Security and Data Privacy under Digital India and IT Security Trends

by

Vinai Kumar Kanaujia, Director(IT)

Department of Telecommunications

Minsitry of Communications

Government of India

Agenda/ Discussion Points

1) Digital India
2) Security versus Privacy
3) Security
   - Communication Sector
   - Banking Sector
   - Health Care Sector
   - CERT-In
4) Data Privacy
5) IT Security Trends

Digital India

India's Digital Profile

- World second largest telecommunication market after China
- More than one billion Mobile phones users and nearly half a billion Internet users
- Highest mobile data consumption in the world (3.7 million gigabytes per month)
- Over 200 million social media users
- About 200 million users of Mobile Banking/ Digital Payments

Digital India

- A programme to transform India into a digitally empowered society and knowledge economy

  IT(India Talent) **+ IT**(Information Tech) **= IT** (India Tomorrow)

- "Faceless, Paperless, Cashless" service is one of professed role of Digital India

Digital India – Vision areas

Digital Infrastructure as utility to every citizen

Digital Services and Governance on demand

Digital Empowerment of citizens

Digital India – 1st Vision area

- Digital Infrastructure as a Utility to Every Citizen
  - High speed internet
  - Unique digital identity
  - Mobile phone & bank account
  - Access to a Common Service Centre
  - Private space on Cloud
  - **Secure cyber-space**

Digital India – 2nd Vision area

- Digital Governance & Services on Demand
  - Integrated services
  - Availability of services through online & mobile platforms
  - Portable Citizen entitlements on Cloud
  - Ease of doing business
  - Financial transactions electronic & cashless
  - Geospatial Information Systems (GIS) as Decision Support System

Digital India – 3rd Vision area

- Digital Empowerment of Citizens
  - Digital literacy
  - Digital resources
  - Digital resources / services in Indian languages
  - Collaborative digital platforms
  - No physical submission of documents

National e-Transaction Count

- e-Governance projects (more than 3500) under Digital India are generating enormous data (https://etaal.gov.in)
- E-Transactions in 2017:

  30.81 Billion

- E-Transactions in 2018 (Till 14th May 2018)

  11.34 Billion

Security versus Privacy

Security versus Privacy

- **Privacy** determines who ought to be able to legitimately access, use, and alter **data** why those particular actors should be viewed as having legitimate entitlements thereto
- **Security** implements privacy's choices - it mediates between information and privacy selections
- The disclosure is a privacy problem, and the hacks are a security problem

