

Offshore Outsourcing : Weighing the Risks of Data Protection and Security

Arjun K. Pai
School of Computer Science
Queen's University Belfast

Subhajit Basu
School of Law
Queen's University Belfast

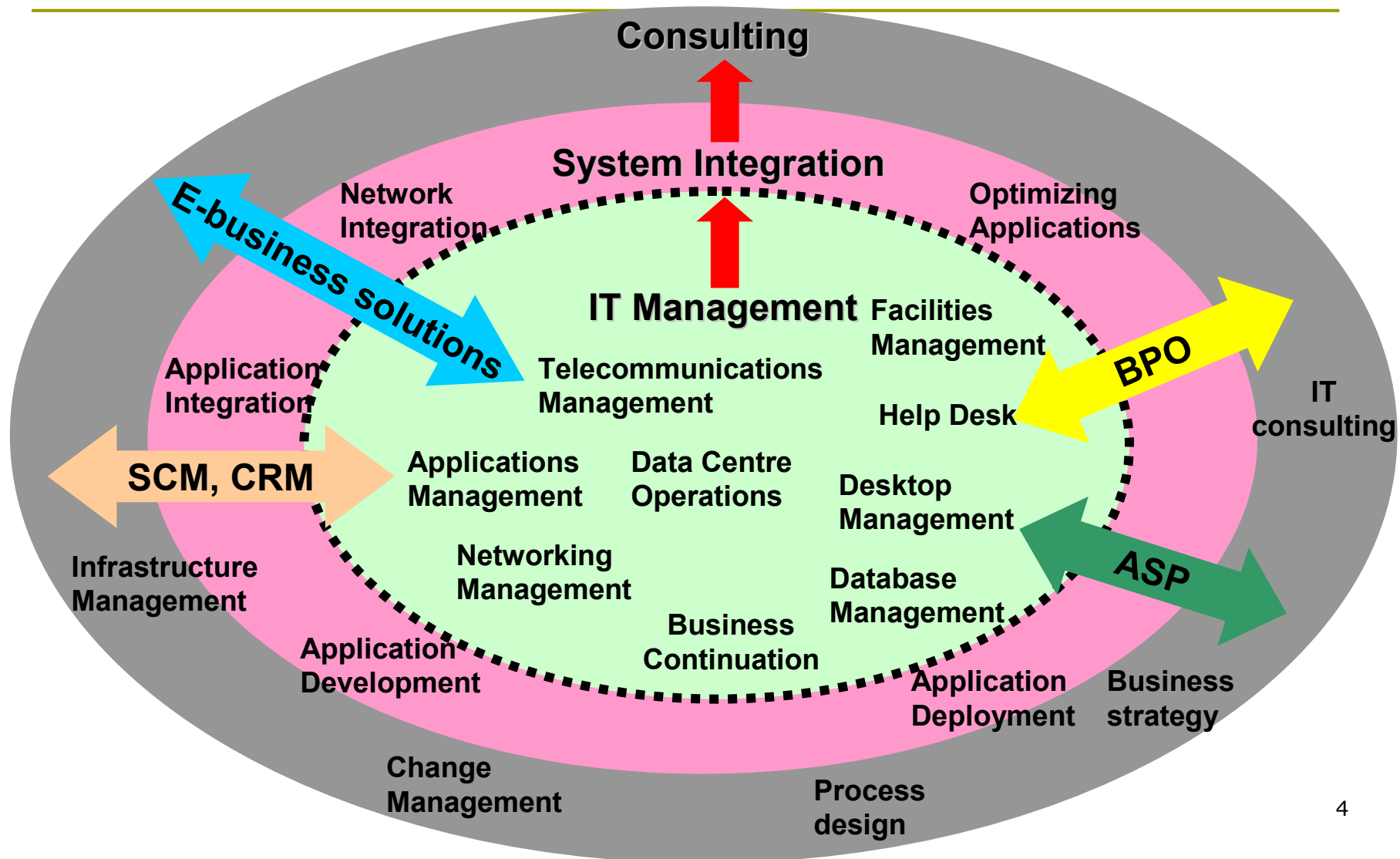
Overview of Outsourcing

- ❑ “Outsourcing is the transfer of internal business processes and capabilities to an external service provider”
- ❑ The basic commercial proposition is that the service provider will do:
 - what the customer currently does
 - at the same or a better level of performance
 - for the same or a lower price
- ❑ Key indicators/drivers of business transformation
 - Highly skilled labour arbitrage
 - Dramatically lower costs

