

Information Security – Best Practices for Strategic Human Resource Management

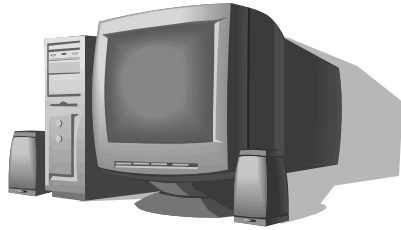
Elitex-2008 – Securing Indian Cyberspace

Sanjay Bahl
Chief Security Officer
Thursday, 17th January 2008, New Delhi

Background

- Technology invading work, home and leisure
- India has 65% and 45% share in global IT and BPO
- USD \$60 billion export revenue for Indian IT industry in 2010. Source: NASSCOM McKinsey Report 2005.
- Then and now
 - 2010: 7% of India's GDP (2000: 1% of India's GDP)
 - 2010: 31% of India's total exports
 - 2010: 2.3 million IT professionals (2005: 700, 000). Including indirect and spin-off employment 9 million people.
 - India : Most preferred destination to get right talent!
 - India is topmost on the list of preferred destinations for countries facing an internal talent crunch situation - Boston Consulting Group (BCG) partner and director James V Abraham
 - Chinese workforce which comes next in the list is mostly preferred for China-specific operations of the western companies as opposed to people in India, who are being tapped for functioning in any country - Source: <http://www.livemint.com> Posted: Wed, Oct 3 2007
 - India : Source for intellectual bright workforce!
 - The reasons for India's rising popularity amongst global employers are language efficiency, a service-oriented culture & an intellectually bright workforce -KPMG International Director for Corporate Citizenship Michael Hastings

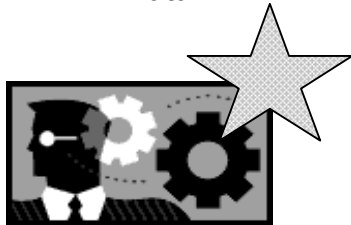
The Importance of “People”



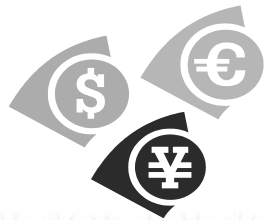
IT Infrastructure

Information

Data



People



Money



Brands



Other Assets

India: The preferred destination

Why?

- Cost savings
- Ability to ramp up or down
- Process and design efficiencies

The Importance of “Brand”

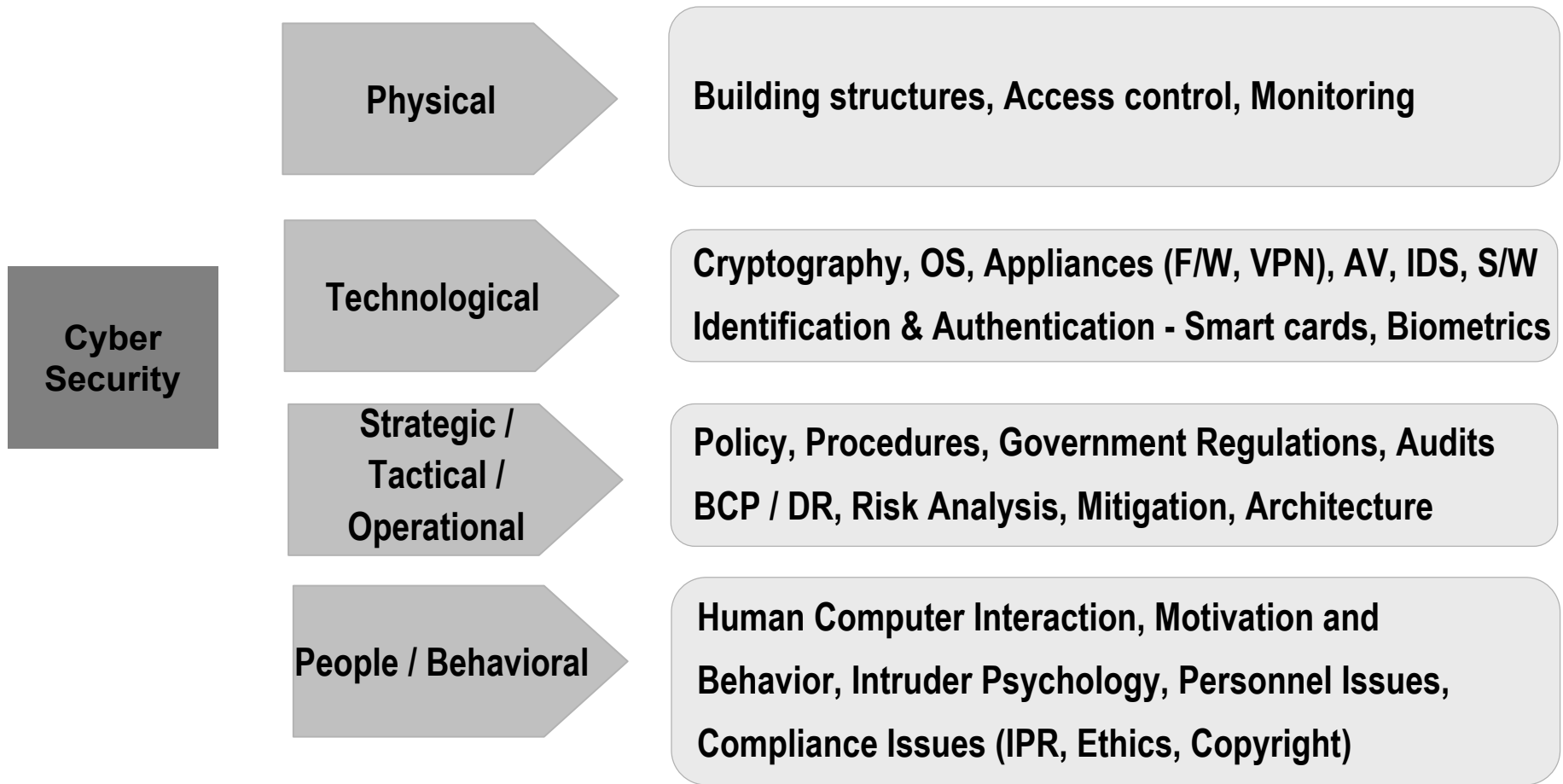
- Brand = **People** + Services + Products + Culture
- Influence choices of customers, employees, investors and government authorities
- Contribute to a third of Shareholder value on an average Source: Interbrand and JP Morgan Study Report



