

DSCI Framework, Best Practices

Vinayak Godse
Sr. Manager- Security Practices, DSCI

IBA-DSCI Security Conference
Mumbai, April 26, 2010

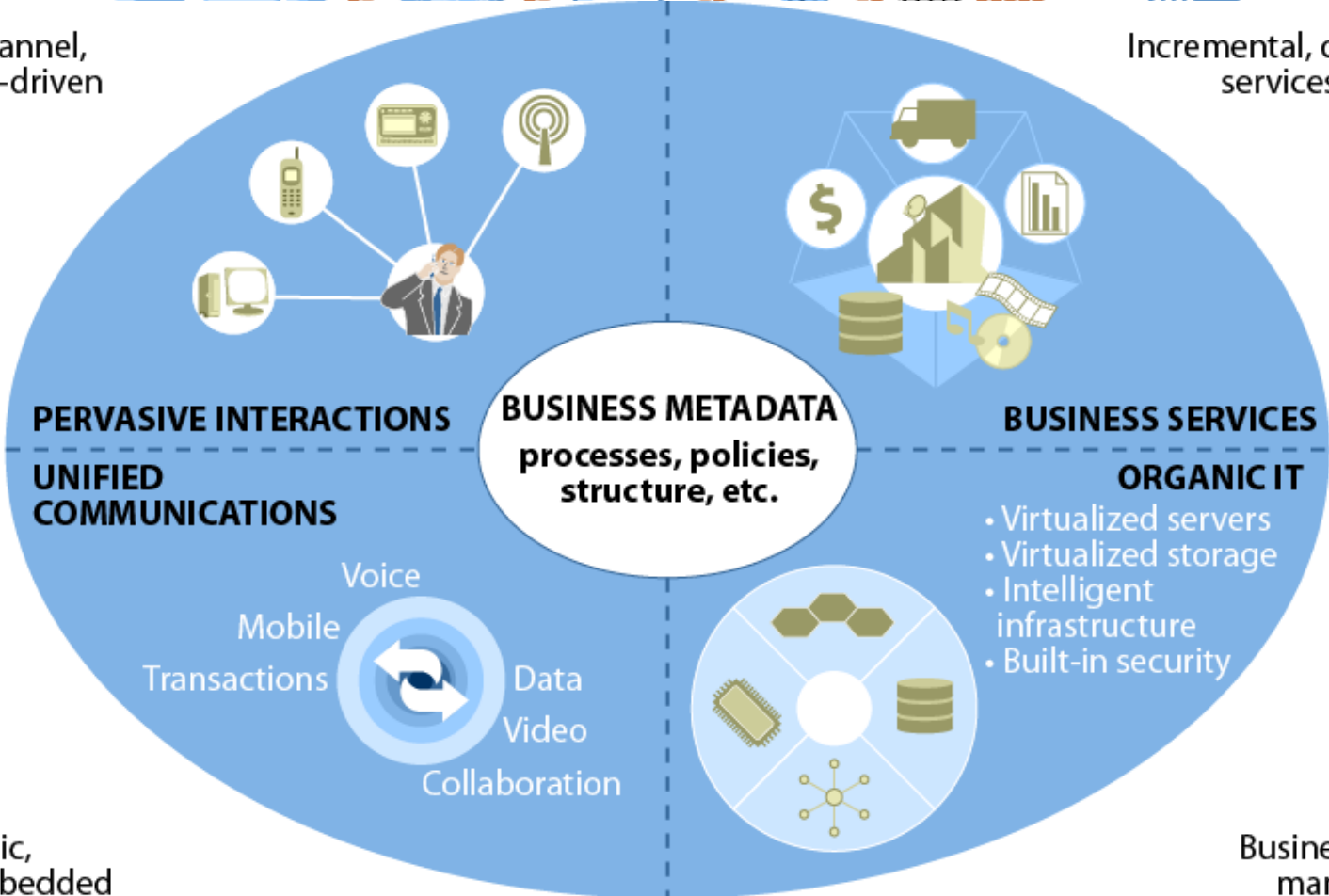
Technology is transforming of Banking Industry



Internet

Multichannel, context-driven

Incremental, composite services and data



IP-centric, app embedded

Business service management

Forrester: The Next-Generation Banking Platform



Data Security is an Universal Concern

Wednesday, August 6, 2008

THE WALL STREET JOURNAL. BUSINESS

Asia Edition | Today's Paper

Home | World | Business | Markets | Market Data | Tech | Life & Style | Opinion

Family Finances | Investing | Retirement Planning | Taxes | Crunchonor

1 of 10

TOP STORIES IN Personal Finance

Too Late To Jump Back Into Stocks? | Insurers Raise Premiums on Term Life

LEADER (U.S.) | AUGUST 6, 2008

U.S. Indict

Article

Email | Printer Friendly

By JOSEPH PEREIRA, BOSTON -- Federal prosecution that stole more than 100 million credit cards from Cos., Barnes & Noble Inc.