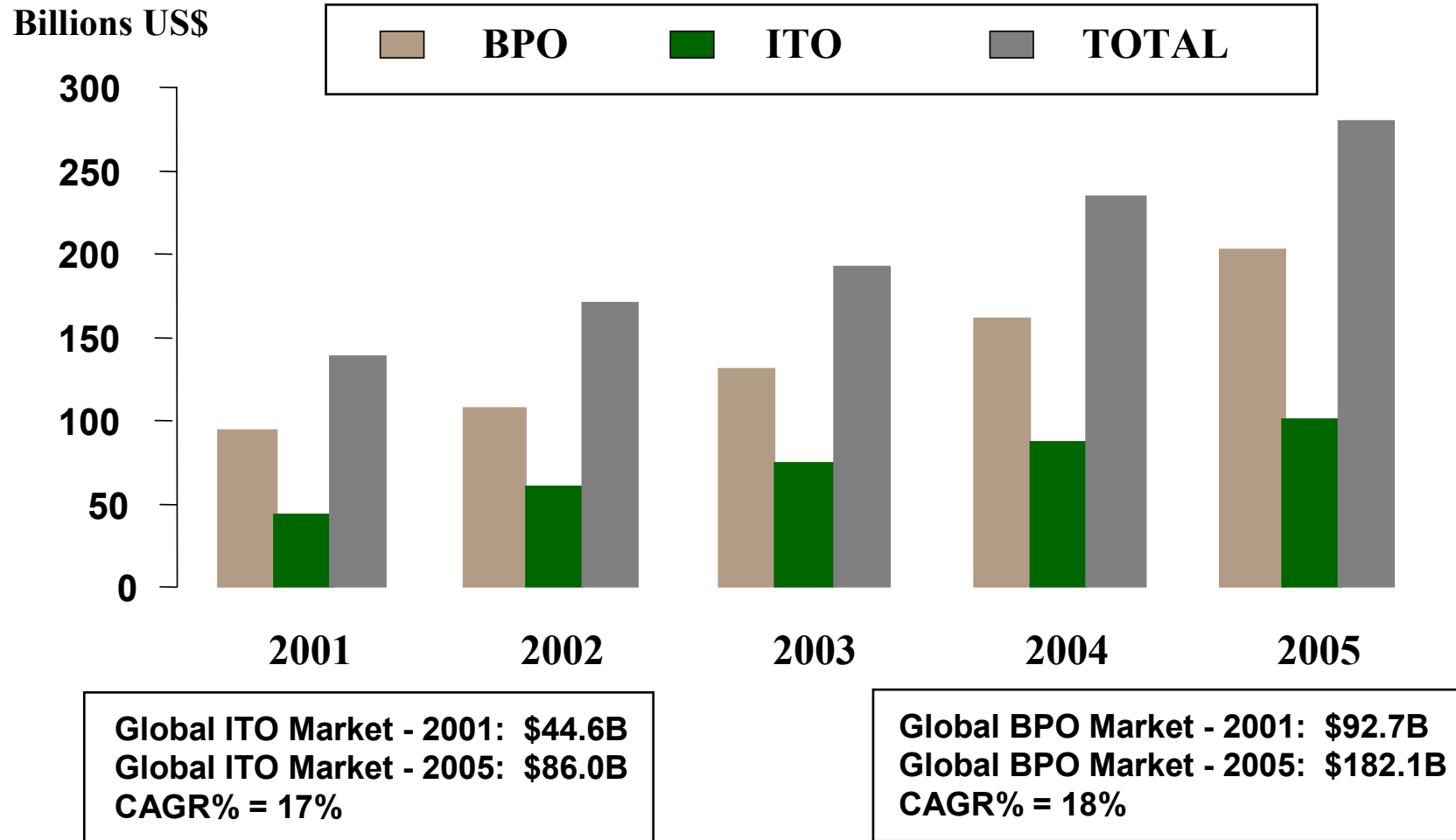
Offshore Outsourcing – The New Paradigm

	Traditional Outsourcing	Transformational Outsourcing
Key motivation for offshore relationship	Cost	Long Term strategic value
Definition of Goals and Objectives	Tactical	Strategic
Management of Relationship/engagements	Activity focussed	Outcome focussed
Vendor Management	Vendors as contractors	Vendors as partners
Management's approach towards offshore program	Disjointed principles	Common principles and goals

Types of Outsourcing : What is being outsourced?



