GRID INFOCOM
YOUR ADVANTAGE

simply perform as you expect

Information Security …

It's All About COMPLIANCE Honey!

INDIAN Honeynet PROJECT

OPEN SECURITY ALLIANCE

DINESH BAREJA
08 October 2011

about.me
It's all about you.

ME: Dinesh Bareja (dinesh.bareja@gridinfocom.com)

AT: Grid Infocom Pvt Ltd, Gurgaon

AS: VP and Principal Consultant (Information Security)

CERTS: CISA, CISM, ITIL, BS7799, Cert in IPR, ERM

ASSNS: ISACA, Indian Honeynet Project, NULL, ClubHack, NSD, Open Security Alliance, The FAQ Project.

An InfoSec professional I believe real life provides most of the answers to the problems that ail cyberia. My heart is happily under constant attack by the dynamics / excitement of the security business, and I happily live in a state of constant surprise at the ignorance of those who think they are secure. Try to give back to the community, in my own small way, for the perennial flow of knowledge, learning and friends.

INDIAN Honeynet PROJECT

COCON

GRID INFOCOM YOUR ADVANTAGE

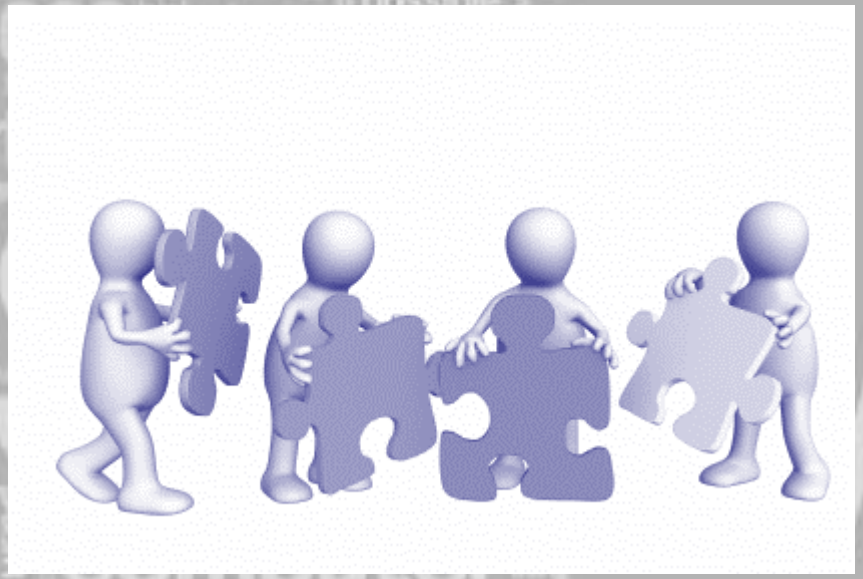
This talk is about…

- Information Security – where does it come into an organization, how…. Why, when..
- InfoSec Drivers – what drives IS
- Analyst reports about IS drivers
- International Regulations
- India – Compliance Drivers

Information Security… what, why, when …

- Good Controls (thinking)
- Awareness
- Compliance (good habits)
- Tools
- Efficiency
- Process Hygiene
- Technology Management

- 24 x 7 x 365
- Proactive … Real time



A LOT OF HARD WORK THAT IS NEVER ENOUGH

IT'S ABOUT COMPLIANCE ..
You are never in order ☺

Information Security Components

- Governance
- Risk
- Compliance
- Availability
- Accessibility
- Accountability

And What Drives InfoSecurity

- Technology Upgrades
- Forward thinking management
- CxO buy in
- Optimized Processes
- Customer Requirements
- Post Incident trauma
- Organization Growth and Maturity

Compliance?

Primary Driver for Information Security

"Compliance with incident disclosure laws, Payment Card Industry Data Security Standard (PCI-DSS), and data privacy regulations is the primary driver of our data security."

40% Agree

49% Strongly Agree

"The Value Of Corporate Secrets," a commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

Primary Driver for Information Security

"Compliance" of all types has become the primary driver of data security programs. Nearly 90% of surveyed enterprises agreed that compliance with PCI-DSS, Data Privacy laws, Data Breach regulations, and existing Data Security Policies is the primary driver of their data security programs