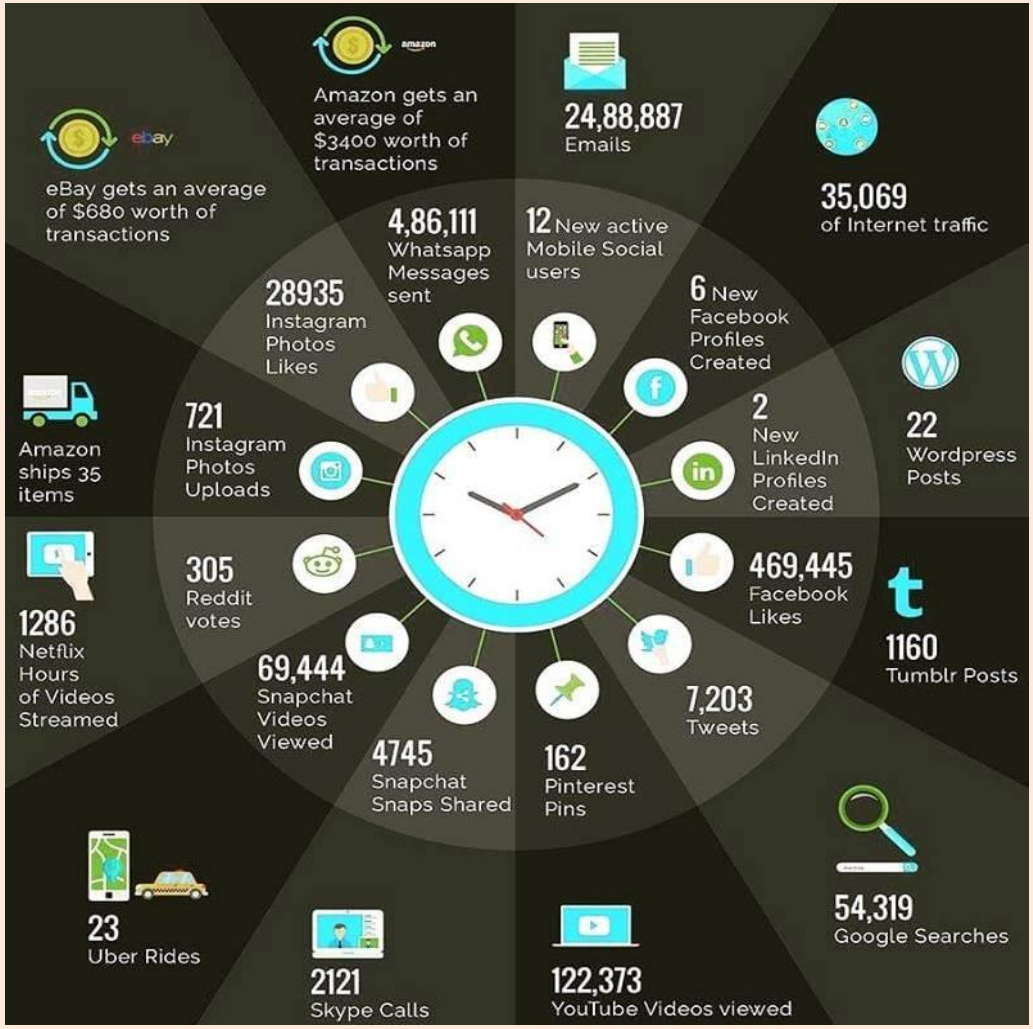
Security/ Privacy - Failure

- **Security failures** generally leave everyone involved (except for the attacker) worse off
- **Privacy failures**, by contrast, leaves user complaining while Service provider and its accomplice are better-off
- Security failures [Innocent or deliberate] should be penalized more readily, and more heavily, than privacy ones, because security flaws make all parties worse off

Quick Exercise

Write down the name of any three Apps frequently used by you on your Mobile/ Tab/ Laptop/ Computer

One second of Internet



Security

(Communication Sector)

Security: Communication Sector

- DoT Notification dated 31.05.2011 amending License Agreement for security related concerns in Telecom/ Internet services
- Numerous provisions inserted in the License agreement between Licensor and Licensee
- **Licensor**: Department of Telecommunications, Government of India
- **Licensee**: Telecom/ Internet Service Providers (TSPs/ ISPs)

Security Policy

- **Licensee** to be completely responsible in respect of their Network
- **Licensee** to frame Policy on Security and Security management of their Networks
- Copy of Security Policy to be submitted to **Licensor**

Security Policy to include

1. Network Forensic
2. Network Hardening
3. Network penetration test
4. Risk assessment
5. Corrective Action
6. Preventive Actions

Security Audit of Network

- Once a year
- As per ISO 15408 and ISO 27001 standards
- By network audit and certification agency

Procurement of Equipment

- **Equipment** to include all contemporary security related features and features related to communication security as prescribed under relevant security standards
- All contemporary security related features to be implemented in the **Network**
- **List** of features, equipment's, software etc. procured and implemented to be retained till they are in use

Induction of Network elements

- After testing and certification as per relevant contemporary Indian or International Security Standards
- IT elements: ISO/IEC 15408 standards
- Information Security Management System: ISO 27000 series standards
- Telecom elements: 3GPP/3GPP2 standards
- Test results & certificates: Retain for 10 years

Manpower

- Employ only **Resident**, trained Indian Nationals as:
  - Chief Technical officer
  - Chief Information Security Officer
  - Nodal Executives for handling interception and monitoring cases
  - Incharge of GMSC, MSC, Softwitch, Central Data base and System Administrator(s)

Records Management (1/2)

- Documentation, including software details to be obtained from manufacturer/ vendor/ supplier in English language
- Operations & Maintenance (O&M) manuals
- O&M Command logs including details of Command, Operator, Location, date and time
  - Online for 12 months
  - Offline for next 24 months

Records Management (2/2)

- List of user ids, along with details of mapped Operator, certified by System Administrator
- List of features, equipment's, software etc. procured and implemented
- Details of each and every Software updations and changes (including firmware)
- Complete details of Supply chain of Hardware & Software since procurement

Remote Access

- Comply with the conditions specified by the Licensor

Monitoring

- Provision for monitoring of all intrusions, attacks and frauds and reporting of the same to **Licensor** and to Computer Emergency Response Team, India (**CERT-IN**)

Inspection

- Suitable agreement with Manufacturer/ Vendor/ Supplier to allow **Licensee**, **Licensor** and/or its designated agency for:
  - inspection of the hardware, software, design, development, manufacturing facility, supply chain
  - **Security/ threat** check of all software & firmware at any time during the supplies of equipment

Agreement with supplier (1/2)