The case is the biggest data breach in U.S. history and San Diego on Tuesday. The scheme involving wireless devices stole card numbers as they passed through less than \$1 apiece on the digital plunder in Latvia.

APRIL 14, 2005

Security Breach Hits Credit Cards

HSBC Notifies 180,000 People Who Shopped at Ralph Lauren; Other Banks May Be Affected

Article | Comments

Email | Printer Friendly | Share: Yahoo Buzz | Save This | Text

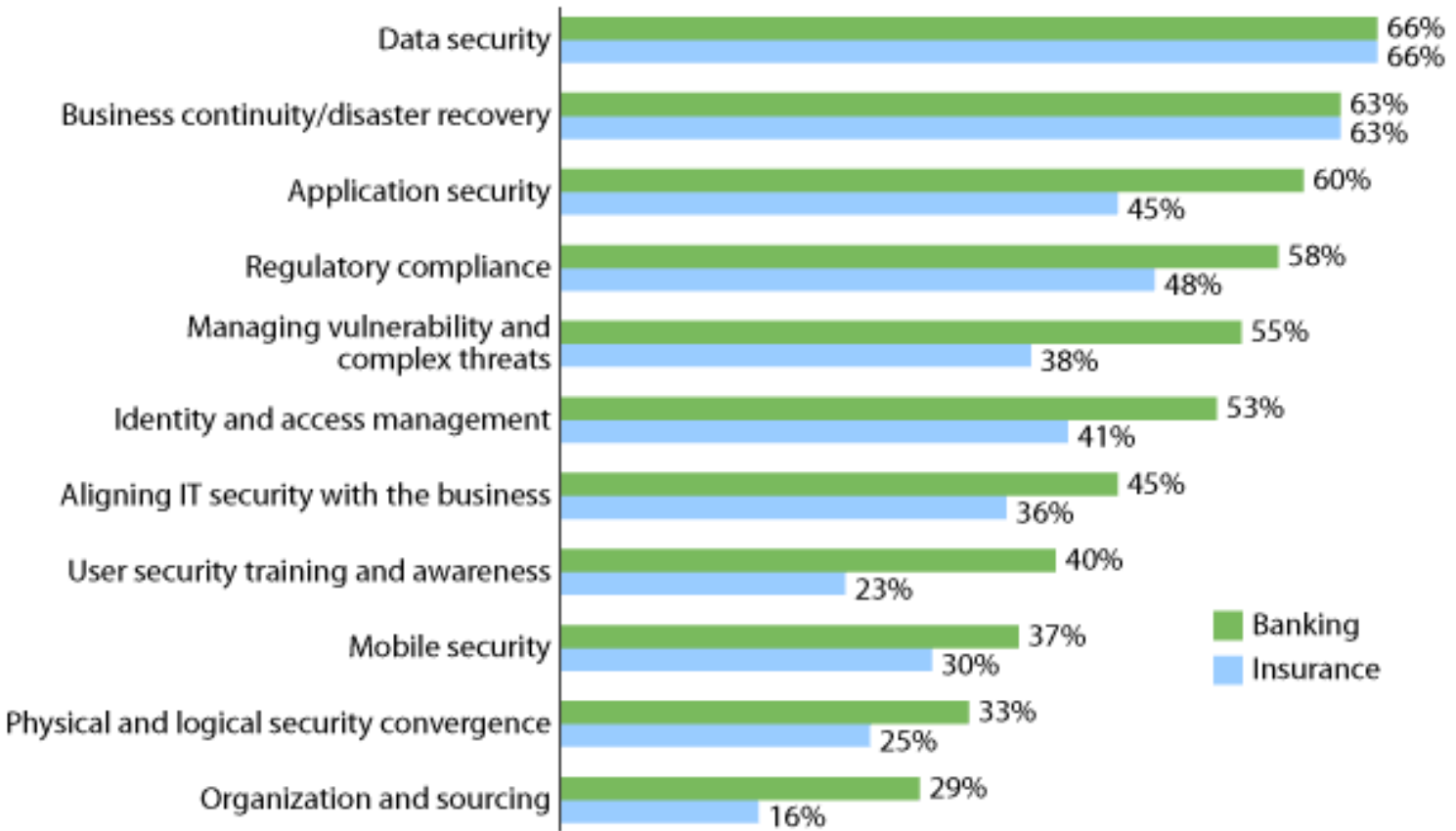
By ROBIN SIDEL and CHRISTOPHER CONKEY | Staff Reporters of THE WALL STREET JOURNAL

British financial giant HSBC PLC is notifying at least 180,000 people who used MasterCard credit cards to make purchases at Polo Ralph Lauren Corp. that criminals may have obtained access to their credit-card information, and that they should replace their cards.