40% Agree

49% Strongly Agree

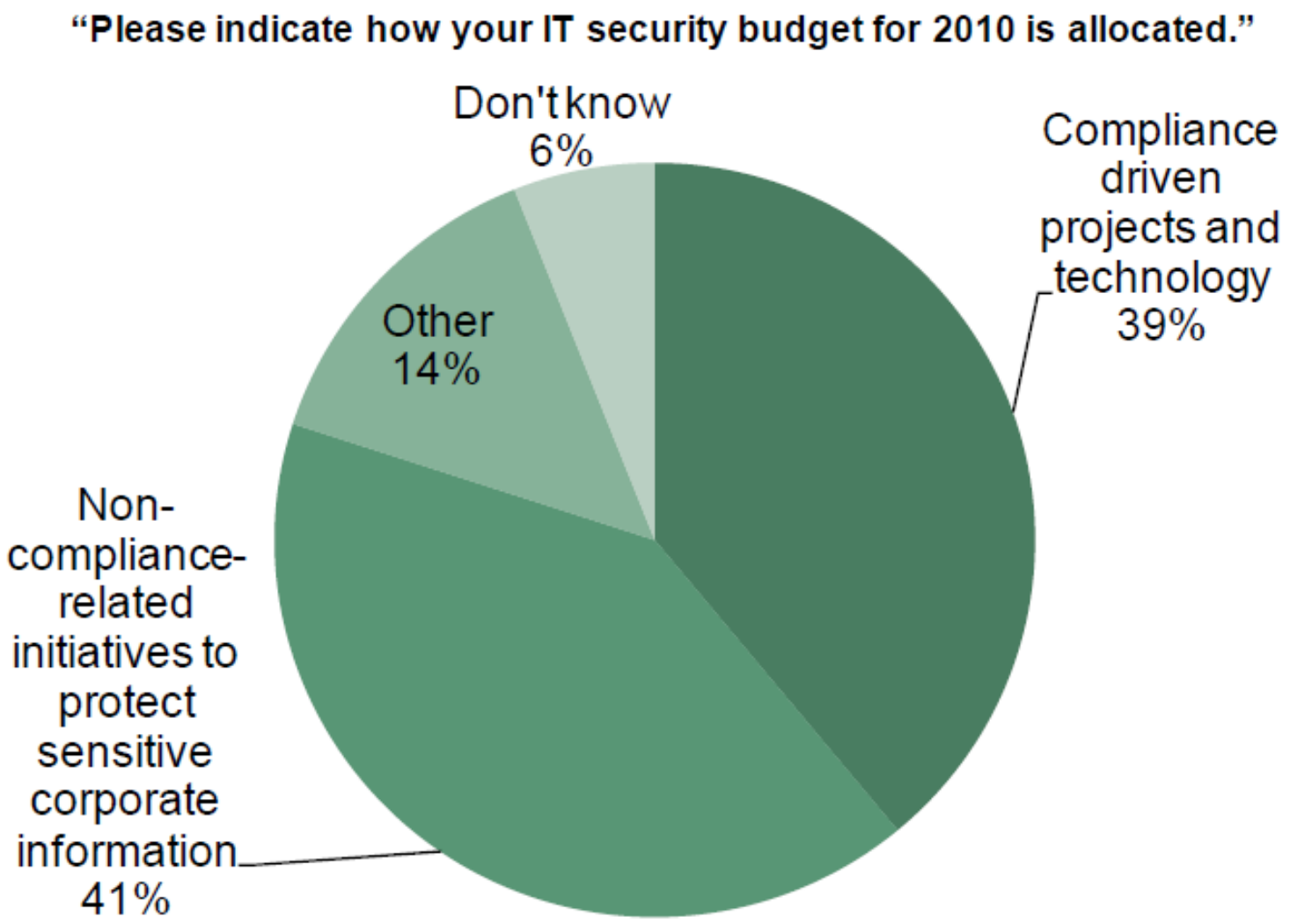
"The Value Of Corporate Secrets," a commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

Why Regulations

- Regulators impose rules to ensure that business risks are minimized
- Corporate accounting scandals and frauds
- Global financial crisis / recession
- Corporate Governance
- Accountability to shareholders
- Guarantee of quality of service
- Compliance rules may prescribe not only a code of conduct for employees, but also how compliance is to be verified
- Non compliance may result in penalties

