

# Cyber Crime & Frauds – India's Response



**Vidya Rajarao, Associate Director  
Forensic & Investigation Services, PwC India**

# Contents

- IT Act 2000 – Objectives
- Civil Wrongs under IT Act
- Computer Related Crimes under Indian Penal Code and Special Laws
- Cyber Crime & Fraud Cases in India
  - The Sun purchases bank details of 1,000 Britons for just £3 each
  - BPO employees arrested for hacking
  - CBI-FBI team nabs IIT engineer for software theft
  - India's first case of "phishing"
  - Credit Card Fraud - Large Nationalised Bank
  - SMS Scam
- PricewaterhouseCoopers' Global Economic Crime Survey, 2007
  - Introduction
  - Victims of Economic Crime
  - Types of Reported Frauds Incidents in India
  - Cost of Economic Crime
  - Perpetrators of Economic crime
  - Techniques for Prevention of Fraud
  - Future of Economic Crime

# IT Act 2000 – Objectives

**The IT Act 2000 aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce” which involve use of alternatives to paper based methods of communication and storage of information.**

## Salient features :

- Legal Recognition for E-Commerce
  - Digital Signatures and Regulatory Regime
  - Electronic Documents at par with paper documents
  
- E-Governance
  - Electronic Filing of Documents
  
- Amend certain Acts
  
- Define Civil wrongs, Offences, punishments
  - Investigation, Adjudication
  - Appellate Regime

# Civil Wrongs under IT Act

- Section 43 – Penalties and Adjudication
- Section 44 – Compensation for failure to protect data
- Section 65 – Source Code  
*Concealment, destruction, alteration of computer source code*
- Section 66 – Hacking  
*Crimes like virus attacks, unauthorized access to computer resources, data theft etc.*
- Section 66A – Sending Offensive Messages through Communication Services  
*Content that is grossly offensive or has menacing character*
- Section 67 – Pornography  
*Obscene material in the electronic form*
- Section 69 – Decryption of information  
*Controller issues order to Government agency to intercept or decrypt or cause to be monitored any information transmitted through any computer resource. Order is issued in the interest of the sovereignty or integrity of India. the security of the State.*
- Section 70 – Protected Systems  
*Acts covered by this section include switching computer on / off, using installed software / hardware, installing software / hardware, port scanning*
- Section 72 – Breach of confidentiality and privacy  
*Secured access to any material, discloses such material to an other person without the consent of the subscriber*
- Section 87 – Encryption for security of data  
*The Central government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce by rules, provided for one or more modes or methods for encryption.*

# Computer Related Crimes under Indian Penal Code and Special Laws

|   |              |
|---|--------------|
| Sending threatening messages by email   | Sec 503 IPC  |
| Sending defamatory messages by email  | Sec 499 IPC  |
| Forgery of electronic records   | Sec 463 IPC  |
| Bogus websites, cyber frauds  | Sec 420 IPC  |
| Email spoofing  | Sec 463 IPC  |
| Punishment for cheating using electronic signature of another person                      | Sec 417A IPC |
| Punishment for cheating by impersonation using communication network or computer resource | Sec 419A IPC |
| Online sale of Drugs  | NDPS Act     |
| Web-Jacking   | Sec 383 IPC  |
| Online sale of Arms   | Arms Act     |

# RECENT CASES



## **The Sun purchases bank details of 1,000 Britons for just £3 each** **Employee sacked**

### Case:

- As communicated by The Sun, its reporter (Oliver Harvey), operating undercover, was sold top secret information on 1,000 bank accounts by Karan Bahree in Delhi. Bahree confirmed as to having obtained the data from contacts at call centers in and around Delhi.
- Bahree claimed that he had acted at the behest of another person to merely deliver a "CD presentation" without knowing that he was passing on classified information.
- However, Bahree has admitted to taking the money as a service charge.

### Action Taken:

- Bahree sacked by his employer (Infinity eSearch).
- Gurgaon Police has initiated a suo moto preliminary enquiry into the case, and has seized the computer Bahree used to work on, at Infinity eSearch.
- His resume, appointment letter and termination letter have also been seized.

## **BPO employees arrested for hacking** **Accused arrested by police**

### Case:

- Two employees of IntelNet Global Service, a BPO firm, tampered with the credit card profiles of American citizens.
- According to sources, the two employees were paid over Rs 10 lakh through a wire transfer from a bank in Detroit, for modifying the personal and financial data of hundreds of credit card holders.
- These records were maintained by a US-based company, Trans-Union Services. IntelNet, a service provider, had undertaken the job to maintain the records of Trans-Union.
- The two employees had hacked into TransUnion's database in August 2005 on the instructions of one Frederick Rodney, based in the US.
- As per police reports, Rodney had provided file numbers of card holders, and had asked the employees to make the changes in their financial profiles.