The situation -- which involves a General Motors-branded MasterCard that is one of the most widely held credit cards in the U.S. -- is the latest in a string of high-profile incidents in which

Data Security- Most important issue in Banking

“How important to your IT security organization will each of the following issues be in the next 12 months?”



Base: 73 banking and 64 insurance North American IT security executives (percentages shown are “very important” responses)

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008

46632

Source: Forrester Research, Inc.

Data Protection Regulations: Rising Liability

UK- maximum **“fine of £500,000”** for **“serious breaches”** of the DPA 1998

UK- FSA proposed to enforce **“penalties of up to 20% of firms income”**

USA- New California law-to impose fine of up to **“\$50,000 per breach”**

France- Amendment to the French DPA, companies **“more 50 employees to appoint CPO “**

Fine

Technical & Organizational Measures

Data transfer

Legal Relationship

Regulatory Infrastructure

Liability - Data Controller and Processor

Data Breach notification

Third party Contract Norms

IT (Amendment) Act, 2008- Body Corporates are liable to the extent of **“Unlimited Liability”** for failure to implement ‘reasonable security practices’ to protection ‘sensitive personal information’

How complex is Security? Functions, organization, technology, operations.....

Geographical locations
 No of locations
 Geographical patterns
 Ownership patterns
 Physical characteristics
 Travel
 HR & Admin
 Key officials
 Connectivity Options
 Project Concentrations
 Application supported
 Process executed
 Services offered

Security Management
 ISO 27001 support processes
 Standards & Processes
 Risk Assessment
 Audit Management
 Continuity Management

Network
 Client owned
 Organization Owned
 Network Diagram

Security Operations
 AV update
 Patch Mgmt
 VA/PT
 Monitoring
 User Management
 Recovery support



Security in HR Processes
 List of actions while recruitment
 Background check, Document verification
 List of actions while joining
 NDA , Ethical Code
 Induction training
 List of actions in case of security breach
 Scenarios for Warning
 Scenarios for punishment
 Scenarios for expulsion
 List of actions while exit
 Exit agreement

Awareness & Training
 Type of training
 Training schedule

Projects /Processes / Services
 Portfolio of projects / processes
 Criticality of project / process
 Security Rating of project / process
 List of Data Exposures

Security Challenges
 Employees underestimating importance of security
 Remote access, mobile computing
 Insecure client applications
 Wireless networking
 Lack of visibility
 Policies are not addressing real threats
 Budget not adequate

Security Organization
 organization structure
 Tactical & operational roles
 Relationship with other divisions
 Reporting structure
 Central structure
 Reporting mechanism

Physical Security
 Organization structure
 Physical security roles
 Security Architecture
 List of technology used
 Processes deployed
 Alert mechanisms
 Security zones

Data Leakage Scenarios
 Data Flow Diagram
 Threat Modelling
 Inventory of scenarios

Security Technology
 Security Architecture
 List of technology deployed
 Perimeter security
 Network Access control
 Detection & Prevention
 Malware protection
 Channel Encryption
 Data Encryption
 Content Monitoring & Filtering
 Application Access control
 Resiliency measures

Incident Management
 Detection requirements
 Investigative requirements
 Logging and monitoring architecture
 Incident reporting mechanism
 Incident Metrics
 Reporting

Compliance Management
 Compliance exposure:
 PCI-DSS, HIPAA, IT Act,
 List of compliance requirements
 Compliance support processes
 Compliance operations
 Compliance reporting
 Compliance artefacts

Transaction Security: Aggravated challenges

“Service is temporarily unavailable”: ***Trojan-based, man-in-the-browser attacks are circumventing strong two-factor authentication.***

Malware sitting inside a user's browser and waits for the user to log into a bank. It copies the user's ID, password and OTP, sends them to the attacker telling the user that the service is "temporarily unavailable."

“**Attacker overwrites user transaction**”: overwrite happens behind the scenes so that the user does not see the revised transaction values

Fraudsters have been “**raiding user bank accounts**” that are protected by protected by strong two-factor authentication,

“**Out-of-band authentication**” using voice telephony is “**also being circumvented**” by fraudsters using call forwarding

What you require?

