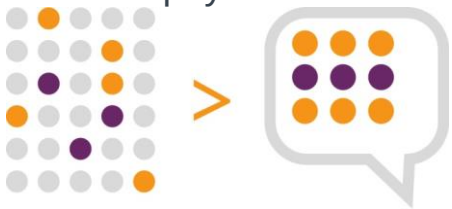
PKI in e-Governance

keeping you ahead

Governance to eGovernance

`> Visibility

From scattered information on physical files TO a consolidated dashboard that can be accessed from anywhere



> Efficiency

From manual work processes with lost bandwidth in finding the files as well as status of a particular work item TO a central system that allows for tracking of work status of a particular item without having to ask anyone

> Analytics

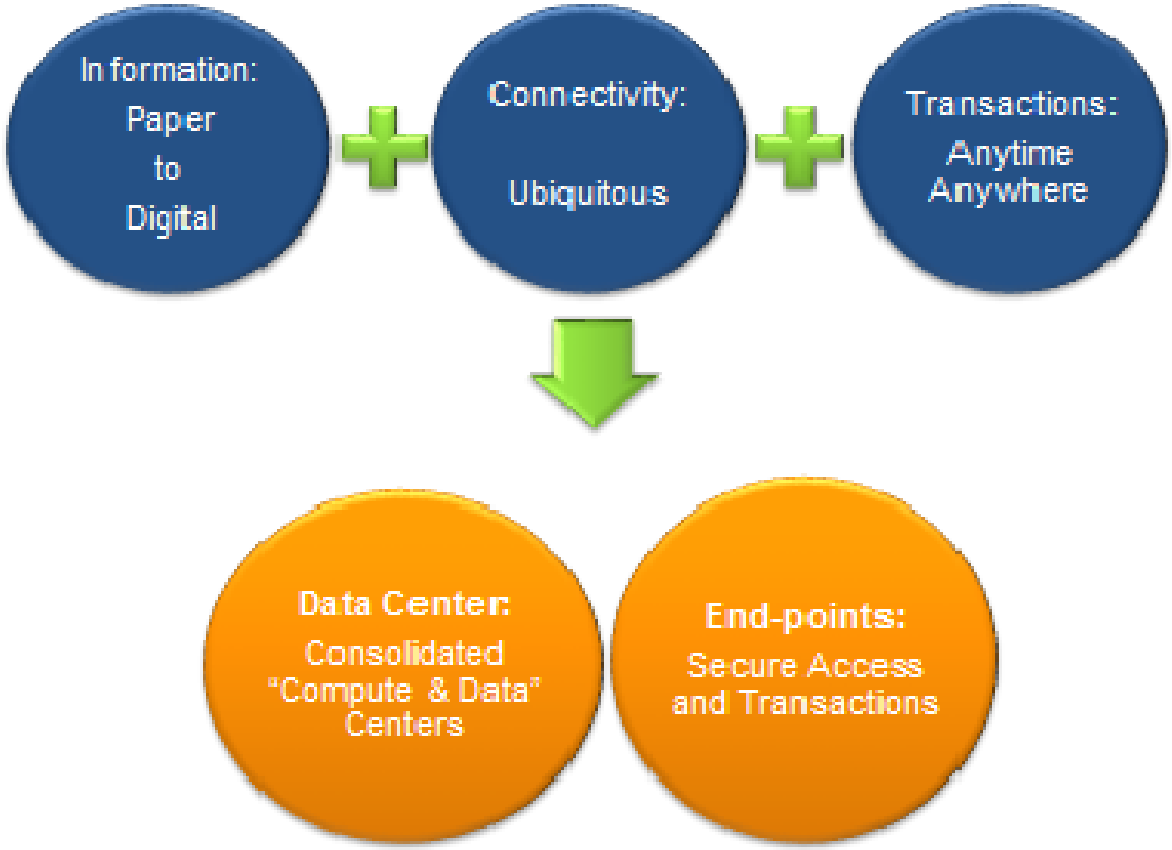
From missing information to delays in getting the information TO real time analytics

keeping you ahead

Governance to eGovernance The Trade-Offs

sify keeping you ahead

Evolving towards eGovernance



sify keeping you ahead

eGOVERNANCE
Business Dynamics

Increase Citizen and Service Adoption

• Drive new services and delivery channels to broadest range of user profiles, speeding up their G2B, G2C and G2G transaction needs