- Brand owners accountable for
 - Quality
 - Performance
 - Ethical practices

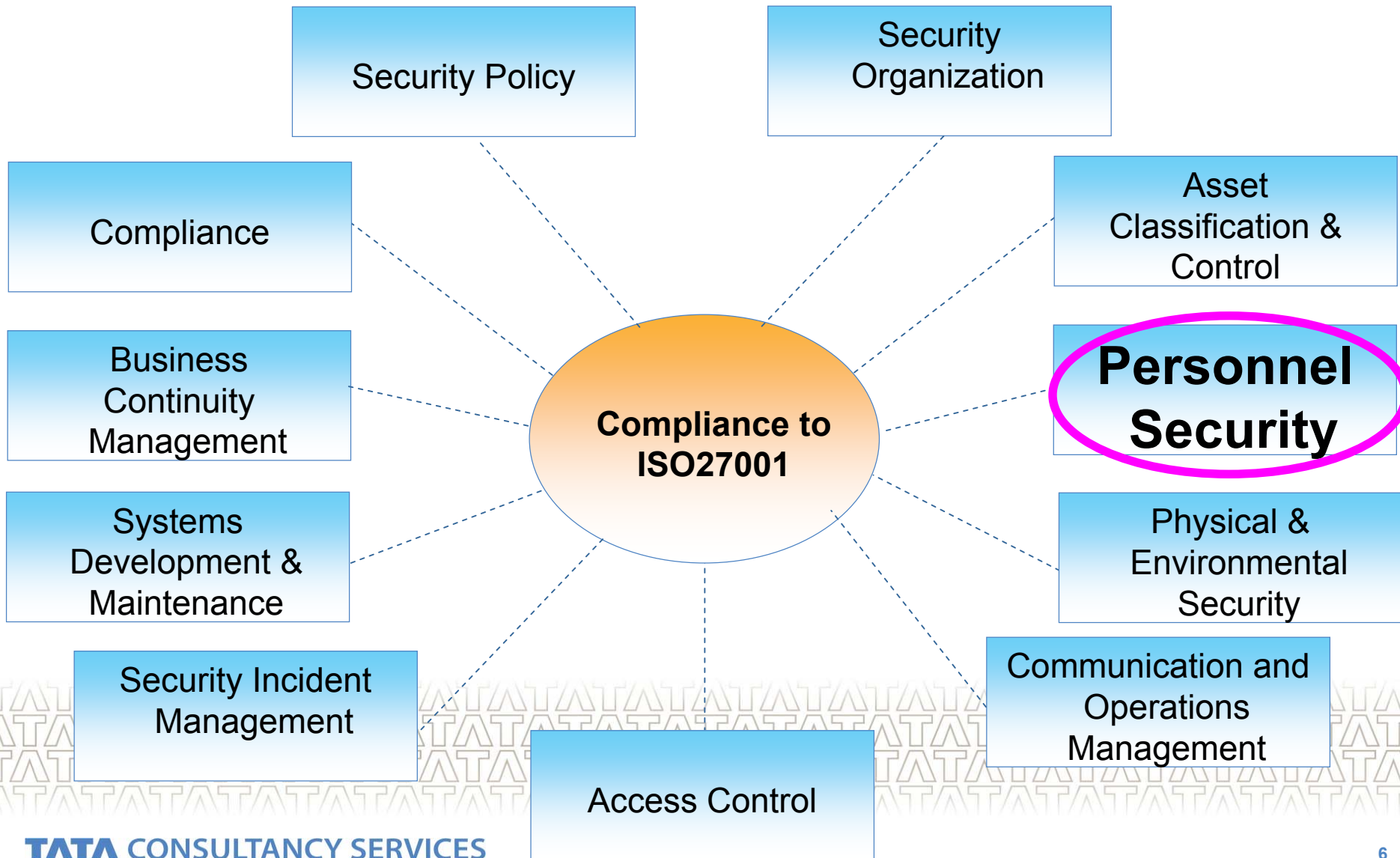
Note: All trademarks and registered trademarks are the property of their respective owners.