‘**Visibility**’ over data, current initiatives, activities

‘**Vigilance**’ over recent issues, trends & approaches

‘**Coverage & Accuracy**’ of security initiatives & programs

Focus on ‘**strategic, tactical & operational**’ layers

Tactical mechanisms for the ‘**discipline in defense**’



‘**Compliance demonstration**’ from security initiatives

Because Specifics become important now

Do you have **complete visibility** over how this data comes to you? **What data** are you securing? **Which process?** Which **function?** **How** are you **accessing?**

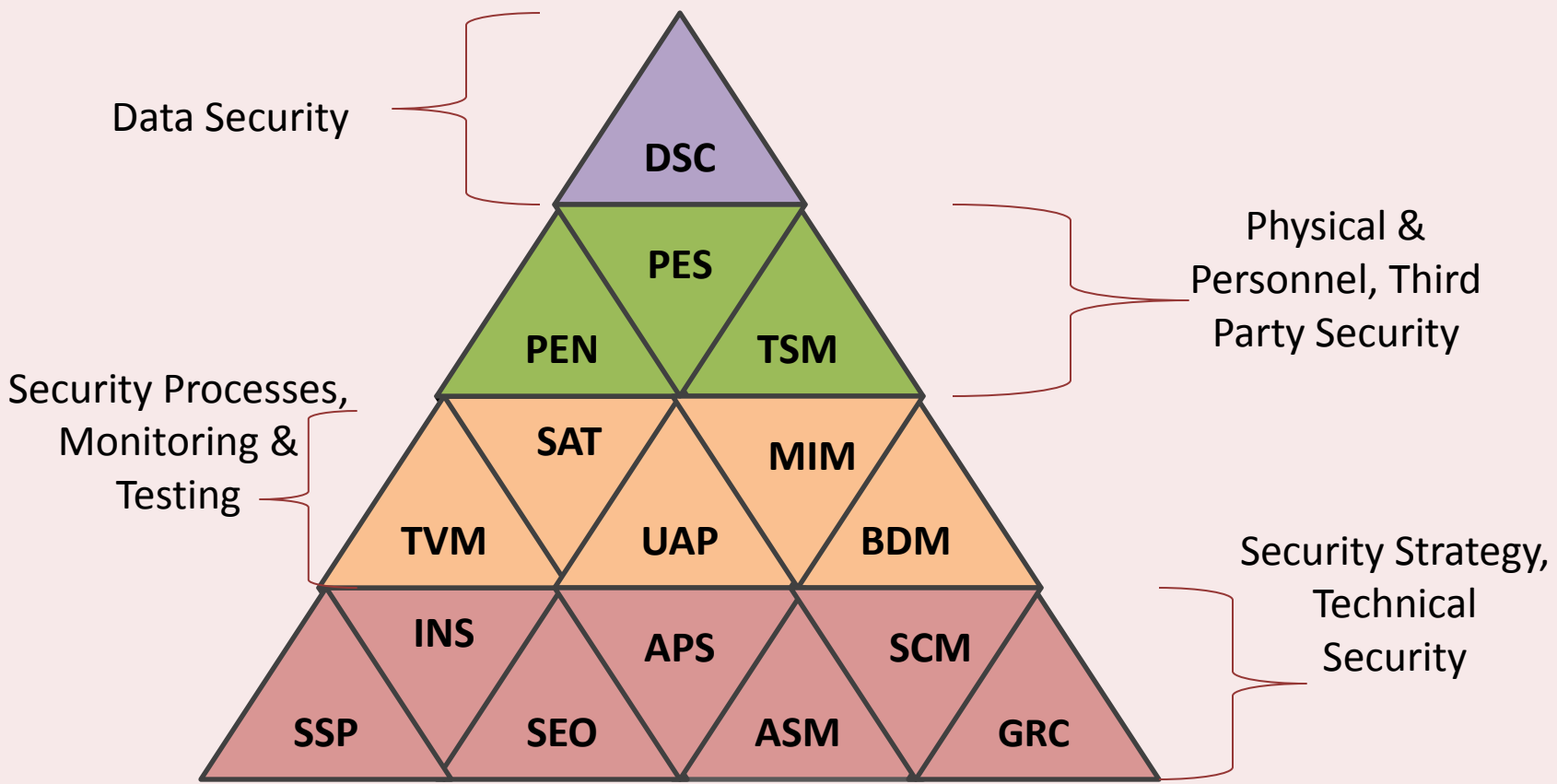
Do you know sensitivity of “**the data element**”? Client perception? Client customer perception? Specific law that makes you liable? Contract provisions? Can you **demonstrate** your preparedness?

