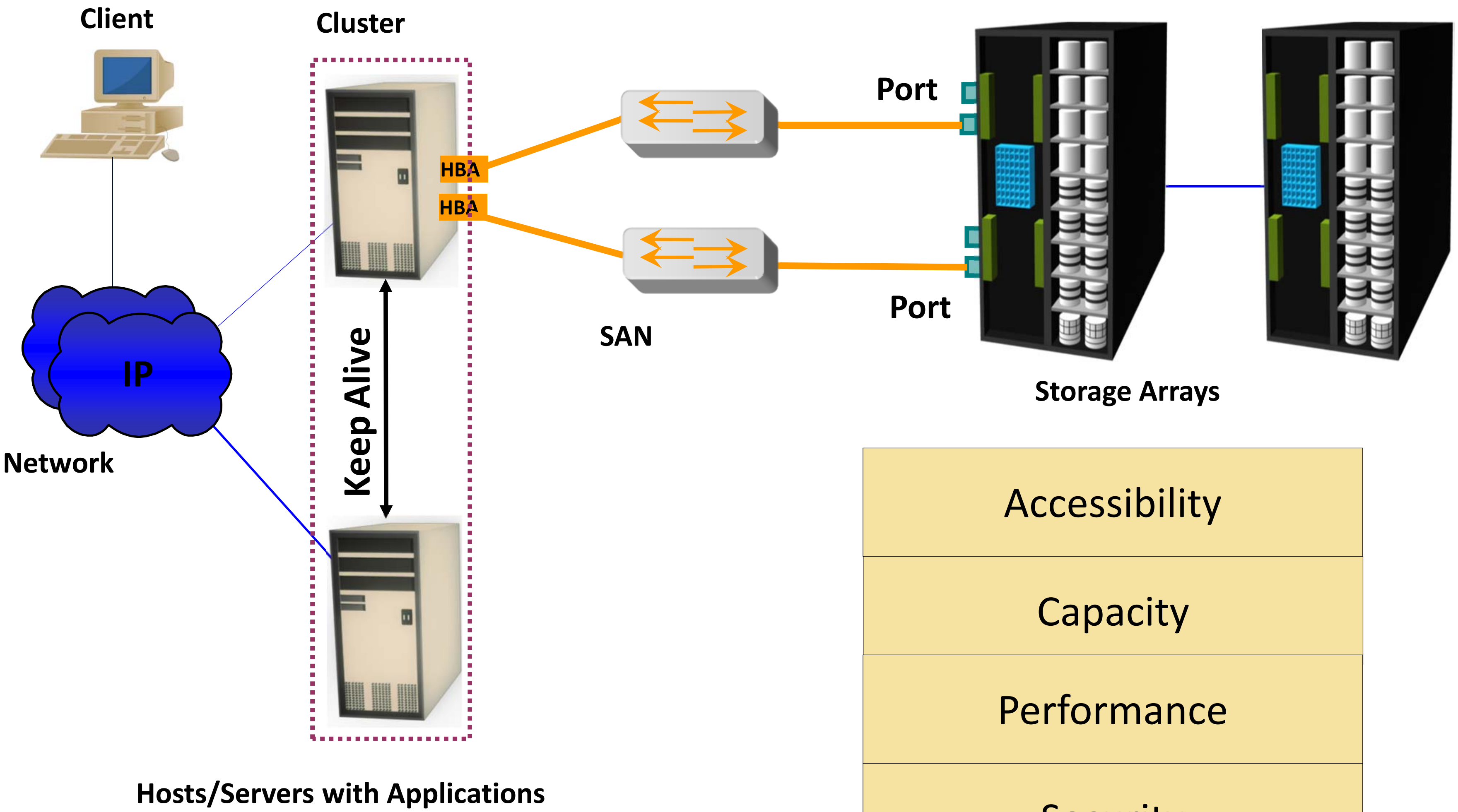
Countermeasures to Vulnerability

- Implement countermeasures (safeguards or controls) in order to lessen the impact of vulnerabilities
- Controls are technical or non-technical
  - Technical
    - implemented in computer hardware, software, or firmware
  - Non-technical
    - Administrative (policies, standards)
    - Physical (guards, gates)
- Controls provide different functions
  - Preventive – prevent an attack
  - Corrective – reduce the effect of an attack
  - Detective – discover attacks and trigger preventive/corrective controls