- To be signed by Licensee with manufacturer/ vendor/ supplier
- The equipment/ services/ software are:
  - 'Safe to Connect' in the network
  - checked thoroughly for risks & vulnerabilities
- All addressable vulnerabilities have been fixed
- Non-addressable vulnerabilities have been listed with remedial measures and precautions provided

Agreement with supplier (2/2)

- Include aspects related to security measures like access control, Password control and management etc.
- Include clauses addressing the service continuity and service upgradation
- Consequences to be defined for each party in case of breach, particularly the security breaches

Penalty

- Upto Rs. 50 crores (approx $ 7.7 million) for security breach caused either due to **inadvertent** inadequacy/ inadequacies in precaution by Licensee
- A five members committee (includes two cyber security experts) constituted by Licensor, to determine whether the breach is due to inadvertent inadequacy/inadequacies or otherwise and also to decide the amount of penalty depending upon loss, gravity of breach etc.
- Rs. 50 crores per breach in case of **intentional** omission of Vulnerability leading to the breach

Liability and Criminal Proceedings

- Additionally, action can be initiated under
  - Indian Telegraph Act, 1885
  - Information Technology Act, 2000
  - Indian Penal Code (IPC)
  - Criminal Procedure Code (Cr PC)
- License of TSP/ISP can be cancelled
- Hardware/ Software manufacturer/ vendor/ supplier can be blacklisted in the Country

Location details

- Location details of mobile customers to be provided to the Licensor as a part of Call Detail record(CDR) in form of latitude and longitude, besides the co-ordinate of the cell sites
  - For all mobile calls
  - As per area-wise defined "Limits of accuracy" in meters, which can be modified depending upon technological developments

Security

(Banking Sector)

Security: Banking Sector

- RBI Notification dated 12.09.2009, 15.04.2011, 29.04.2011, 02.06.2016, 09.12.2016
- System audit of Payment Systems so that digital payments ecosystem remain robust and fully secure
- Regulator of Banks: Reserve Bank of India (RBI)

Annual System Audit (1/2)

- By a firm of Chartered Accountants
- To be Conducted by
  - Certified Information Systems Auditor (CISA) and registered with Information Systems Audit and Control Association (ISACA) or
  - Holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI)
- Auditor report to be submitted to RBI

Annual System Audit (2/2)

- Scope of the System Audit includes
  - Evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc.

Special Audit

- By empanelled auditors of Indian Computer Emergency Response Team (CERT-In)
- Audit should cover compliance as per security best practices, specifically the application security lifecycle and patch/vulnerability and change management aspects

Cyber Security Framework in Banks (1/3)

- Board approved Cyber Security Policy elucidating the strategy containing an appropriate approach to combat cyber threats
- Arrangement for continuous surveillance by setting up Security Operations Centre(SOC)
- IT architecture should be conducive to security. It can be upgraded as per the risk assessment in a phased manner

Cyber Security Framework in Banks (2/3)

- Comprehensively address network and database security
- Ensure Protection of customer information
- Cyber Crisis Management Plan addressing following aspects: Detection, Response, recovery & Containment
- Cyber security preparedness indicators

Cyber Security Framework in Banks (3/3)

- Sharing of information on cyber-security incidents with RBI
- Cyber-security awareness among stakeholders/ Top Management/ Board
- To implement at Baseline Cyber Security and Resilience Requirements proposed by RBI

Baseline Cyber Security in Banks (1/4)

1. Inventory Management of Business IT Assets
2. Preventing execution of unauthorised software
3. Environmental Controls
4. Network Management and Security
5. Secure Configuration
6. Application Security Life Cycle (ASLC)

Baseline Cyber Security in Banks (2/4)

7. Patch/Vulnerability & Change Management
8. User Access Control / Management
9. Authentication Framework for Customers
10. Secure mail and messaging systems
11. Vendor Risk Management
12. Removable Media

Baseline Cyber Security in Banks (3/4)

13. Advanced Real-time Threat Defence and Management
14. Anti-Phishing App Service
15. Data Leak prevention strategy
16. Maintenance, Monitoring, and Analysis of Audit Logs
17. Audit Log settings
18. Vulnerability assessment and Penetration Testing

Baseline Cyber Security in Banks (4/4)

19. Incident Response & Management
20. Risk based transaction monitoring
21. Metrics for various activities
22. Forensics
23. User / Employee/ Management Awareness
24. Customer Education and Awareness

Security

(Healthcare Sector)