Do you know who is **accessing** the data? how it is **processed** at your end? How are you **transmitting, storing & processing?**

Does your **security program covers** that data element? How are you securing it? Is the security adequate & **accurate?**

Are you **aware of scenarios** that lead to leakage? Are you aware **of trends** that affect security of the data? Have you checked their **relevance** for the specific data? What if any breach happens?

DSCI Data Security Framework



SSP – Security Strategy & Policy	SEO – Security Organization	ASM – Asset Management	GRC – Governance, Risk & Compliance
INS – Infrastructure Security	APS – Application Security	SCM – Security Content Management	TVM – Threat & Vulnerability Management
UAP – User, Access & Privilege Management	BDM – Business Continuity & Disaster Management	SAT – Security Audit & Testing	MIM – Monitoring & Incident Management
PEN – Physical & Environmental Security	TSM – Third Party Security Management	PES – Personnel Security	DSC – Data Security

Best Practices



Technology Business Resiliency Business Alignment Security Crisis Management
Log Management Security Function Strategy for Modular approach Incident Management

Strategy for Physical Security Inventory of business processes A catalog of all of BDM elements
Dedicated function for APS Visibility over all access points x access control measures
Operational processes structure Inventory of log information
Roles & responsibilities APS system Inventory of physical assets systems
Consolidated log collection source dependency mapping with IT
function Enterprise application portfolio

Resiliency at application layer Centralized visibility exists over Responsibility of associated
Centralized visibility exists over Enterprise application portfolio
Responsibility of associated Criticality of each application
Classification of key architectures Enterprise program requirements
functions & LOBs LOBs involvement Facility is restriction
parameters Lines of Business (LOBs) Roles & responsibilities function

Major physical security solutions Standards & Guidelines
Standards & Guidelines Mechanism exists to identify, authenticate & authorize
Centralized logging archival, Log management architecture Tools for change management
Resources and efforts for APS requirements Integration with user life cycle management
retention, disposal regulatory visibility significant incident Mgmt ESPs
Continuity Plan An inventory of all BDM BDM Strategy vehicle entry & exit
Availability of logging platform can't visibility over application BDM Operations report

Protection at Application layer Incident management (IM) & reliability incident response
defined & documented Security ratings to all elements
Log management plan scenario based requirements applications Detect Manage
visibility over current protection integration of IM with log mgmt
level security Application x security architecture BDM as an ongoing

Review & analysis of logs ship with Catalogue of security inventory of instances analysis & security vulnerabilities
Flow analysis, threat modeling A catalog of recovery services APS testing requirements
Threat analysis of facilities MIM Strategic road security authorization of physical intrusion management
Security Intelligence Reporting of BDM function for physical intrusion management
Focusing on risk, proportionate resources, efforts and skills for remediation

Security Intelligence Extension of BDM program coverage A catalog of testing services
Reasonable configuration for PEN MIM Physical security incident management
Knowledge mgmt- threats, new Strategic roadmap tools, services, Program to build skills
Integration with cyber security with skills BDM Oversight, Collaboration- Coordination
malware outbreaks, new vuln. A BDM Oversight, Collaboration- Coordination
operations with incident response for emerging threats

Historical information about Continuity plan A Roles- Strategic, tactical, operational, Knowledge mgmt
incidents Collaboration for physical security IM - Knowledge mgmt
Responsibilities of (LOB) units Coordination with local & law enforcement agencies
& support functions results management