Global Outsourcing Market : Continued Growth



BILETA 2005

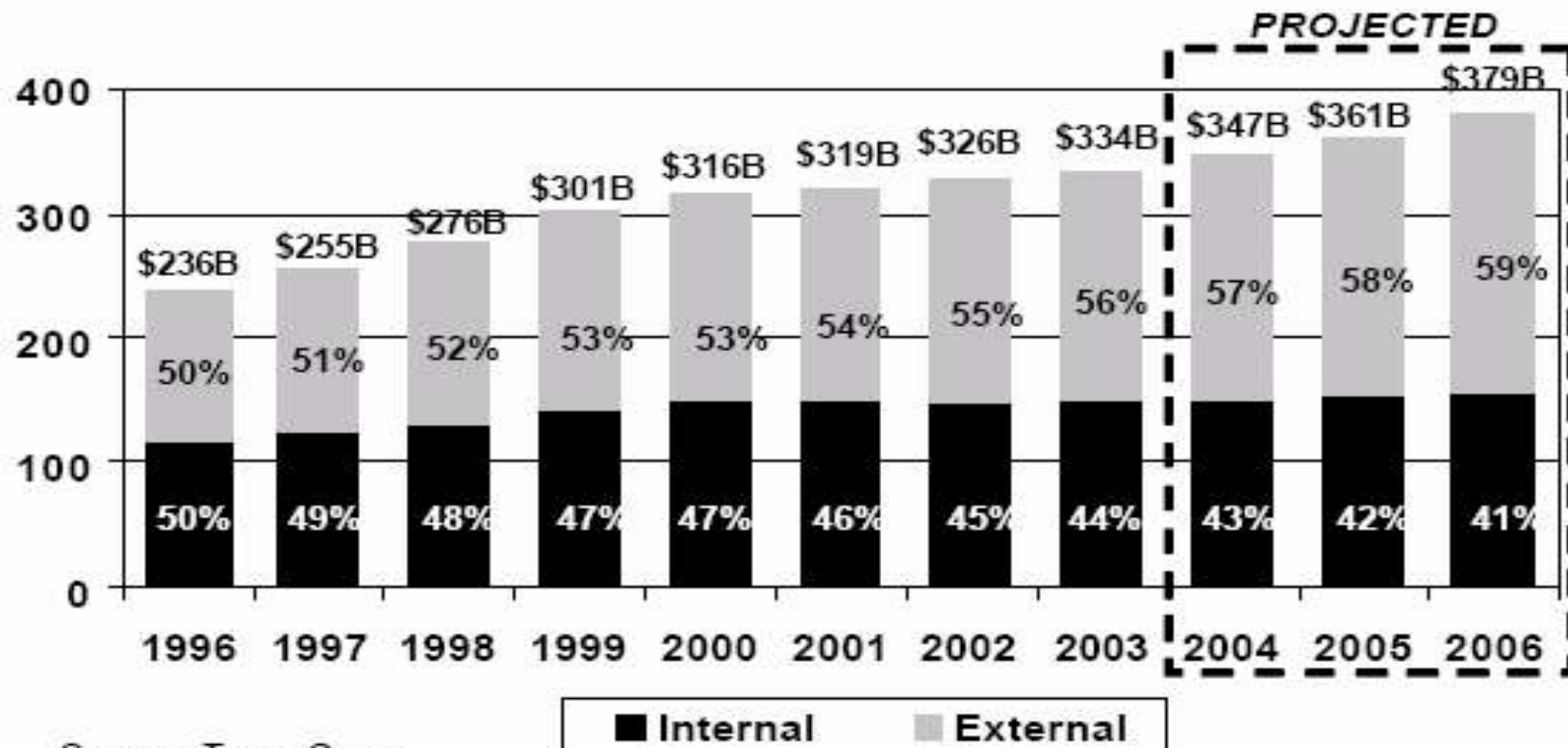
5

Source: Gartner

'Offshored' Global Financial Services: IT Spending

External IT Spending is Rising Rapidly, From 50% of Total IT in 1996 to Nearly 60% in 2006