Security: Health Care Sector

- Ministry of Health and Family Welfare Notification dated 30.12.2016
- Electronic Health Record (**EHR**) **standards v2.0**
- Adoption in IT systems by healthcare institutions/ organizations in India (Health Record IT standards**)**
- Interoperability and content exchange

Electronic Health Record (EHR)

- A **collection** of various medical records that get generated during any clinical encounter or events
- Self-care and homecare devices and systems used by us generate healthcare data 24x7 and this has long-term clinical relevance
- Efficient 21st century healthcare delivery

EHR: Security Management (1/2)

- Standards includes seven items

1) Data Privacy and Security
   - Basic security and privacy management
2) Information Security Management
3) Privilege Management and Access Control
4) Audit Trail and Logs

EHR: Security Management (2/2)

5) Data Integrity
   - Data Hashing with SHA-256 or higher
6) Data Encryption
   - Encryption key length 256 bit or higher
   - Encrypted connection(SSL v3.0, TLS v1.2)
7) Digital Certificate use and Management

Security

(CERT-In)

Security: CERT-In

- Indian Computer Emergency Response Team - India (CERT-in)
- National nodal agency for responding to computer security incidents as and when they occur
- Information Technology Amendment Act 2008, has designated CERT-In as the national agency to perform numerous functions in the area of cyber security

Functions of CERT-In

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

CERT-In empanelled Auditors

- To provide IT Security Auditing services
- Assess the information security risks by
  - **Conducting** vulnerability assessments & penetration testing
  - **Cataloguing** existing security policies and controls
  - **Examining** IT assets for External, Internal & Integrated threats

Cyber Swachhta Kendra (1/3)

- Botnet Cleaning and Malware Analysis Centre
- Launched in the year 2017 by Computer Emergency Response Team - India (CERT-in) under provisions of Section 70B of the Information Technology Act, 2000
- To enhance the cyber security of Digital India's IT infrastructure by providing information on botnet/malware threats and suggesting remedial measures

Cyber Swachhta Kendra (2/3)

- Indigenously developed security tools
  - USB Pratirodh
  - AppSamvid (Application whitelisting)
  - M-Kavach (for Mobile devices)
  - Browser JSGuard
- Alerts on current Cyber security threats and security measures

Cyber Swachhta Kendra (3/3)

- Security Best Practices
  - Digital Payment Suraksha
    - Merchants & Customer
  - Security for Personal Computer
    - Parents, Children, Women & Businesses
  - Security Tips for Common user
    - Desktop Security, Broadband Security, USB Security, Avoid Phishing Attack & Mobile Phone Security

Data Privacy

Data Privacy (1/3)

- Knowledge about a person gives a power over that person (Data->Information->Knowledge)
- We create perpetual digital footprints on **social network websites** on a 24/7 basis as we learn our 'ABCs': Apple, Bluetooth, and Chat followed by Download, E-Mail, Facebook, Google, Hotmail, and Instagram
- Humans forget, but the internet does not forget and does not let humans forget. In the **digital world** preservation is the norm and forgetting a struggle

Data Privacy (2/3)

- **Uber**, the world's largest taxi company, owns no vehicles
- **Facebook**, the world's most popular media owner, creates no content
- **Alibaba**, the most valuable retailer, has no inventory
- **Airbnb**, the world's largest accommodation provider, owns no real estate

Data Privacy (3/3)

- Without any **data protection Law**:
  - Profiling of individuals
  - Increased surveillance
  - An impact on individual independence

Data Privacy: IT Act, 2000 (1/2)

- Section 43A of IT Act provides that where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected

Data Privacy: IT Act, 2000 (2/2)

- Section 72A of IT Act provides for the punishment for intentionally or knowingly disclosing personal information relating to a person that was acquired for providing services under a lawful contract, without the consent of the person concerned or in breach of a lawful contract

Right to Privacy (1/2)

- **Supreme Court of India** in judgement dated 24.08.2017 recognised the Right to Privacy as a fundamental right
- It stated that Right to Privacy is protected as an intrinsic part of the right to life and personal liberty under the Constitution of India

Right to Privacy (2/2)

- Informational privacy is a facet of the Right to Privacy. The dangers to privacy in an age of information can originate not only from the **state** but from **non-state actors** as well
- Government of India to put in place a robust regime for data protection with a careful and sensitive **balance** between individual interests and legitimate concerns of the state

Data Protection Framework of India (1/3)

- The Government of India has constituted a Committee of Expert on 31.07.2017 to Identify and study the key issues relating to data protection in India, make Specific suggestions on principles underlying a data protection framework in India and suggest a Data Protection Bill paving way for Data Protection Law
- The Committee has issued a White Paper, completed public consultation and its report is awaited