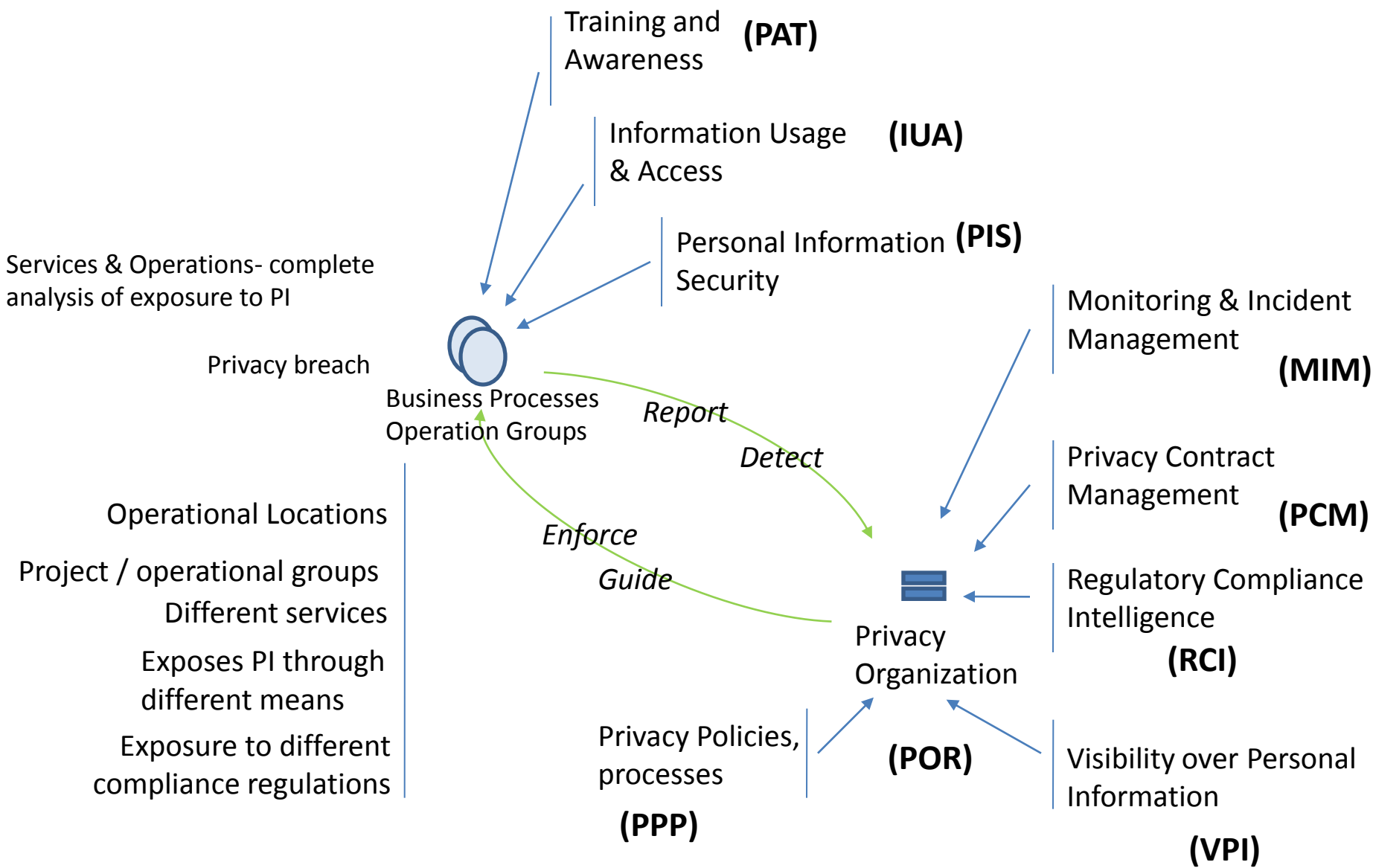
Why Privacy treated separately from Security?

- **“Data protection regulations”** focus on privacy initiative, and demand separate function for Privacy Initiatives. E.g. CNIL, France Data Protection Act asks appointment of CPO
- **“Privacy Compliance”**, resides with Legal department of organization; they like to see privacy as a different activity, or a function
- **“Service Providers”**, increasingly exposed to privacy regulations of client geographies
- **“Privacy preparedness”** seems lagging to security, needs special emphasis, & increased awareness