Increase Operational Efficiencies

Streamline deployment & management of systems and Reduce Time and Costs through

•Efficiency Improvement
•Reduce red-tape and bureaucracy
•Real-time Analytics

Compliance

Adherence to requirements of standards such as

•India IT Act (protection of PII, legal liabilities)
•CCA guidelines (digital certificates on hardware tokens)
•Central Vigilance Commission guidelines (cryptographic data protection)

sify keeping you ahead

AWARENESS Cyber Attacks

- The Sources
  - Employees
  - Amateur -> Organized
    - Hacktivists, Cyber Criminals
  - Nations
- The Method
  - Malware is the most prevalent method of cyber attacks today
    - Trojans, Rootkits, Worms, Viruses
  - DDOS
  - Lost Devices
  - Phishing, SQL Injection

sify keeping you ahead

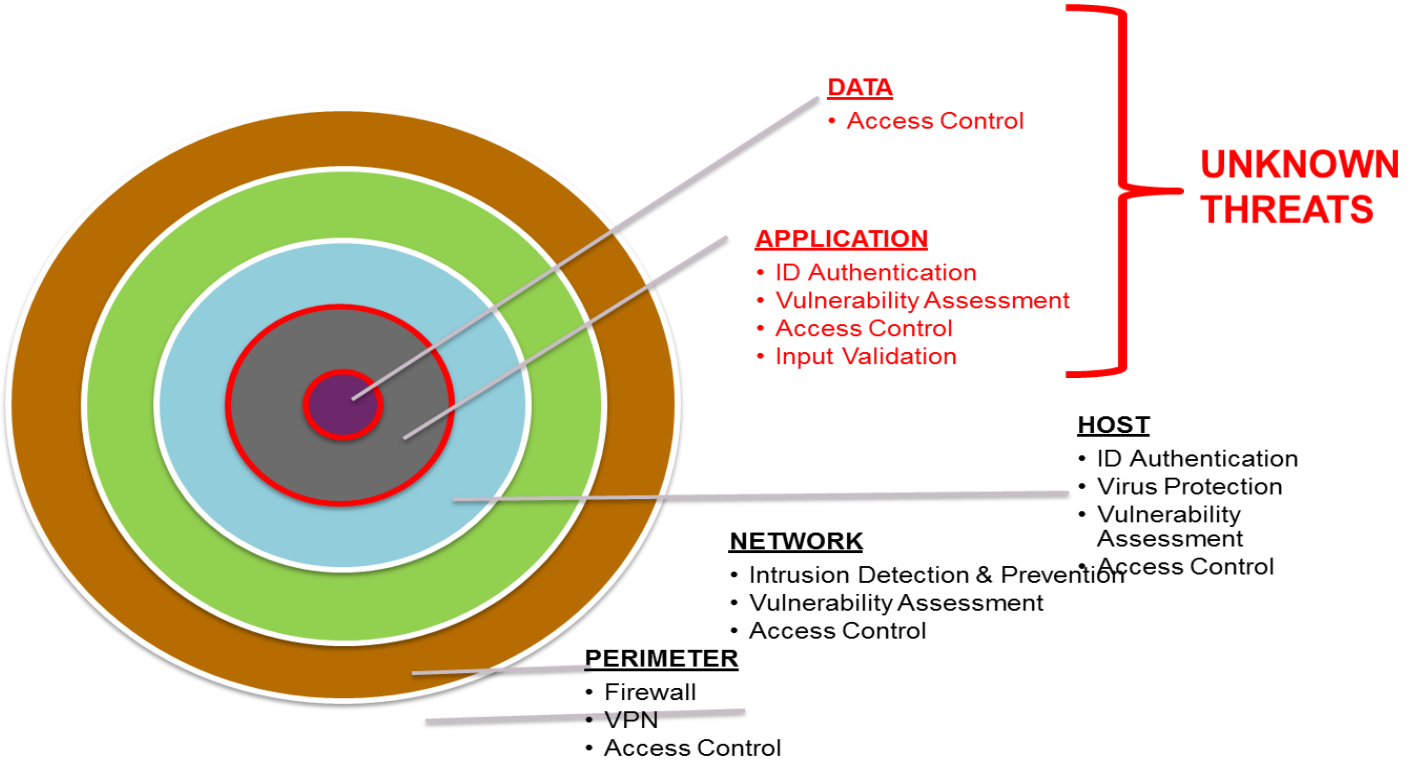
AWARENESS Cyber Attacks

- The Impact*
- Cyber attacks are very costly
- $1.5 million - $36.5 million lost every year per company annually
- Information Theft is the costliest loss due to cyber attacks
- Business Disruption, follows
- An organization encounters 1.4 successful attacks per week
- Detection and Recovery are the costliest activities
- Average number of days to resolve cyber attacks is 18
- Malicious insider attacks take more than 45 days to recover

To eliminate the threat, identify the ***Motive***!

sify keeping you ahead

An eGovernance Ecosystem



sify keeping you ahead

Protection needs to be *centered* on data itself.