Figure 4

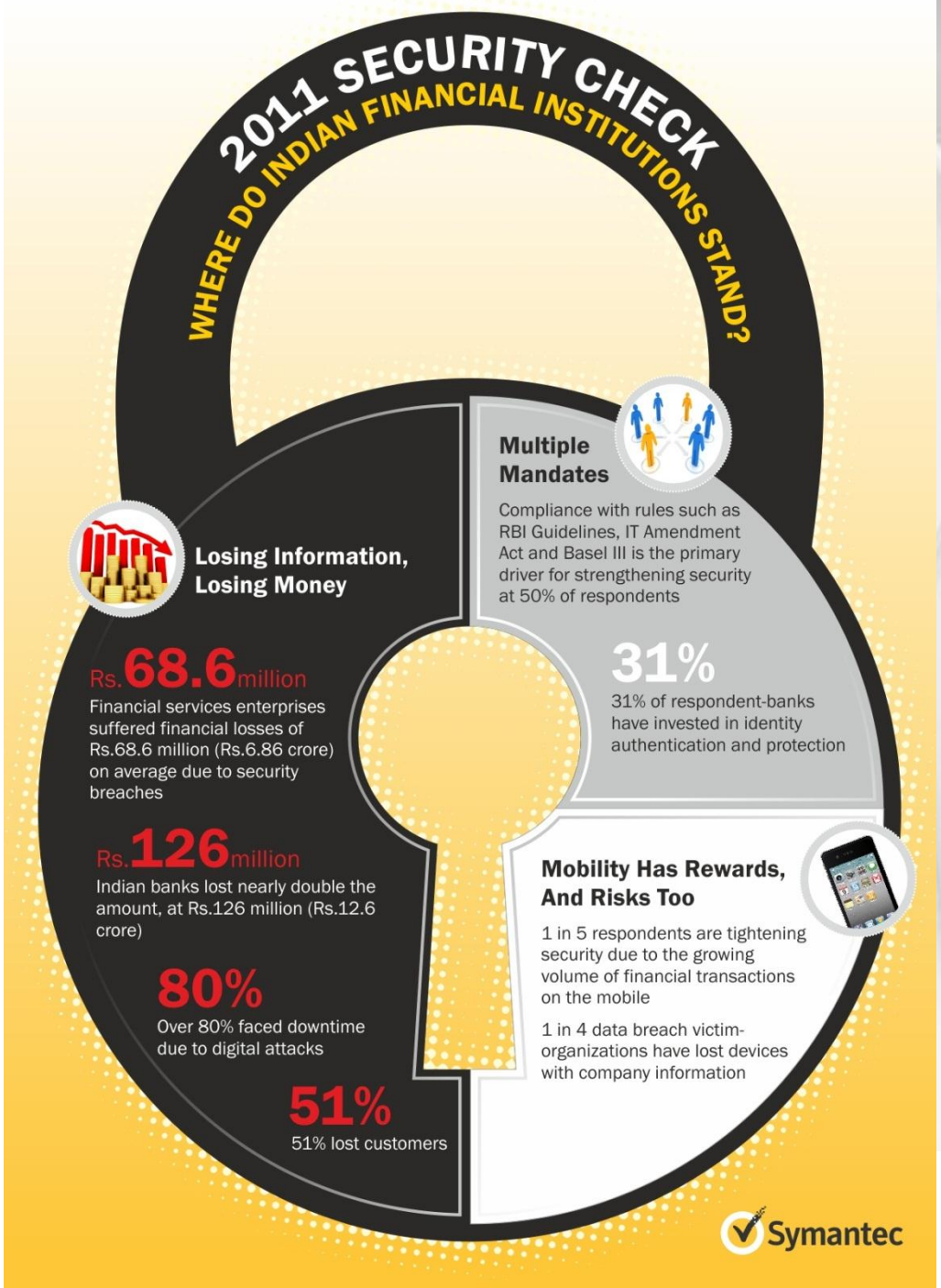
Compliance Drives Budgets, But Enterprises Underinvest In Other Data Security Areas



The_Value_of_Corporate_Secrets : Source: A commissioned study co[illegible]ting on behalf of RSA and Microsoft, November 2009

Regulatory compliance is the key driver of IT security adoption for 50 % of Indian financial services enterprises

Symantec Security Check – Indian Financial Services Industry 2011 (Banking, Financial Services and Insurance industries).



Overview

What's driving information security at large organizations? In spite of all of the headlines, data breaches, and malicious code exploits, information security remains largely driven by government and industry regulations like FISMA, HIPAA, GLBA, and PCI DSS (see Figure 1).[1]

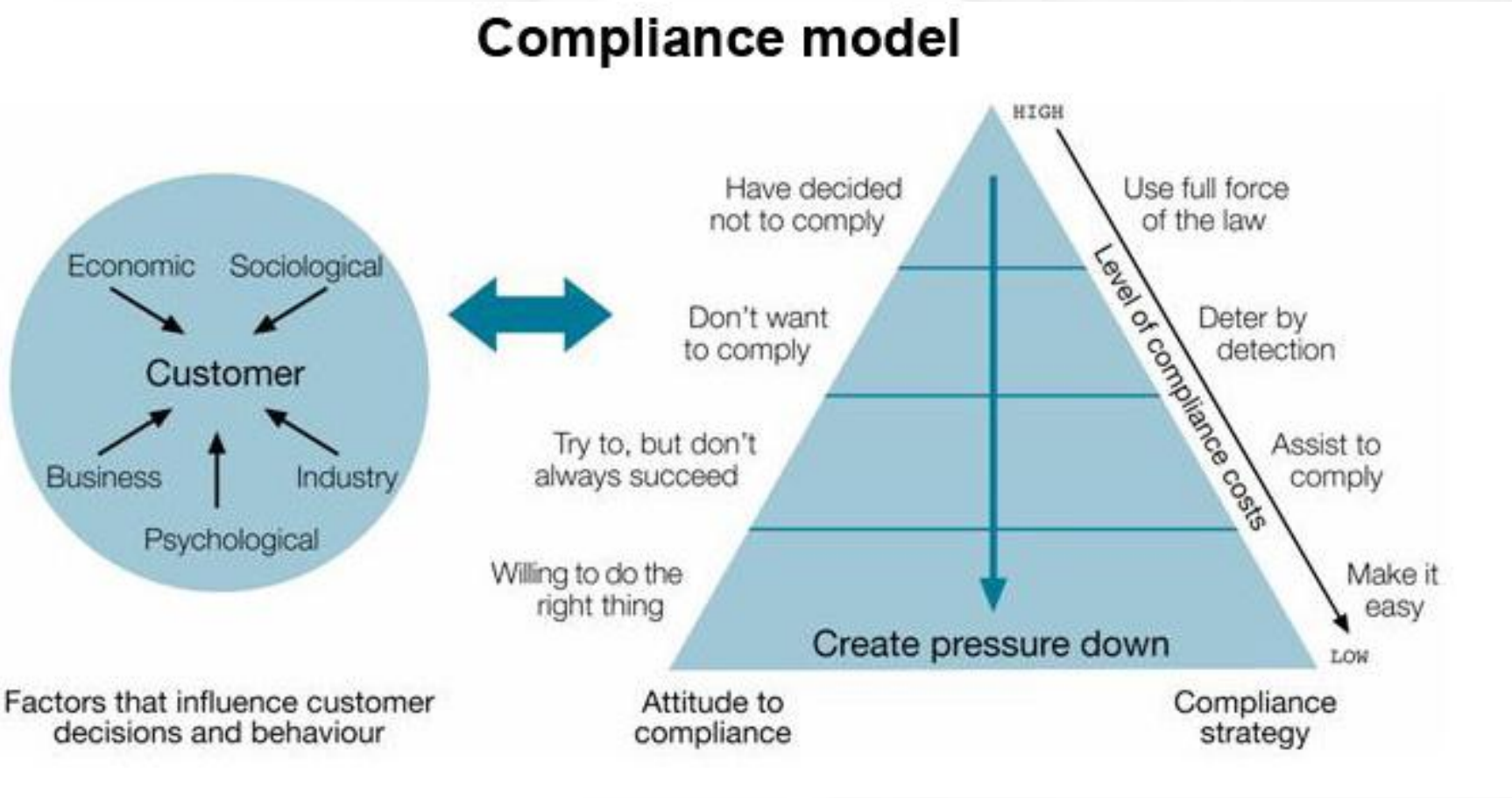
Figure 1. Regulatory Compliance Drives Information Security