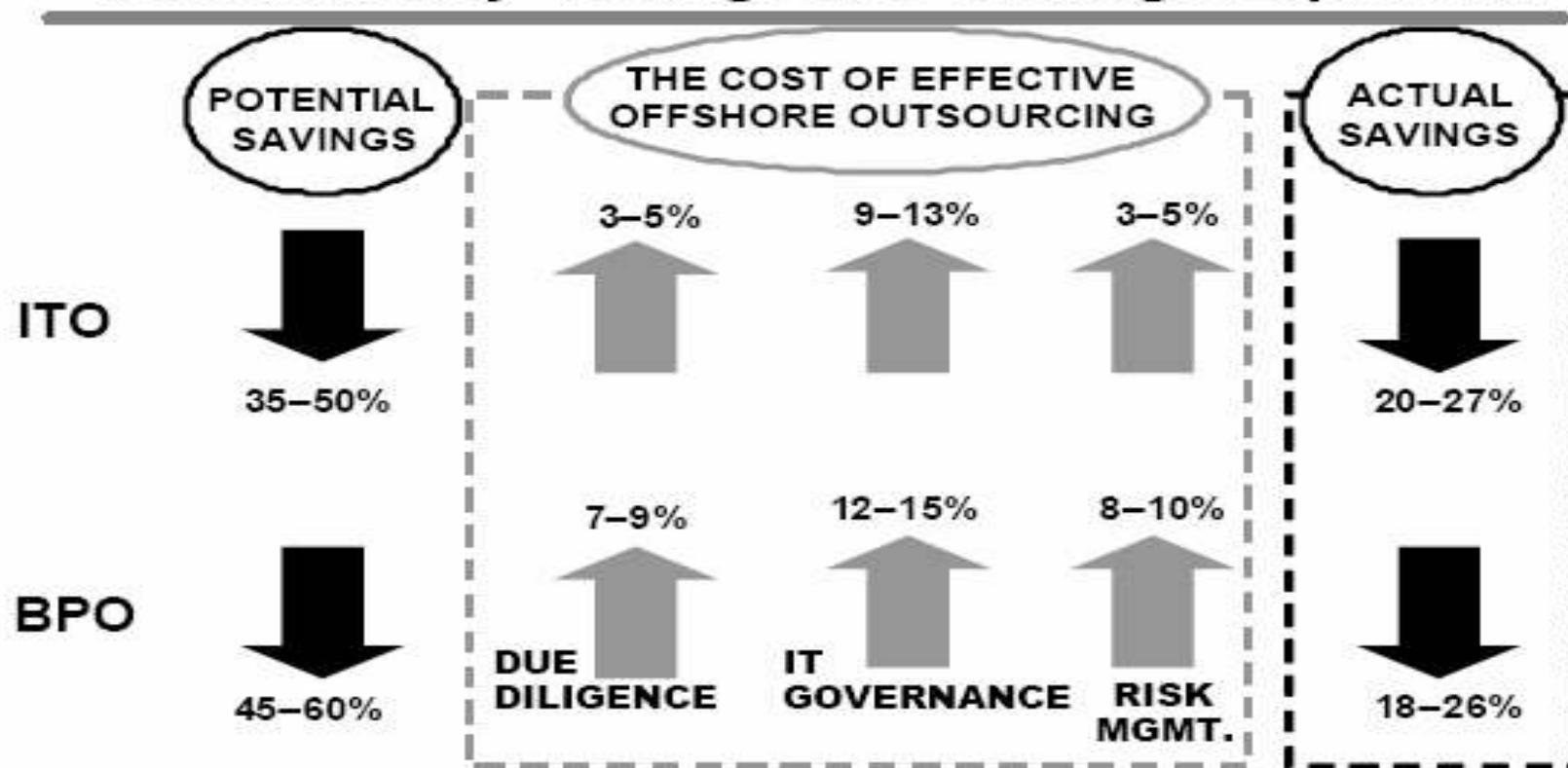
Global FSI IT Spending (in US\$ Billions)