Data-centric Protection Security Strategy Objectives

- Data Confidentiality
- Integrity of digitized information
- Non Repudiation In Transactions
- Authenticity

sify keeping you ahead

- **SafeScrypt Security Solutions**
  - SafeScrypt - First Licensed CA in India
  - SafeScrypt CA Services
    - Offers multiple classes of digital certificate to meet varying levels of trust
    - Direct Certificate subscription services follows stringent CCA and Internationally acclaimed regulations meeting very high levels of Trust and Security
    - SafeScrypt MPKI Services make certificate life cycle management simple and cost effective
  - SafeScrypt Security Products
    - Standards compliant state-of-the-art PKI enabling products makes usage of digital certificates and digital signatures simple and effective
  - Securing online applications with SafeScrypt Security Products:
    - Reduces go-to-market efforts for online applications & portals
    - Shorter implementation cycles – reduces costs
    - Higher performance using state-of-the-art techniques

sify keeping you ahead

- E-Security Compliance(including CVC Guidelines)

	Issues to be checked	
1	eProcurement System should deploy **PKI based technologies** for authenticating the bids, and opening electronic tender box. Secure methodology for decrypting bids should be deployed corresponding to the encryption methodology deployed (viz symmetric, or PKI-based asymmetric).	Page 6
2	**Data Storage Security Audit** This is to be done to ensure the use of standard and strong cryptography while storing the sensitive data and user credentials in the application or associated data base. It is also verified that the cryptography used is compliant with the Information Technology Act and the CVC guidelines	Page 12
3	The information on reaching the server where e-procurement software is deployed through SSL mode will remain encrypted even after the SSL encryption is removed. Information will lie encrypted in the system hosting eprocurement software. Data Base Administrator (DBA) will not be able to decrypt the information as he will not be having the decryption keys. **It may be mentioned here that at no point of time the System Administrator or Data Base Administrator should be authorized to hold the private (decryption) key.**	Page 27

sify keeping you ahead

E-Security Compliance(including CVC Guidelines)

	Issues to be checked	
7	**Encryption for data storage:** Sensitive data should be encrypted or hashed in the database and file system. The application should differentiate between data that is sensitive to disclosure and must be encrypted, data that is sensitive only to tampering and for which a keyed hash value (HMAC) must be generated, and data that can be irreversibly transformed (hashed) without loss of functionality (such as passwords). The application should store keys used for decryption separately from the encrypted data.	Page No. 50;Table 5;Sl.No: 1 Page No. 19;Sl.No: CVC Guidelines
8	**Data transfer security:** Sensitive data should be encrypted prior to transmission to other components.	Page No. 50;Table 5;Sl.No: 1 Page No. 19;Sl.No: CVC Guidelines
9	**Insecure Cryptographic Storage** Many web applications do not properly protect sensitive data, such as **credit cards**, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.	A7 Controls – Pg 81 e-procurement guidelines

sify keeping you ahead

Compliance with IT ACT (IT ACT 2000 and Amendment 2008)

	Issues to be checked	
1	**Data Protection:** i) Adequate and reasonable security practices and procedures are in place to protect confidentiality and integrity of the users data and credentials	IT Ref:43A, Draft rule under Section 43A Page No:73;Sl.No.3 IT Rules 2011
2	The private key or the signature creation data should not be stored in the e-Procurement System or kept under the control of the e-Procurement Service Provider.	Page No. 72;Sl.No.1(ii)

Components to build Trust

- Data Privacy → Encryption
- Who am I dealing with? → Authentication
- Message integrity → Message Digest
- Non-repudiation → Digital Signature
- Access Control → Certificate Attributes

sify keeping you ahead

Common e-Security Technologies

	Authentication	Confidentiality	Integrity	Non-repudiation
Anti-virus			✓	
Firewalls	✓	✓		
Access Control	✓	✓		
Encryption		✓		
Public Key Infrastructure	✓	✓	✓	✓

sify keeping you ahead

Success Stories.

Income Tax Department

As a part of the day to day functioning of the Department, Officers and other employees are/will be required to issue letters, notices, orders to Income Tax assesses or other addressees within the Department or outside or upload documents, reports, forms or to perform several ITBA / Human Resource Management System related activities like APAR, IPR etc. on the ITBA system. In order to enable digital authentication of such communications within and outside the Department, it is envisaged that the officers and other select employees shall use the Digital Signature Certificate issued to them by the Department to digitally sign such letters, notices, orders to Income Tax assesses or other addressees within the Department or outside or upload documents, reports, forms or to perform several ITBA / Human Resource Management System related activities on the ITBA system

.

In this regard, Department has empanelled M/s Sify Technologies Ltd. as a Licensed Certifying Authority (CA) for providing DSC to all officers up to the level of Income Tax Officer or equivalent in the Income Tax Department and also for selected officials such DDOs, AOs or Inspectors based on need

sify keeping you ahead

Cont…

Bank of Baroda

We gave an automated verifier cut signing utility for NACH mandate verification system of NPCI. Files from NPCI come to bank, gets validated from our utility, contents get extracted and presented to Bank. The bank at the eod signs files using the same utility and send the signed file to NPCI

DGS&D : PKI Enablement Of Oracle Forms and Report Signing for DGS&D Application.

FSSAI - FSSAI require digital signing facility for its department user(AO/DO/FSO) to digitally sign the soft copy of Registration Certificates (RC), Licenses, No Objection Certificates (NOC)documents using his/her Digital Signing Certificate (issued by authorized Indian CA).

IFFCO has as a web application that is used by an external community for responding to electronic tenders hosted by IFFCO

sify keeping you ahead

Thanks