Source: Enterprise Strategy Group, 2009.

Linking information security to regulatory compliance isn't necessarily a bad thing. After all, regulations like PCI DSS are meant to establish a comprehensive security baseline for organizations handling credit cards and personally identifiable information (PII) and address potential risks to this data. Regulatory compliance is far from a panacea, however. When

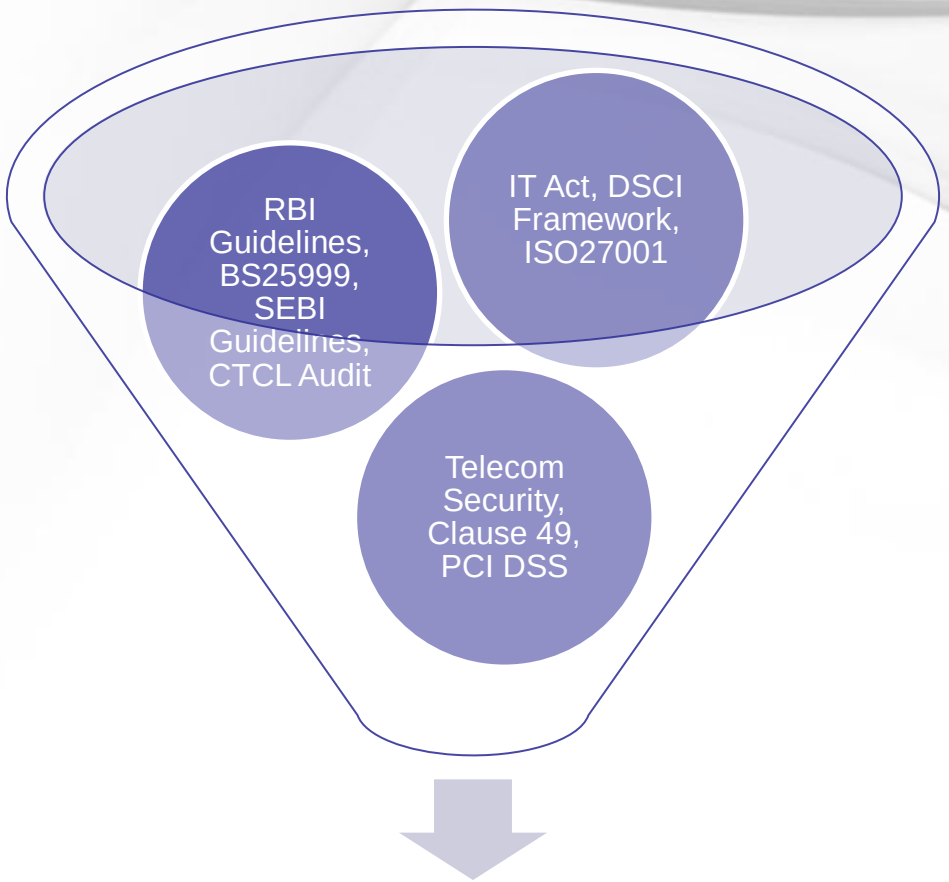
Why Should I Comply

- Internal Revenue, New Zealand




Compliance
following
compliance
organizational
regulations
laws
rules
Authority
requirements
codes
process
business
organization
people
Documents
programs
use
comply
set
authority
among
reading
often
one
transactions
foisted
really
applies
policies
effected
promote
measurable
prevent
identify
governing
mean
also
breaches
executed
effect
material
direct
control
arrangements
nature
externally
personnel
complied
government
break
type
confusing
accordance
subject
means
instilled
simply
driven
industry
identified
become
statements
contractual
aim
guidance
provide
respond
supplementary
always
call
time
stewardship
apt
ensuring
required
met
writers
cheated
However
course
i.e
imposed
information
management
wide
broken
bent
occurring
within
program
criteria
think
documents
doctrines
designed
audit
financial
solitaire
put
place
left
human
controls
image
necessary
need
ensure
culture
least
words
mess
plethora
assurance
limit
reasonable
budget
follow