## **CBI-FBI team nabs IIT engineer for software theft** **Accused remanded to CBI custody**

### Case:

- In August 2002, Shekhar Verma, an IIT Kharagpur graduate and a former employee of software firm Geometric Software Solutions Ltd, GSSL, was caught red-handed trying to sell a data source code.
- The source code was the property of GSSL's American client Solidworks.
- The employee had demanded a price of \$240,000 for the code.

### Action Taken:

- The US firm (Solid Concepts), which was offered the source code by Verma, had got suspicious, and had informed Solidworks and GSSL.
- In turn, Solidworks and GSSL got in touch with the Central Bureau of Investigation, CBI, and the Federal Bureau of Investigation, FBI.

## **CBI-FBI team nabs IIT engineer for software theft (contd...)**

### **Accused remanded to CBI custody**

- Following it, the CBI and FBI laid a trap for Verma, and arrested him for attempting to sell the code under Sections 379 (theft) and 406 (criminal breach of trust) of the Indian Penal Code and the Information Technology Act.
- The accused was produced before a designated court in New Delhi, which remanded him to four days of CBI custody.
- The CBI recovered all copies of the Solidworks source codes in Verma's possession, and verified that Verma had not previously provided it to any other party.

## **India's first case of "phishing"**

### **Accused arrested by police**

#### Case:

- Kamal Kumar, with assistance from his friend in Nigeria, develops a clone of the ICICI website (original – [www.icicibank.com](http://www.icicibank.com); clone – [www.icicibank.net](http://www.icicibank.net)).
- E-mails are sent by Kumar to ICICI customers, asking them to validate their details like credit card numbers, account numbers, banking passwords etc. Link at the bottom of e-mails would lead customers to the fake website.
- Details provided by customers on fake website are used by Kumar to do shopping on the net, for which the real card holder ended up paying.

#### Action Taken:

- Case lodged by ICICI Bank with Mumbai police on 7<sup>th</sup> February 2006.
- Kumar is arrested by the Mumbai police on 2<sup>nd</sup> March 2006 on various counts of cheating, forgery and hacking, and the fake site has been brought down.

## **Large Nationalised Bank** **Accused arrested by police**

### Case:

- Shaikh working in the Credit Card department of State Bank of India had access to credit card details of customers, which he passed on to his friend kale who further passed on to his friend Lukkad who used this information to book air tickets.
- These air tickets were sold to customers & institutions for money. One such customers got an alert message of ticket purchases when he was holding the card with him & had not done any transaction.

### Action Taken:

- On Complaint the police found that all tickets were booked online. Police requested the log details & got the information of a private institution. Investigations revealed that the details were obtained from State Bank of India.
- Cyber Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate were involved in eight days of investigation and finally caught the culprits.
- In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested.

## **SMS Scam**

### **Accused arrested by police**

#### Case:

- Two Nadar brothers along with their friend Ramesh Gala, took help of SMS technology and launched the first of its kind SMS fraud in India. They launched a campaign in print media & also put up a website ([www.getpaid4sms.com](http://www.getpaid4sms.com)) wherein subscribers were asked to pay deposit of INR 500 and they receive 10 SMS every day against it. The customers were promised handsome commissions if they managed to rope in more subscribers by forwarding the messages.
- They told their customers that they were working for a US based company called Aropis Advertising Company which wanted to conduct a market survey about local response to their advertisement and were using SMS as it was the latest means of communication.
- Initially small amounts were paid but when large amounts of cheques began to get dishonored the customers started to worry. On November 30, one of the duped agents approached the DN Road police station and lodged a complaint after a bank failed to honour a pay order amounting Rs.2.17 million issued by the Nadar brothers.
- A case was registered with the DN Nagar Police station & later transferred to Economic Offences Wing (EOW).

## **SMS Scam (contd..)**

### Action Taken:

- By December 2006 the scam had membership of 50,000 customers in Mumbai alone. The Police suspected that hundreds of thousands from across the country were also hooked to the scheme, thanks to a massive agent network and a door-to-door campaign carried out by the firm's now duped agents.
- During investigations, the EOW came to know that the Nadars, residents of the upmarket Juhu-Tara Road, owned a fleet of imported sport utility vehicles and Sedans.
- Jayanand Nadar, 30, and Ramesh Gala, 26, were arrested from a hotel in Mira Road in the western suburbs. Nadar, a first year college dropout, along with his brother Jayaraj had allegedly duped at least 50,000 people of Rs.400 million, said officials in the city police's EOW.