Cyber Security Chain - Technical and Non Technical Aspects



Attackers attack the weakest link

Adoption of ISO27001 Standards Framework



Technical Safeguards for Security

- Convergence of Cyber and physical space
- Security = Risk Management + Effective Countermeasures
- Security = Confidentiality + Integrity + Availability + Non-repudiation
- Multi Layered Security = People + Processes + Technology
- Protection of Intellectual Property (IP)
- Regulatory requirements
- Technical safeguards
 - Authentication controls
 - Access controls
 - In-depth defense: system level + network level
 - Firewalls, virus scanners, vulnerability assessment tools, content filtering tools, log analyzers, intrusion detection systems
 - VPNs, IPsec channels, encryption
- Awareness of security issues among employees
- Benchmarks (ISO 27001)

Why security in HR?

- **75% of IT Security incidents are caused from within the Company – not by hackers**
 - Gartner Group Report
- **87% of the frauds perpetrated internally**
 - Management employees (18%) , Other employees (69%)
 - The Malaysian KPMG Fraud Survey Report 2004
- **42% of Indian Companies feel that levels of fraud have increased in the last two years**
 - 9th Global Fraud Survey Report 2006, E & Y, India
- **Research finds that enterprises rank insider sources as their top security threat**
 - Hudson, Sally; Privileged Password Management: Combating the Insider Threat and Meeting Compliance Regulations for the Enterprise, IDC, 2007
- **Employees – most likely source of information security event**
 - Global State of Info Security Study by PricewaterhouseCoopers, CIO and CSO Magazines



Not just monetary loss.....but of confidence and trust
- core element upon which Customer Relationship is built

Why security in HR?

- **Research finds that when it comes to insider attacks, 86% of perpetrators held technical positions. Of these, 57% performed the attack after termination**
 - Cappelli, Dawn; Akash Desai; Andrew Moore; Timothy Shimeall; Elise Weaver; Bradford Willke - Management and Education of the Risk of Insider Threat (MERIT) CERT3 Program, Software Engineering Institute and CyLab at Carnegie Mellon University, 2006
- **Insider attacks resulting in**
 - Costly outages, Lost business, Legal liability, Failed Audits
- **20% of Candidate's Resumes contain major inconsistencies**
- **IPR at high risk fraud**
- **High recruitment costs**
- **Escalating training costs**
- **Decreased Customer confidence & trust due to security concern**

Protect principle of vicarious liability

- employers held responsible for wrongful acts of their employees

HR Issues for IT Industry

Two classes of human threat sources:

- **Intentional** - Intent and method targeted at the intentional exploitation of a vulnerability.

- **Insider Threats**

- Malicious Authorized User
- Former Employees

- **External Threats**

- Hackers / cracker / script kiddies
- Foreign Intelligence Service

- Terrorist

- **Unintentional** - A situation and method that may accidentally trigger a vulnerability