The Regulatory Cocktail



Compliance Requirements lead to Information Security

Regulatory / Compliance Requirement Extracts

- **FISMA Section 3534** *"(a) The head of each [Federal] agency shall delegate to the agency Chief Information Officer ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques;"*
- **ISO 27002 Section 5.1** *"A written policy document should be available to all employees responsible for information security"*
- **HIPAA Security Final Rule, 164.316 (a) Policies and Procedures** *"(R) Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart."*

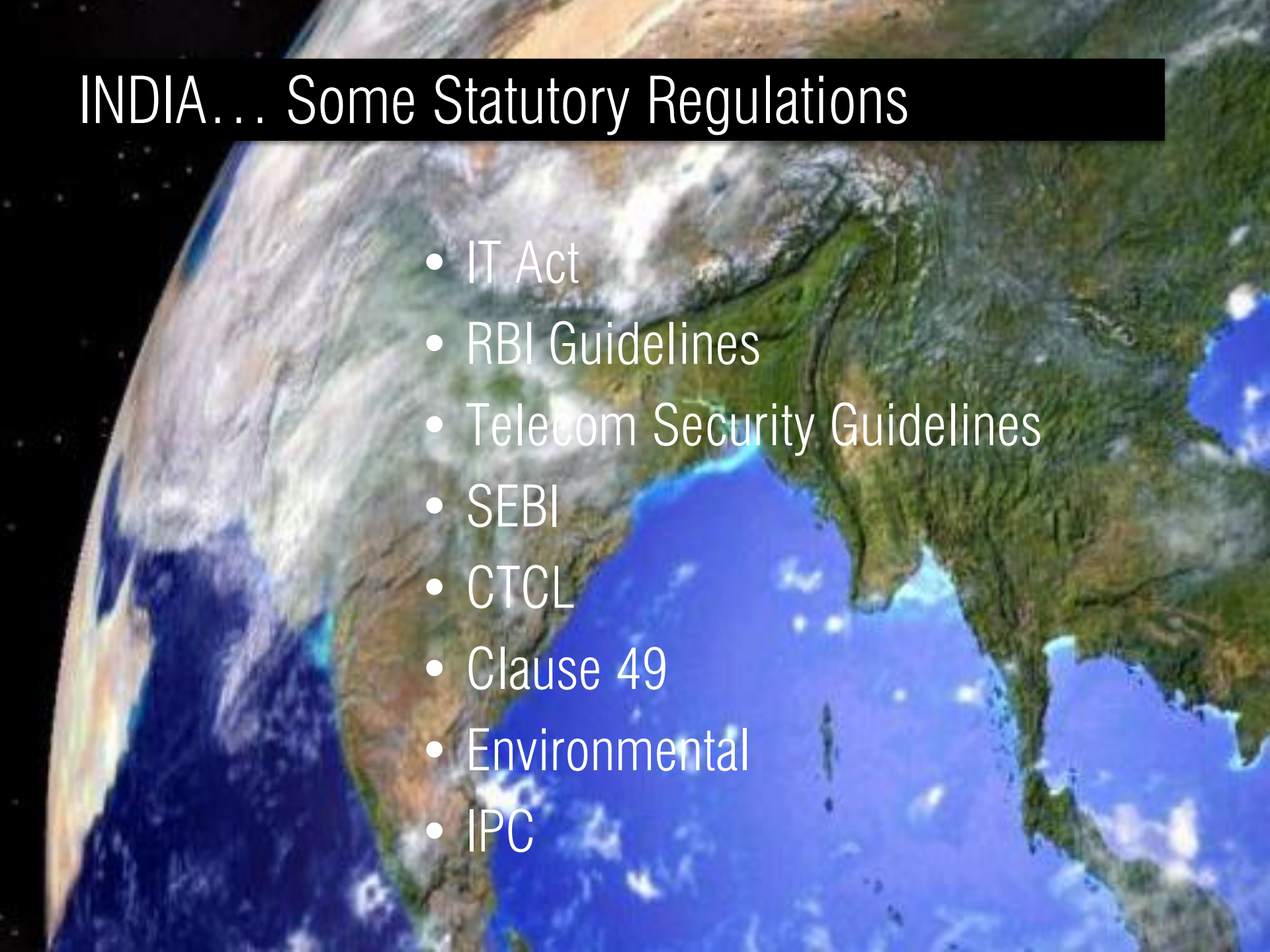
Information Security Related…

Some Laws / Statutory Regulations

- **Health Insurance Portability and Accountability Act (HIPAA) of 1996** - requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- **Gramm-Leach-Bliley Act of 1999 (GLBA)**, also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.
- **Sarbanes-Oxley Act of 2002 (SOX). Section 404** - publicly traded companies assess the effectiveness of their internal controls for financial reporting. CIO responsible for the security, accuracy and the reliability of the systems that manage and report the financial data.
- **Payment Card Industry Data Security Standard (PCI DSS)** - requirements for enhancing payment account data security.
- **Personal Information Protection and Electronics Document Act (PIPEDA)** –protecting personal information that is collected, used or disclosed