Source: TowerGroup

Reasons for Offshoring

The Costs of Offshore Outsourcing Dramatically Change the Savings Equation



Source: TowerGroup

Step Approach towards Outsourcing Relative Threats

- ❑ Strategic Planning
- ❑ Due Diligence/Assessment
- ❑ Human Resource Strategy
- ❑ Technology Strategy
- ❑ Risk Mitigation Strategy
- ❑ Compliance Issues (HIPAA, Gramm-Leach Bliley)
- ❑ Service Level Agreements
- ❑ Negotiating the Agreement
- ❑ Business Process Management
- ❑ Conflict/ dispute resolution
- ❑ Exit strategy

- Reviewing physical &
- Logical security
- Access, vulnerability
- Internal and external threats

- Technology oriented threats
- Cyber fraud, Phishing
- Authentication
- Risk assessment

- Compliance issues
- Operational/transactional risks
- Legislations and regulations
- Watchdogs of Law

Offshoring Threats

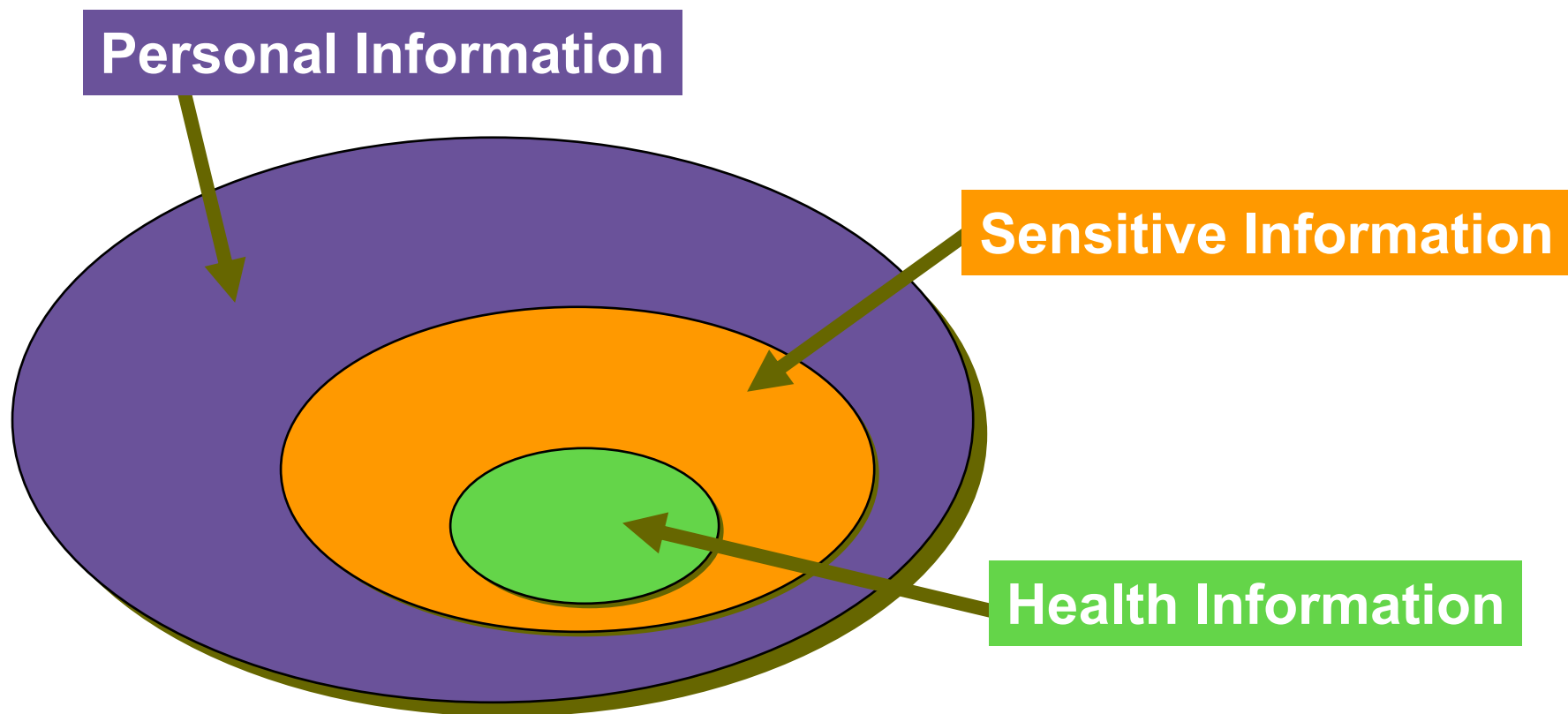
- ❑ Hackers and crackers
- ❑ Industrial/ corporate espionage
- ❑ Trusted Insiders
 - Employees
 - Consultants
- ❑ Organised crime, Phishing, identity thefts
- ❑ Political stability and socio-economic impact
- ❑ Terrorism?