HR related security breaches – Analysis & Prevention

- **Major causes**

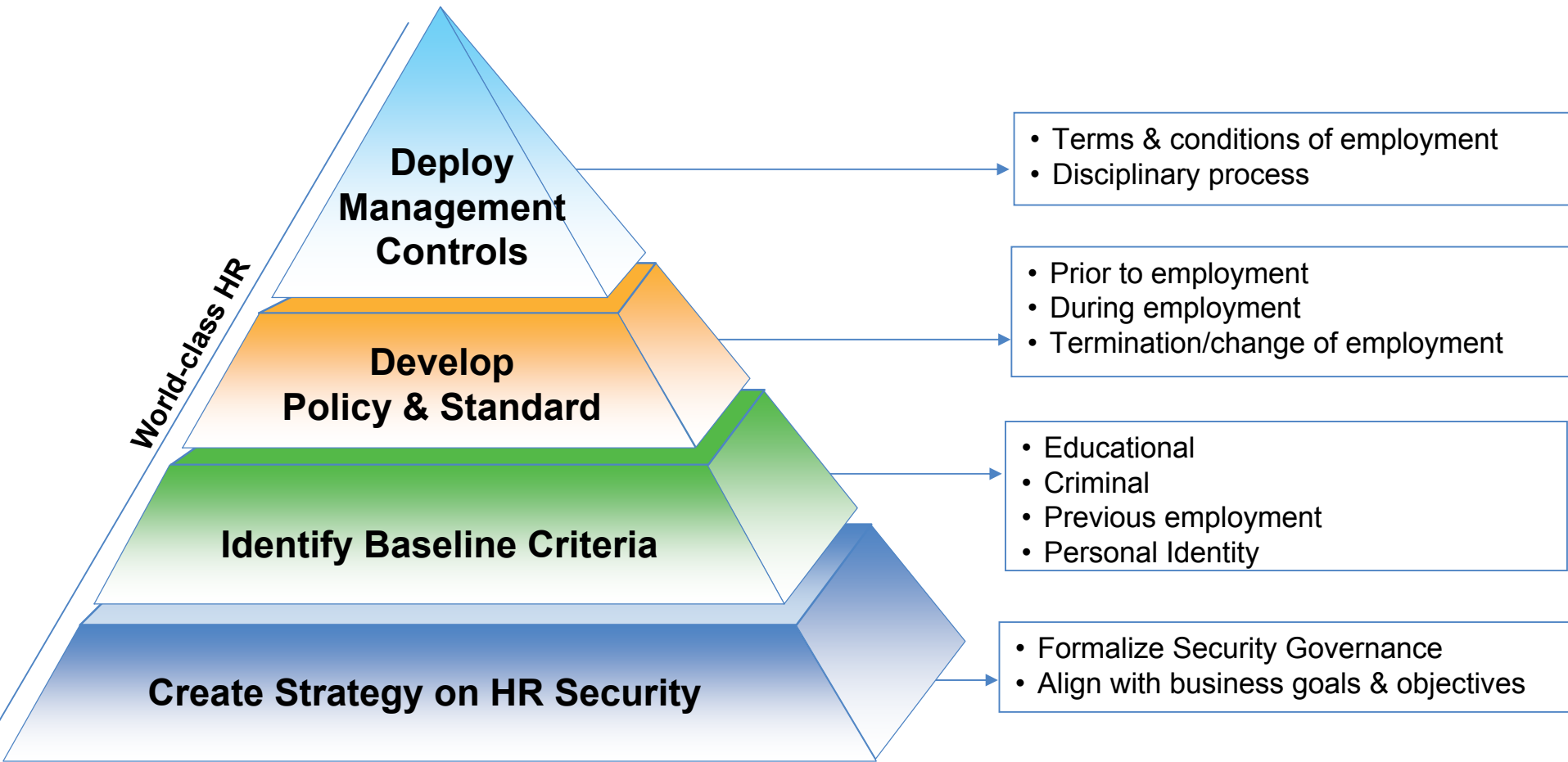
- Inadequate internal controls
- Poor hiring practices
- Diluting hiring policies informally
- Pre-requisites criteria for hiring not verified completely
- ‘Red Flags’ ‘Warning Signs’ ignored

- **Prevention Methodologies**

- Effective Pre-employment screening
- Establish, review and improve screening policy & procedures
- Effective Internal Audit with focus on Background check process
- Periodic Management review & monitor
- External/Client audit review
- Improved security measures
- Increase awareness on Background Check process
- Train internal auditors

Breach of Confidentiality, Integrity & Availability of information...

What can be done?



HR Security Model

Conclusion

- **Major focus areas**

- Enhance talent pool advantage by focusing on soft skill development
- Emphasis on security at an early stage and imbibe in the culture
- Improve and align regulatory norms with international bodies
- Strengthen key business infrastructure to support rapid growth
- Benchmark with world-class standards consistent with needs of the Organisation
- Proactively contribute to improve current practices and methodologies

"We in the security domain need to attract the attention of

- Government Authorities
- Educational and Research Institutions
- Corporate

to educate users and encourage changes in

- basic operating systems

to sustain continuous healthy growth and nurture **positive innovations for a safe and healthy environment.**"

Towards a positive innovation for a safe and healthy environment...

Thank You