Some Laws / Statutory Regulations

- **The Family Educational Rights and Privacy Act (USA** Federal law) privacy of student education records.
- **UK Data Protection Act 1998** - provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.
- **UK Computer Misuse Act 1990** - computer crime (e.g. cracking - sometimes incorrectly referred to as hacking) a criminal offence.
- **EU Data Protection Directive** - adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.
- **EU Data Retention** – ISPs, phone companies keep data on every electronic message sent and phone call made for between six months and two years.



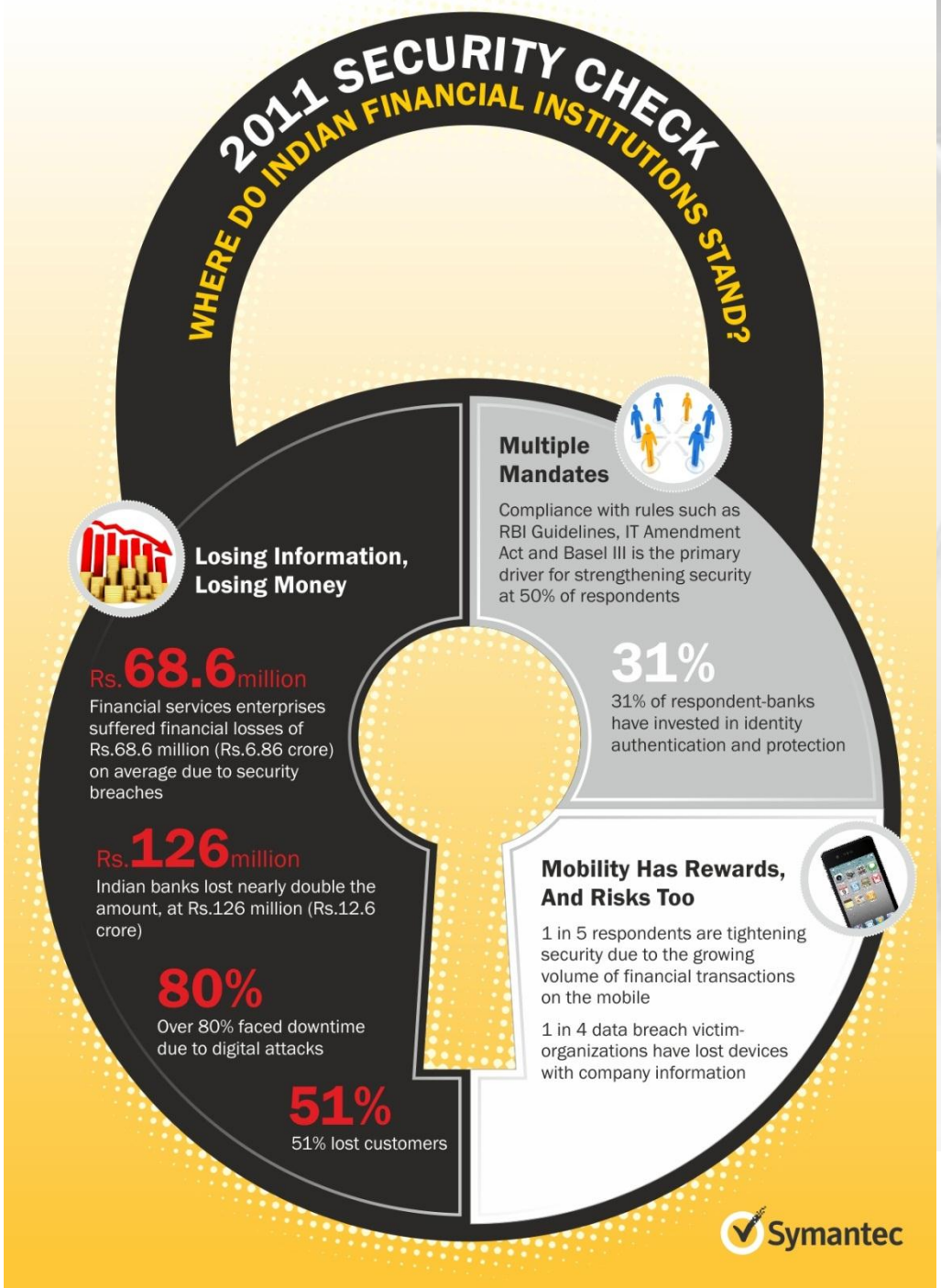
INDIA… Some Statutory Regulations

- IT Act
- RBI Guidelines
- Telecom Security Guidelines
- SEBI
- CTCL
- Clause 49
- Environmental
- IPC