Data Protection Framework of India (2/3)

- Broad scope defined by Committee
  a) the territorial reach of the law
  b) the contours of personal data
  c) the application of the law to the private and the public sector
  d) the entities regulated by the law
  e) the activities regulated by the law
  f) cross border flow of data and
  g) data localisation

Data Protection Framework of India (3/3)

- Individual participation rights being considered by Committee
  a) confirmation and access
  b) rectification
  c) objection to processing
  d) objection to automated decision making
  e) restriction of processing
  f) data portability and
  g) right to be forgotten

IT Security Trends

Cyberworld

- An increasing interconnected world
- Proliferation of Digital Identities
- Adoption of new digital technologies and process – SMAC technologies
- Both Government and Business are evolving
- **Multitude** of Vulnerabilities and exponential **increase** in threat perception

Prominent Cyber attacks in recent past in India (1/2)

- **Union Bank of India heist** (June 2016): Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171 million, Prompt action helped the bank recover almost the entire money
- **Wannacry Ransomware** (May 2017): The global ransomware attack took its toll in India with several thousands **computers getting locked** down by ransom-seeking hackers.

Prominent Cyber attacks in recent past in India (2/2)

- **Data theft at Zomato** (May 2017): The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web
- **Petyya Ransomware** (June 2017): The ransomware attack made its impact felt across the world, including India.

Hardware/Firmware Concerns

- Software builds on hardware, Hardware is the root of trust. Security begins with a trustworthy hardware!!!
- Manufacturing backdoors may be created for malware or other penetrative purposes or/ and Faults may be included for causing the interruption in the normal behavior of the IT equipment
- Systems are vulnerable to cyber threats as Most equipment and technology in India are currently procured from global sources

Privacy and Data Protection

- Increased focus on Privacy and personal data protection. Growing number of organizations are now processing **Aadhaar**-related information and personally identifiable information of customers
- In view of the **Supreme Court of India's** ruling in favour of 'Right to Privacy' Organizations are showing keen interest in advanced encryption and key management technologies in order to secure customer data

Security to be the boardroom issue

- Securing **data** is one thing but the value that security offers to business is huge especially in terms of regulatory compliance, potential lost revenue, customer relationships, legal liability, competition, intellectual property, stockholder loyalty and brand protection et
- Security is no more a technology issue rather it is gradually becoming a part of a regular boardroom/ top management discussion

Protecting Physical lives from breach

- Medical device or wearable that is hacked and remotely controlled
- Industrial IoT device or self-driving car getting compromised
- Blue Whale Challenge Game (The suicide game) - Players (generally children's suffering from depression) can’t stop playing once they’ve started; they are blackmailed and cyber bullied into completing the “game”

End-user education (1/2)

- User benefits as well as no. of unprotected computers, that are available for hijacking by criminals to mount attacks, are reduced
- Be cautious about all communications; think before you click. Don't reveal too much information about yourself on social media websites. Depending on the information you reveal, you could become the target

End-user education (2/2)

- Smart phones and other mobile devices - Encryption and Password protection
- Proper configuration and patching of operating systems, browsers, and other software programs in all devices – Mobile, computer, browser, Router, TV, AC, Fridge etc
- Use and regular updation of firewalls, anti-virus, and anti-spyware programs

Cyber Surakshit Bharat programme

- Training around 1200 Chief Information Security Officers(**CISOs**) of Central Government, State Government, Banks, Public Sector Undertakings etc. to address impending Cyber Security challenges

To conclude or To begin….

- SEC_RITY is not complete without U

- Security by design (Architecture)
  - Machine/ System
  - Man


thank you
danke
рахмат
謝謝
spas
ngiyabonga
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
gracias
хвала
kiitos
dankie
nanni
nandri
dhanyavad
bedankt
maururu
köszönöm
hvala
gràcie
bayarlalaa
asante
manana
obrigada
tenki
enkosi
akun
dankon
aĉiū
djiere dieuf
tau
mochchakkeram
murakoze
dziękuję
дякую
mamnun
chokrane
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dēkuji
taiku
obrigado
mèsi
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
ありがとう
didi madloba
najis tuke
tanemirt
grazie
kam sah hamnida
rahmat
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
mercé
мерси
ευχαριστώ
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

You can contact me…

Vinai Kumar Kanaujia
Director(Information Technology)
Department of Telecommunications
Ministry of Communications
Room No. 1005, Sanchar Bhawan, 20, Ashoka Road,
New Delhi –110001
Telephone: +91 11 23036509
Mobile: +91 9013131052
Email: vk.kanaujia@gov.in