Storage Security Domains



Monitoring Storage Infrastructure



Accessibility

Capacity

Performance

Security

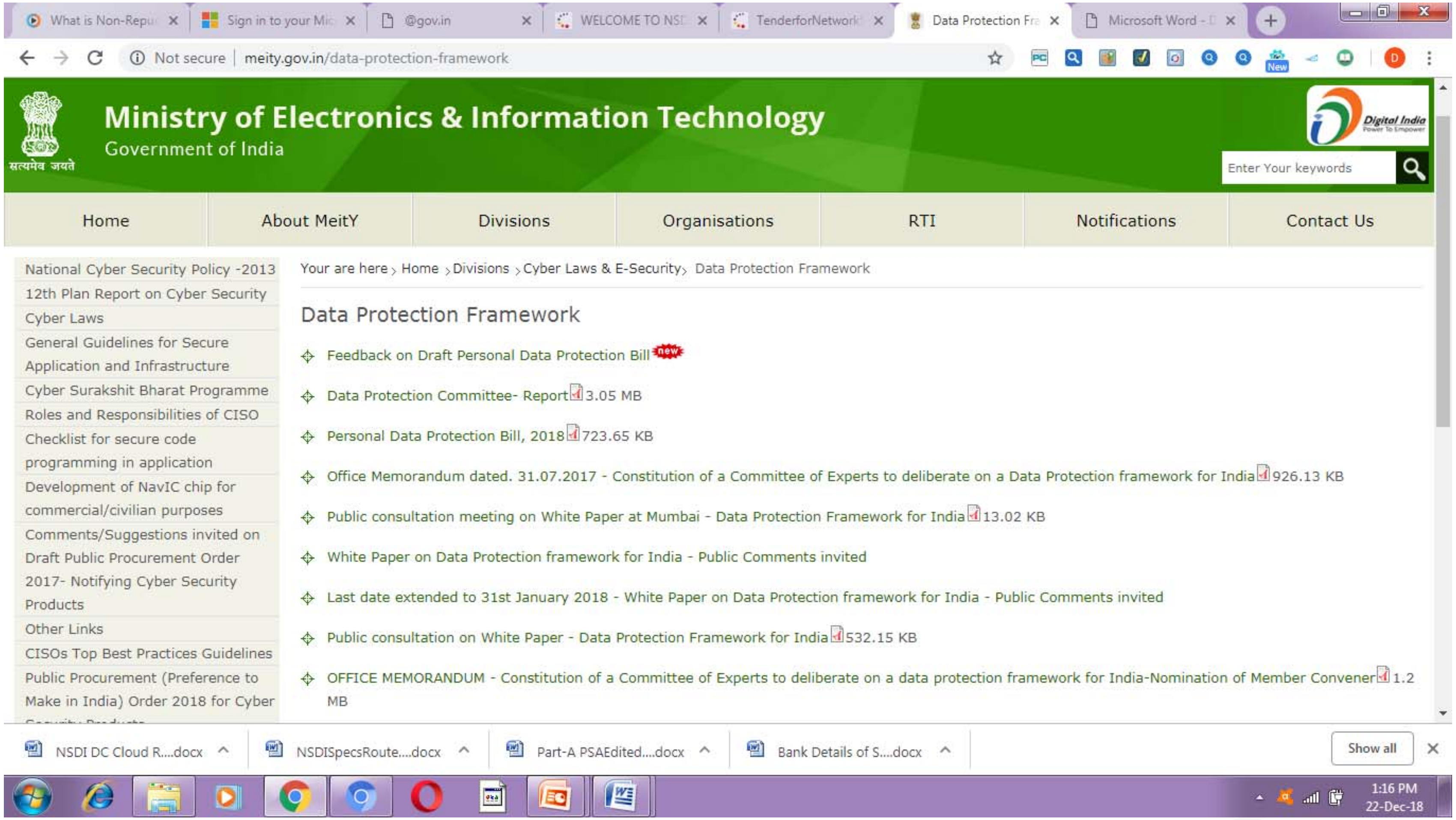
Monitoring Hosts

- Accessibility
  - Hardware components: HBA, NIC, graphic card, internal disk
  - Status of various processes/applications
- Capacity
  - File system utilization
  - Database: Table space/log space utilization
  - User quota
- Performance
  - CPU and memory utilization
  - Transaction response times
- Security
  - Login and authorization
  - Physical security (Data center access)

Storage Infrastructure Management Challenges

- Large number and variety of storage arrays, networks, servers, databases and applications
- Variety of storage devices varying in capacity, performance and protection methodologies
- Deployment of both SAN and IP networks for storage devices
- Servers with different operating systems: UNIX, LINUX, Windows, mainframe
- Interoperability issues between devices from multiple vendors
- Multiple vendor-specific tools to monitor devices from different vendors

Geo Spatial Security in India



Ministry of Electronics & Information Technology

Government of India

Home | About MeitY | Divisions | Organisations | RTI | Notifications | Contact Us

- National Cyber Security Policy -2013
- 12th Plan Report on Cyber Security
- Cyber Laws
- General Guidelines for Secure Application and Infrastructure
- Cyber Surakshit Bharat Programme
- Roles and Responsibilities of CISO
- Checklist for secure code programming in application
- Development of NavIC chip for commercial/civilian purposes
- Comments/Suggestions invited on Draft Public Procurement Order 2017- Notifying Cyber Security Products
- Other Links
- CISOs Top Best Practices Guidelines
- Public Procurement (Preference to Make in India) Order 2018 for Cyber

Your are here › Home › Divisions › Cyber Laws & E-Security › Data Protection Framework

Data Protection Framework

- Feedback on Draft Personal Data Protection Bill new
- Data Protection Committee- Report 3.05 MB
- Personal Data Protection Bill, 2018 723.65 KB
- Office Memorandum dated. 31.07.2017 - Constitution of a Committee of Experts to deliberate on a Data Protection framework for India 926.13 KB
- Public consultation meeting on White Paper at Mumbai - Data Protection Framework for India 13.02 KB
- White Paper on Data Protection framework for India - Public Comments invited
- Last date extended to 31st January 2018 - White Paper on Data Protection framework for India - Public Comments invited
- Public consultation on White Paper - Data Protection Framework for India 532.15 KB
- OFFICE MEMORANDUM - Constitution of a Committee of Experts to deliberate on a data protection framework for India-Nomination of Member Convener 1.2 MB