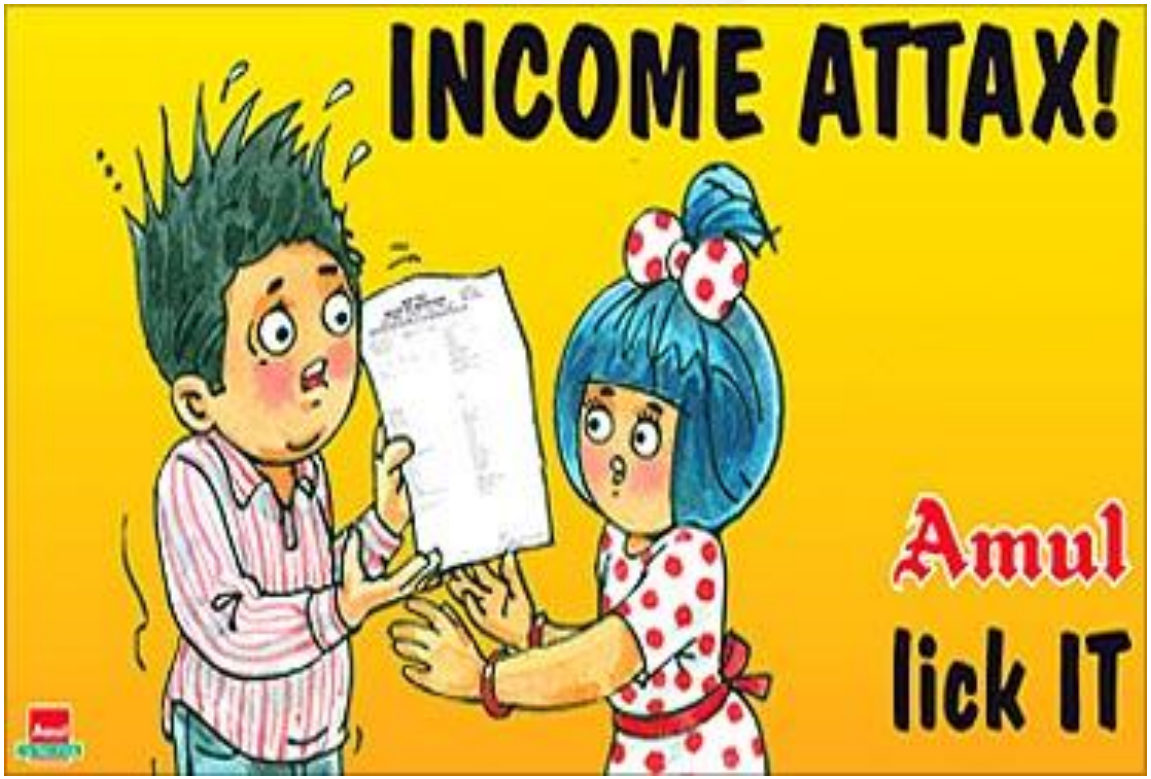
ATTACKS ARE COSTLY

- **23%** **experienced external attacks** (phishing attempts, IP theft, DoS attacks).
- **67%** experiencing a data breach **lost man hours**
- **61%** **lost customers** as a result
- **80%** **faced downtime** due to online attacks
- **Rs 6.86 crore** avg losses due to security breaches at Financial services
- **Rs 12.6 crore** avg losses at Indian banks
- External theft of confidential information was faced an average of 1.5 times
- Internal theft of information an average of 5.8 times.
- 4 hours (average) to resume normal operations

- 51% financial services enterprises in India cited compliance as the primary driver for adopting IT security.
- 25% respondents that experienced a digital attack faced monetary penalization.



The Consequences of Non-Compliance



Dept of Telecommunication

Rs 50cr for a security breach due to inadequacies

Liability of criminal proceedings under Indian Telegraph Act, IT Act, IPC, CrPC

License cancellation

Cost of Non Compliance

- 2010 … Example – Encryption (Ponemon Institute's annual "U.S. Enterprise Encryption Trends Report" - 964 IT and business leaders surveyed)
- In the past, protecting data and mitigating data breaches drove encryption adoption.
- Now regulatory compliance became the top reason for implementing encryption technologies
- 69% compliance is their primary driver for encryption
- 63% mitigating data breaches was the driver for encryption adoption
- The results show the growing realization that compliance is important as companies try to avoid post-breach legal noncompliance penalties.

Business Benefits for InfoSec Vendors

Over the last year, RBI has mandated two factor authentication at banks for all delivery channels.

- In the past 12 months…
  - 31% of respondent-banks invested in identity management
  - Investment in technologies to address such regulations is likely to continue.
- Survey finding..
  - Technology investments during the next financial year will be made towards stronger governance, business continuity planning, securing mobile and wireless transactions, data loss prevention and network security.