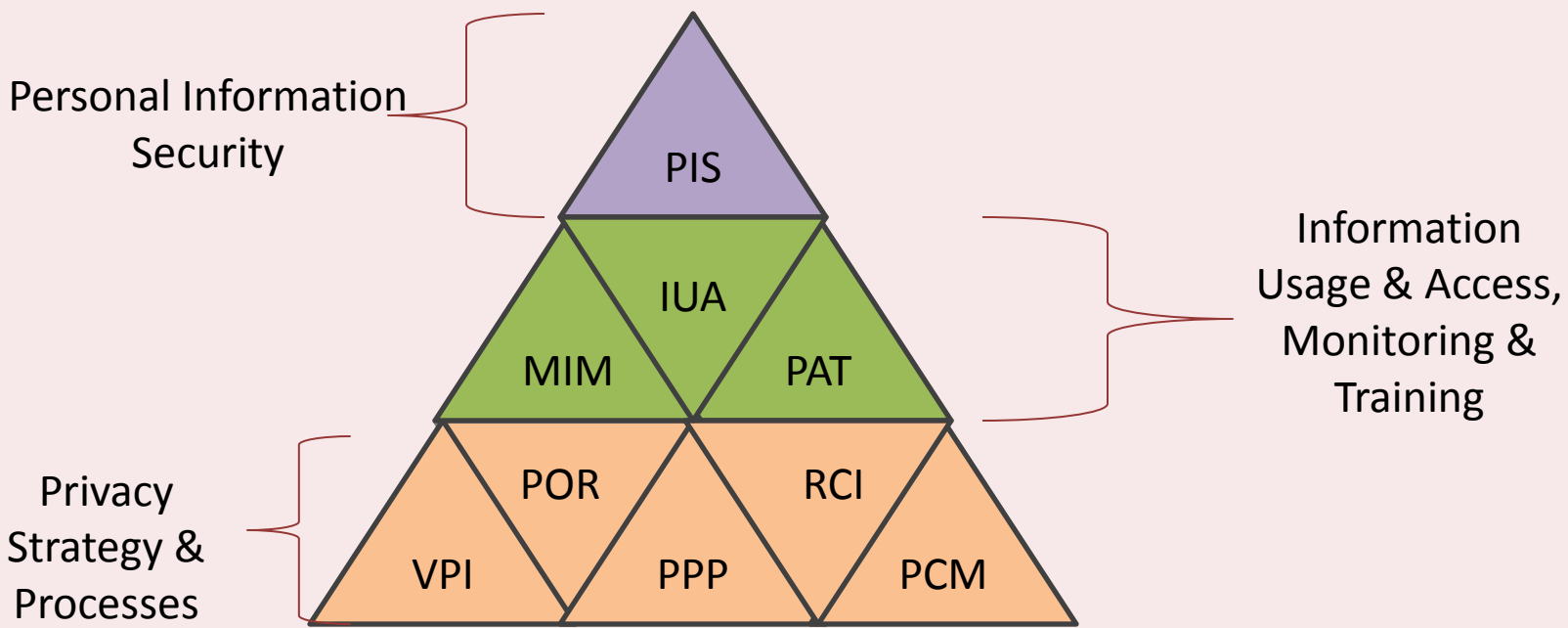
Mapping of privacy requirements across the globe

			APEC Framework	OECD Guidelines	US Privacy Act 1974	EU Data Protection	Australia ANPP	JPIPA	Canada PIPEDA	HIPAA
Privacy Requirements	1	Accountability	Organization's accountability towards personal information	✓	✓		✓		✓	
	2	Notice	Notice in clear language for collection, policy notification	✓	✓	✓	✓	✓	✓	✓
	3	Consent	For collection and use	✓	✓	✓	✓	✓	✓	✓
	4	Collection Limitation	Restricting the collection to the identified purpose only	✓	✓	✓	✓	✓	✓	
	5	Use Limitation	Restricting the use for the stated purpose only	✓	✓	✓	✓	✓	✓	✓
	6	Disclosures	Terms to disclosure to third parties & any other reason	✓		✓		✓	✓	✓
	7	Access & Corrections	Individual's access to his info Individual's right to update/correct his info	✓	✓	✓	✓	✓	✓	✓
	8	Security/Safeguards	To prevent loss, misuse, unauthorized access, disclosure, alteration & destruction	✓	✓	✓	✓	✓	✓	✓
	9	Data Quality	To ensure info is accurate, complete & up-to-date	✓	✓	✓	✓	✓	✓	
	10	Enforcement	Assurance over adherence to privacy policies & Complaint resolution	✓			✓		✓	✓
	11	Openness	Policies clearly published & available	✓	✓	✓	✓	✓	✓	✓
Additional Requirements	12	Anonymity	De-identification of personal information					✓		
	13	Transborder data flow	Personal data transfer across geographies	✓	✓		✓			
	14	Sensitivity	Specified inf that requires specific controls				✓			

DSCI Privacy Approach



DPF[©] - DSCI Privacy Framework



DSCI- Privacy Framework

VPI – Visibility Over Personal Information	POR – Privacy Organization & Relations	PPP – Privacy Policy & Processes
RCI – Regulatory Compliance Intelligence	PCM – Privacy Contract Management	MIM – Privacy Monitoring & Incident Management
IUA – Information Usage & Access	PAT – Privacy Awareness & Training	PIS – Personal Information Security

DSCI Framework and Practices

How

- Study emerging compliance regime
- Content aggregation, best practices
- Knowledge collaboration with ‘Gartner’, ‘Forrester’ etc
- Close watch on technology trends
- Focus on the verticals: Banking, Telecom, Manufacturing
- DSCI Steering Committee
- DSCI Chapters
- Content vetting team
- Projects with partners
- Information sharing by security vendors

DSCI Corporate members: 470

DSCI Chapters (800 members)

- Pune
- Mumbai
- Hyderabad
- Kolkata
- Delhi
- Bangalore
- Chennai
- Chandigarh
- Jaipur
- Ahmedabad