Offshoring Risks

- ❑ Country Risk: political, socio-economic, or other factors may amplify any of the traditional threats
- ❑ Outsourcing risks, including those listed below:
 - Operations/Transaction Risk: weak controls may affect customer privacy
 - Compliance Risk: offshore vendors may not have adequate privacy regulations
 - Strategic Risk: different country laws may not protect “trade secrets”
 - Credit Risk: a vendor may not be able to fulfill its contract due to financial losses

What Should be Protected?



Case Study 1 – e-Banking Services

- ❑ “The Tower Group estimates that the banks outsource 85% of their IT services”
- ❑ Reviewing Physical and Logic security controls:
 - Intrusion detection, location security and response capability
 - Network , system vulnerabilities and unauthorised access
 - Back-up databases and disaster recovery
- ❑ Reliable customer authentication mechanism:
 - Electronic agreements, digital signature
 - Secure access and transactions (eg. Encryption, biometrics)
 - Prevent fraudulent transaction, identity theft, computer crime
 - Promote legal enforceability
- ❑ Periodic compliance and legal reviews

Key Threats to e-Banking Services

- ❑ Vendor management and risk issues
- ❑ Security, data integrity and confidentiality
- ❑ Authentication, identity verification, and authorization
- ❑ Strategic and business risks
- ❑ Business continuity planning
- ❑ Permissibility, compliance, legal issues, computer crimes

Case Study 2 – e-Healthcare Services

- ❑ “The U.S. healthcare market alone will touch \$800 million for the Indian BPO companies in 2005”- NASSCOM report
- ❑ Involves emerging interactive technologies (i.e interactive TV, kiosk, interactive voice response systems)
- ❑ Provides various products & services in Healthcare Management :
 - e-Health Services category includes :
 - ❑ Customer (Patient) Content (eg. Transcription, telemedicine)
 - ❑ Medical supply distribution
 - ❑ Medical claim processing
 - ❑ Pharmaceutical outsourcing
 - ❑ Transplant Services
 - Health Insurance