RBI Security Guidelines Framework

NINE areas identified from the use of IT in Banking

Recommendations of the "Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds"

Conduct current state Gap Analysis

Plan for remediation and compliance

Implement basic framework by Oct 31, 2011 and rest within a period of one year

Report management oversight and review in bank Annual Report from 2011-12 onwards

Continuously improve controls based on emerging risks and concerns

Requirements & GIC Solution

Policies and procedures	Vulnerability Assessment
Risk Assessment	Establishing on-going security monitoring processes
Inventory , information/data classification	Patch Management:
Defining roles and responsibilities	Change Management
Access Control	Audit trails
Information security and information asset life-cycle	Information security reporting and metrics
Personnel security	Information security and Critical service providers/vendors
Physical security	Network Security
User Training and Awareness	Remote Access:
Incident management	Distributed Denial of service attacks(DDoS/DoS):
Application Control and Security	Implementation of ISO 27001 Information Security Management System
Migration controls	Wireless Security
Implementation of new technologies:	Business Continuity Considerations:
Encryption	Information security assurance
Date Security	General Information Security delive channels

- Develop and maintain security policies ***(Automated Compliance)***
- Generation of meaningful security metrics of security performance ***(Archer)***
- Assignment of roles, responsibilities and accountability for information security ***(Access Manager)***
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures ***(Archer, enVision)***
- Classification and assignment of ownership of information assets ***(DLP)***
- Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security ***(Consulting)***
- Processes to monitor security incidents ***(SIEM)***
- Effective identity and access management processes ***(Access Manager)***
- IS awareness program for users/officials

(2) Information Security

PROJECT

GRID INFOCOM YOUR ADVANTAGE

Telecom Security …

23.7(i) Security Responsibility

HIGHLIGHTS OF AMENDMENT TO NLD LICENSE AGREEMENT DATED 31 MAY 2011

23.7(i) Security Responsibility
- Complete and Total Responsibility for Security of Networks under which the following must be done – Network Forensics, Network Hardening, Network PT, Risk Assessment

23.7(ii) Security Audit
- Conduct a network security audit once a year by network audit certification agency, as per ISO15408 and ISO27001

23.7(iii) Security Testing
- Network elements must be tested as per defined standards – IT and IT related against ISO15048, ISMS against ISO27001; Telecom elements against 3GPP 3GPP2 security standards. Up to 31 Mar 2013 this can be done overseas and after this date in India

23.7(iv) Security Configuration
- Include all security features, as per standards, while procuring equipment and implement the same.
- Maintain list of all features while equipment is in use
- List is subject to inspection by Licensing Authority

23.7(v) Security Personnel
- CISO, System Administrators, Nodal Executives for handling NLD/ILD switches, central database, softswitches … all must be Indian Nationals.

CTCL Audit – shall broadly cover…

- Existing features and system parameters implemented in the trading system.
- Identify the adequacy of input, processing and output controls
- Identify the adequacy of the application security so that it commensurate to the size and nature of application.
- Event logging and system monitoring.
- User management.
- Password policy/standards
- Test of adherence to policies
- Network management and controls
- Change management and version controls.
- Backup systems and procedures
- Business continuity and disaster recovery plan
- Documentation for system processes
- Security features such as access control network firewalls and virus protection measures.
- Any other area/aspect which may be material for inclusion in the audit certificate and/or which may be specified by the Exchange from time to time.

ISO270001


Security Policy
Organization of Information Security
Asset Management
Human Resource Security
Physical and Environment Security
Communicati on and Operations Management
Access Control
Information Systems Acquisition Development Maintenance
Information Security Incident Managament

Bottom Line …. On Compliance

To Be Or Not To Be.

Should Compliance be the end goal or the catalyst of Information Security initiatives – in conclusion, we look at the options and issues.

Same Message Another Source!

There is a rider !

Compliance is one of the biggest drivers of information security initiatives.

However, despite the findings, industry observers believe that compliance efforts aren't necessarily making organizations more secure..

TechTarget survey of U.K. information security professionals

Corporate intellectual property comprises 62% of a company's data assets, but security programs are focused on compliance rather than data protection (CNET)

This confuses the argument further

Strategy – Compliance / Security

- Compliance is NOT Security
- Security is NOT Compliance

- Organizations must drive Compliance and NOT be driven by Compliance
- Information Security to leverage Compliance FUD to get Management attention
- Compliance provides good ROI numbers for reporting

Strategy – Compliance / Security

- Security requires organizations to step up to extract benefits from both C and S initiatives
- Build maturity, through awareness programs, among stakeholders to recognize and support intangible benefits
- Identify and enforce C >< S balance through practical controls and measures

Remember

Compliance ≠ Security

Security ≠ Compliance

Thank You

E: dinesh@opensecurityalliance.org
E: dineshobareja@gmail.com
M: 9769890505

INDIAN Honeynet PROJECT

COCON

GRID INFOCOM YOUR ADVANTAGE

References and Credits

- CSO Online
- Purpleslog on flickr
- Internet Crime Complaint Center
- flickr.com/GDS Infographics
- freedigitalphotos.net/digitalart
- Google Uncle !