# **PricewaterhouseCoopers' Global Economic Crime Survey, 2007**



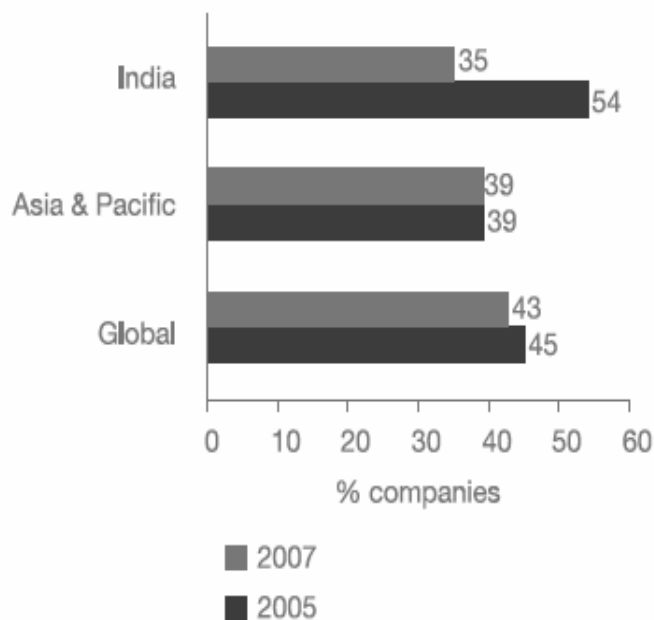
# Introduction

- PricewaterhouseCoopers' Global Economic Crime Survey 2007 is the largest, most comprehensive international survey of economic crime. Some of the key highlights of the survey were as under
  - 4th biennial survey on economic crime by PwC
  - Respondents covered 40 countries
  - Over 5,400 companies globally (incl.1,500 executives with experience in emerging markets)
  - 152 Companies in India
  - 22 languages
  - 16 industries/sectors
  - The survey was undertaken through computer-assisted interviews (Telephonic & Web) from a randomly selected sample of organisations in the country.

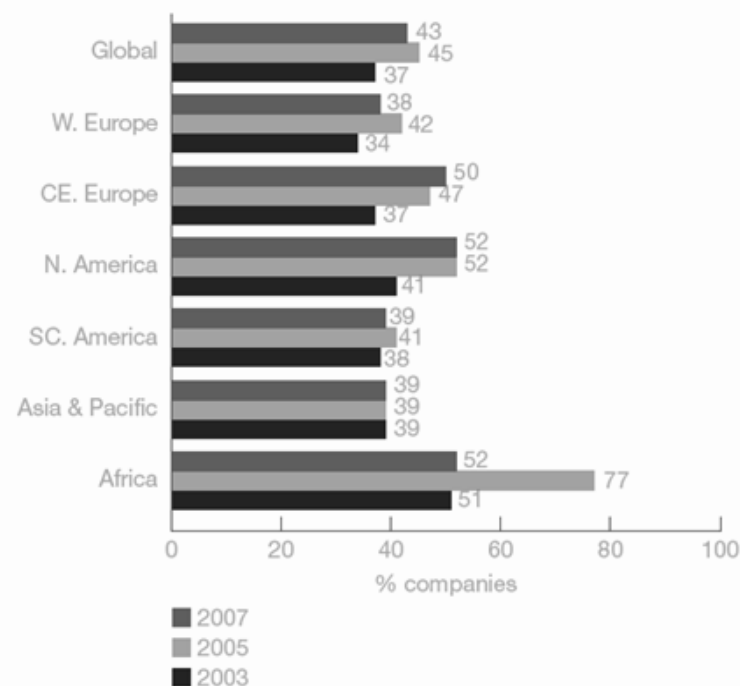
*Further information on survey methodology and definitions of economic crimes can be found in the Global Economic Crime Survey 2007 report and at [www.pwc.com/crimesurvey](http://www.pwc.com/crimesurvey)*

# Victims of Economic Crime

The 2007 economic crime study reveals that 35% of companies in India were victims of economic crime during the past two years.



Globally Over 43% of the companies interviewed reported suffering one or more significant economic crimes



# Types of Reported Frauds Incidents in India

Most common types of fraud incidents reported in India were as follows

- asset misappropriation
- money laundering
- IP infringement
- Corruption & bribery
- Accounting fraud, etc

Corruption and bribery is one area in which reported fraud in India has increased since our last survey