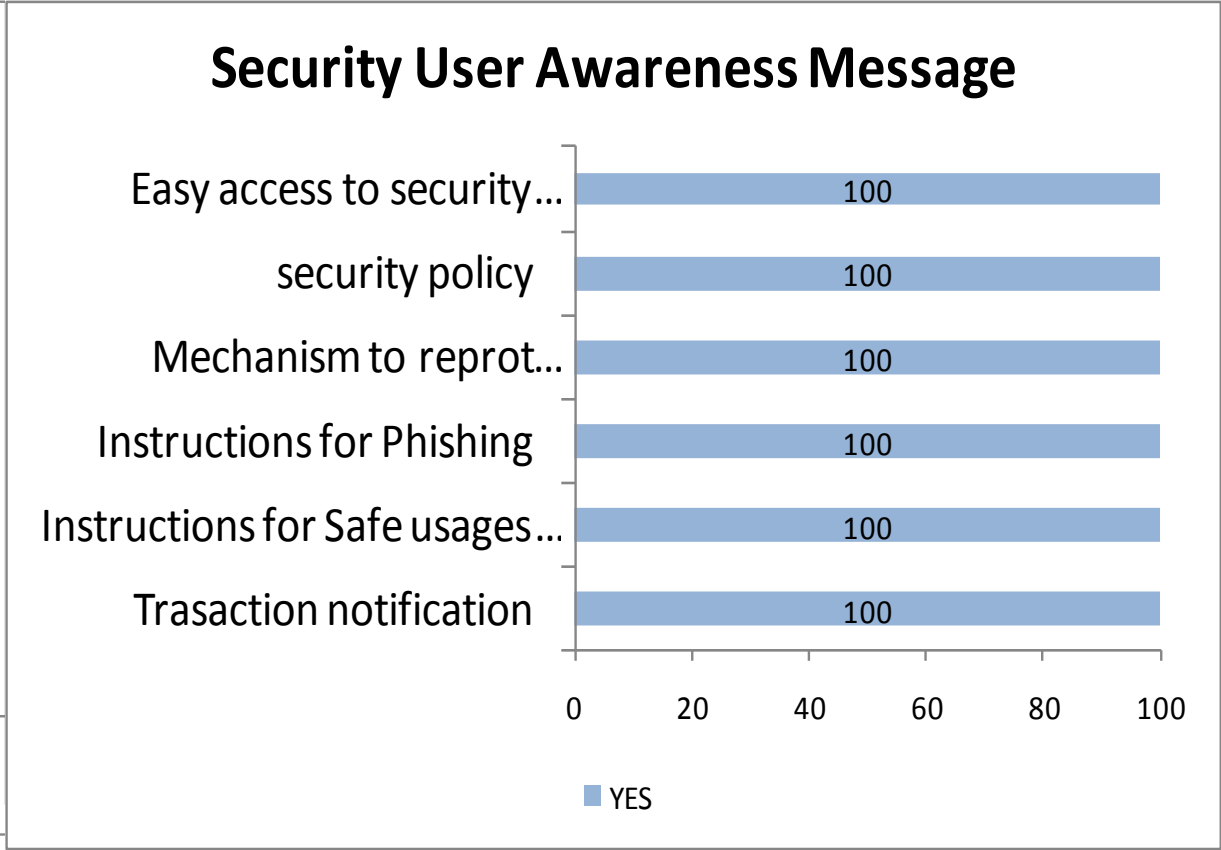
SPs	Infosys, TCS, Wipro, WNS, Tech Mahindra, HCL , IntelinetGlobal, etc
Big4	KPMG, Deloitte, E&Y
MNCs	IBM, HP, Oracle, MS, Intel , Accenture etc
Clients	BT, Wachiova, Metlife, etc
Vendors	RSA, McAfee, Symantec, CA etc
Govt	CERT-IN

Banking Security Survey-Next Step

Objective: State of technology implementation, countermeasures deployed and preparedness against the new age threats

- Public Sector Banks
- Private Banks
- Foreign Banks

- Authentication, Identity mgmt
- Session Security
- Transaction Security
- Fraud Management
- Anti Phishing measures
- Privacy initiatives
- End user education



DSCI Value statements

Connected Endeavour-

— **industry + government + clients + regulatory bodies + knowledge sources**

Continuously Engaged for the cause of data protection

Building Ecosystem for enhanced security and privacy culture

Proactive role for policy enablement that affects ICT

Collaborate with multi-stakeholders and interest groups at national and international forums

Approaches, Frameworks and Practices to align security and privacy practices to recent trends

Repository of knowledge and document ecosystem for the benefit of industry

Thank You