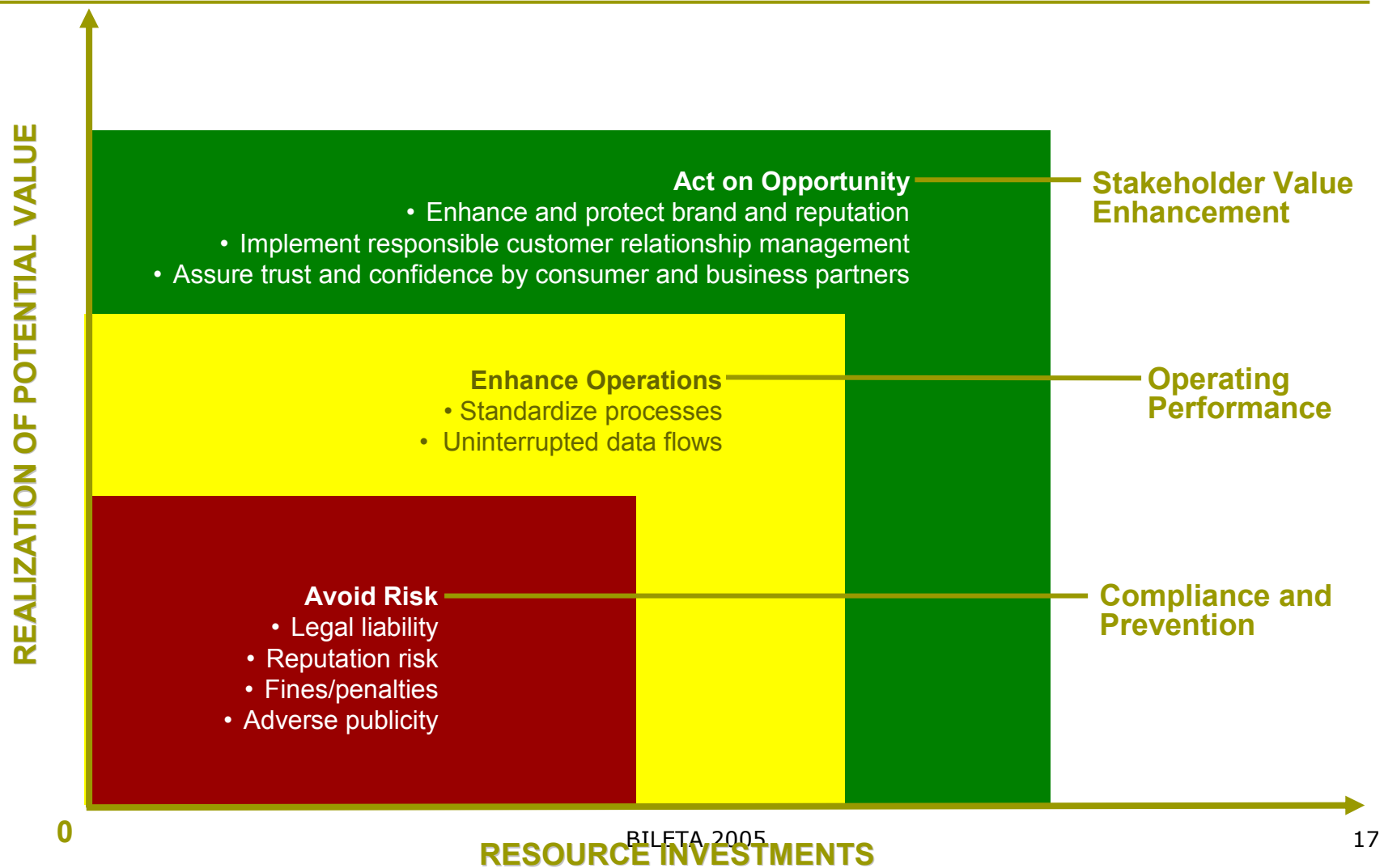
Key Threats to e-Health Services

- ❑ Technology upgradation crucial - IT and health care
- ❑ Translation of results (eg. Remote diagnosis, remote hosting)
- ❑ Tension between innovation and sustainability
- ❑ Quality and the effects of technology on health care industry
 - Risk of loss of control, quality, and customer good will
- ❑ Internet-based Physician Portals (eg. quacks, fraud, liability, e-prescriptions)
- ❑ Support provider adherence to evidence based care

Data Privacy

- ❑ Privacy has various interpretations associated with it.
- ❑ In the EU it means an individual's (or a group's) right to determine what information about them is stored by, and passed to, whom.
- ❑ In the USA it tends to mean the individual's right to be left alone, free from interference or surveillance.
- ❑ There are legal implications, particularly in the EU where the Data Protection Directive prevails.

Privacy Strategy Spectrum



Privacy and Outsourcing

- Securing communications in external environments
 - What laws govern?
 - *Can offshore vendors satisfy Gramm-Leach-Bliley/HIPAA?*
 - EU Privacy Directive
 - Technological security and testing
 - *Are all reasonable and necessary steps being taken?*
- Is vendor contract agreements sufficient to protect privacy rights?

Procedural Safeguards and Compliance Obligations

- ❑ Regulatory compliance obligations are generally non-delegable.
- ❑ Liability for non-compliance and reputational damage falls primarily on customer, not service organization.
- ❑ Requirements often evolving and still unclear; new additional requirements may emerge.
- ❑ Compliance may be costly both for customer & service organization.

Conflicting Priorities?

- European law on business transfers
 - Acquired rights directive - and “TUPE”
 - Data protection directive
 - Work council directive
 - Information and consultation framework directive
- Commercial Imperatives
 - Best solution
 - Knowledge transfer/ acquisition
 - Business continuity
 - Time frames
- Combined impact on the outsourcing relations



Thanks for your attention

E-mail: a.pai@qub.ac.uk

E-mail: s.basu@qub.ac.uk

Off: 028 9097 4846