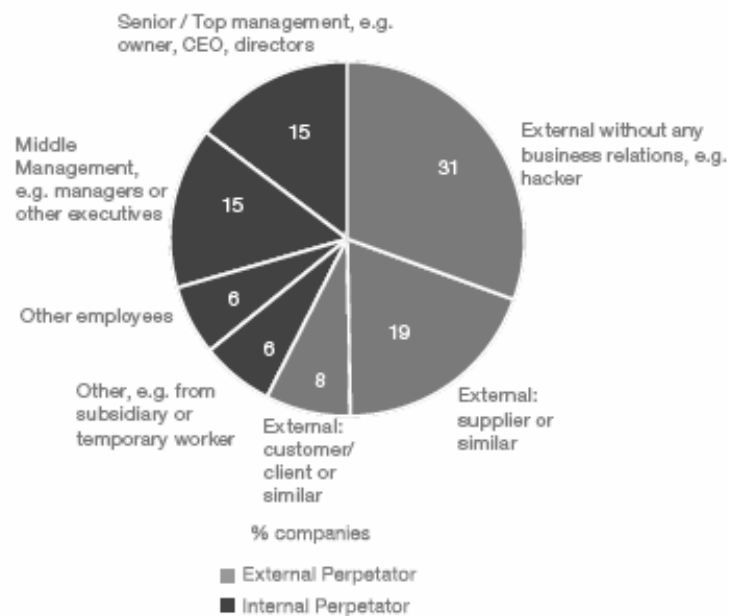
## Cost of Economic crime

- Economic crime continues to be an expensive proposition for companies, both in terms of losses due to such crimes and the cost of managing frauds.
- Companies in India suffered average direct losses of US \$1.5 million (INR 6 crore) due to fraud in the preceding two years (i.e. 2005 to 2007).
- The level of collateral damage is directly proportional to the seniority of the perpetrator. In 35 percent of the occasions in India where senior managers were involved, the collateral damage to the brand was very significant.

|  | India     | Asia & Pacific | Global    |
|--|-----------|----------------|-----------|
| Direct loss (average in US\$)                      | 1,535,217 | 1,438,526      | 2,420,700 |
| +  |           |                |           |
| Management cost (average in US\$)                  | 1,029,184 | 416,393        | 550,355   |
| +  |           |                |           |
| Damage to reputation or brand (% of cases)         | 92        | 89             | 88        |
| +  |           |                |           |
| Decline in staff morale (% of cases)               | 88        | 92             | 88        |
| +  |           |                |           |
| Damage to external business relations (% of cases) | 84        | 87             | 84        |
| +  |           |                |           |
| Strained relation with regulator (% of cases)      | 75        | 83             | 80        |

## Perpetrators of Economic crime

- It is generally accepted that frauds are committed (by individuals) when the following three conditions co-exist:
  - The individual must have an incentive to commit fraud
  - The individual must identify an opportunity to commit fraud
  - The individual must be able to rationalise the reason for committing fraud.
- The survey found that 42% of the frauds reported were perpetrated by employees. Out of these, members of senior management were responsible for 35% of frauds. A typical perpetrator of fraud is shown in figure below.



# Techniques for Prevention of Fraud

- Internal controls are not enough. An ethical corporate culture plays an equally important role in deterring fraud.
- Companies should comprehensively assess fraud risks on a periodic basis in order to identify potential fraud types and to determine the likelihood of and risk of occurrence of such fraud.
- In addition, companies should also implement tailored controls to reduce the likelihood and impact of identified risks.
- PricewaterhouseCoopers' seven step approach to an effective fraud risk assessment covers the following:
  - Organise the assessment – identify key business functions
  - Determine the scope of the assessment – areas such as sales, procurement, finance and key business units should be considered
  - Identify potential fraud schemes and scenarios that are inherent to the geographic region and industry sectors in which the company operates
  - Assess likelihood of occurrence and impact
  - Evaluate design and test effectiveness of controls
  - Identify and assess residual risks
  - Adjust design and implementation of controls to reflect changes in company structure and business conditions.

## Future of Economic Crime

- Fraud has and will remain an intractable problem. While some types of fraud like asset misappropriation have remained static, others like hacking and theft of intellectual property are on the rise.
- As companies in India expand their reach and presence in other countries, they are not only at the risk of 'home-grown' frauds, but also exposed to bribery and corruption risks in those markets.
- Additionally, safeguarding intellectual property and protecting trade secrets is paramount as competitors attempt to 'copy' or 'steal' successful products and services. Against this backdrop, detection of economic crime by chance is clearly inadequate.
- The results of our survey have clearly shown that internal control mechanisms by themselves were ineffective in preventing and detecting fraud, despite the fact that multiple controls had been installed by the companies surveyed.
- Instead, our experience suggests that companies that adopt a proactive and risk-based approach are better equipped to combat economic crime. This entails effectively implemented and regularly updated controls along with a strong culture of the organisation that supports a holistic compliance program working in tandem with a clearly understood code of ethics, emanating from the top management.

# Thank You

© 2008 PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers", a registered trademark, refers to PricewaterhouseCoopers Private Limited (a limited liability company in India) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

PRICEWATERHOUSECOOPERS 