Emerging cyber threats

for ISACA Mumbai Chapter Meeting

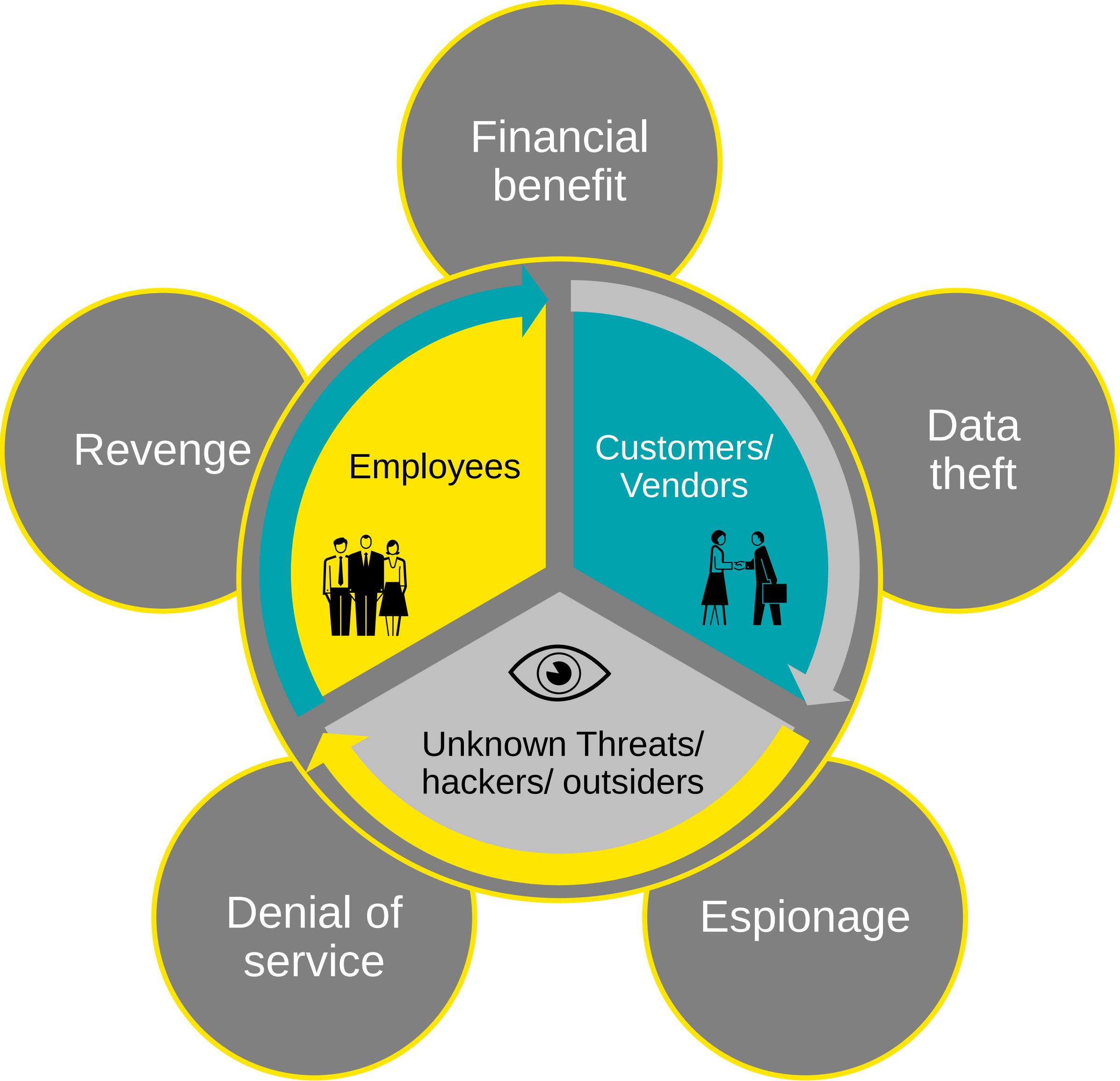
EY Forensic Technology and
Discovery Services

14 January 2017

Agenda

- **Threat Landscape**
- **Attack Vectors**
- **Ransomware**
  - Evolution of ransomware
  - Modus Operandi
  - Statistics
  - Impact of ransomware
- **Cryptocurrencies**
  - How Cryptocurrencies work
  - Why Cryptocurrencies

Threat Landscape



Attack Vectors

- Phishing
- Distributed Denial of Service (DDOS)
- Specific Applications (SWIFT/ SAP)
- Data Theft
- Social Media
- Ransomware
- Unauthorized software
- Control weaknesses
- Lack of technological defenses

Ransomware

Malware:

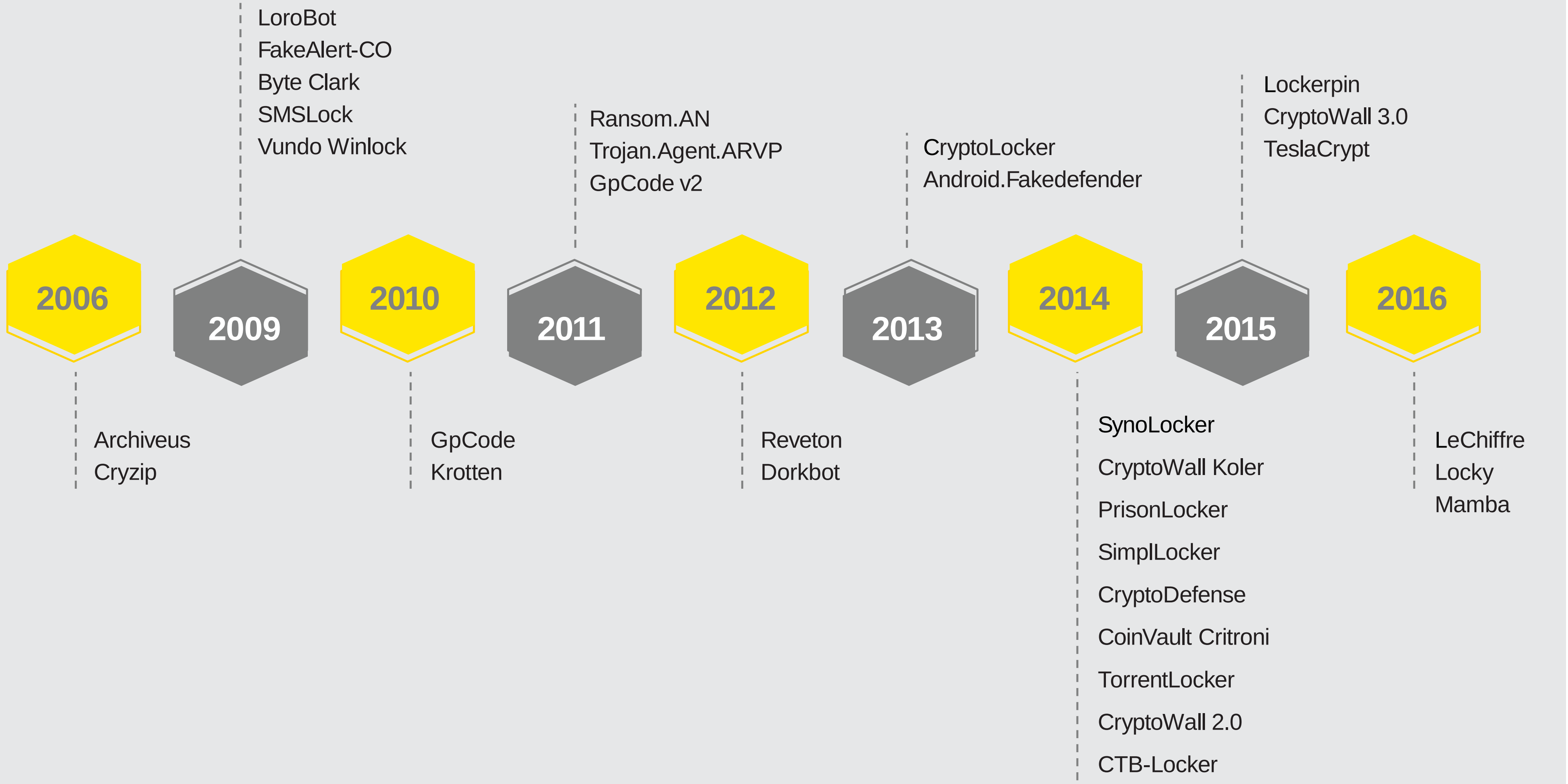
Malware (**Mal**icious soft**ware**) is a code that disrupts or damages computer systems and data. Malware can be computer viruses, worms, Trojan horses, spyware, adware or any other program with malicious content.

Ransomware:

A malware that exploits security vulnerabilities in a system and blocks a user’s access to his/her computer files either by locking them up or encrypting them. The user’s system / data is held hostage for a ‘ransom’ in exchange for a decryption key that can be used to regain access to the data.

- India was among the top 5 countries affected by ransomware attacks, along with US, Canada and Australia
- While the initial victims for ransomware were consumers, the focus is steadily shifting towards organizations as the attackers are moving from indiscriminate targeting to focused attacks. The latest surge in healthcare industry is another indicator of this trend

Evolution of ransomware



2006

Archiveus
Cryzip

2009

LoroBot
FakeAlert-CO
Byte Clark
SMSLock
Vundo Winlock

2010

GpCode
Krotten

2011

Ransom.AN
Trojan.Agent.ARVP
GpCode v2

2012

Reveton
Dorkbot

2013

CryptoLocker
Android.Fakedefender

2014

SynoLocker
CryptoWall Koler
PrisonLocker
SimplLocker
CryptoDefense
CoinVault Critroni
TorrentLocker
CryptoWall 2.0
CTB-Locker

2015

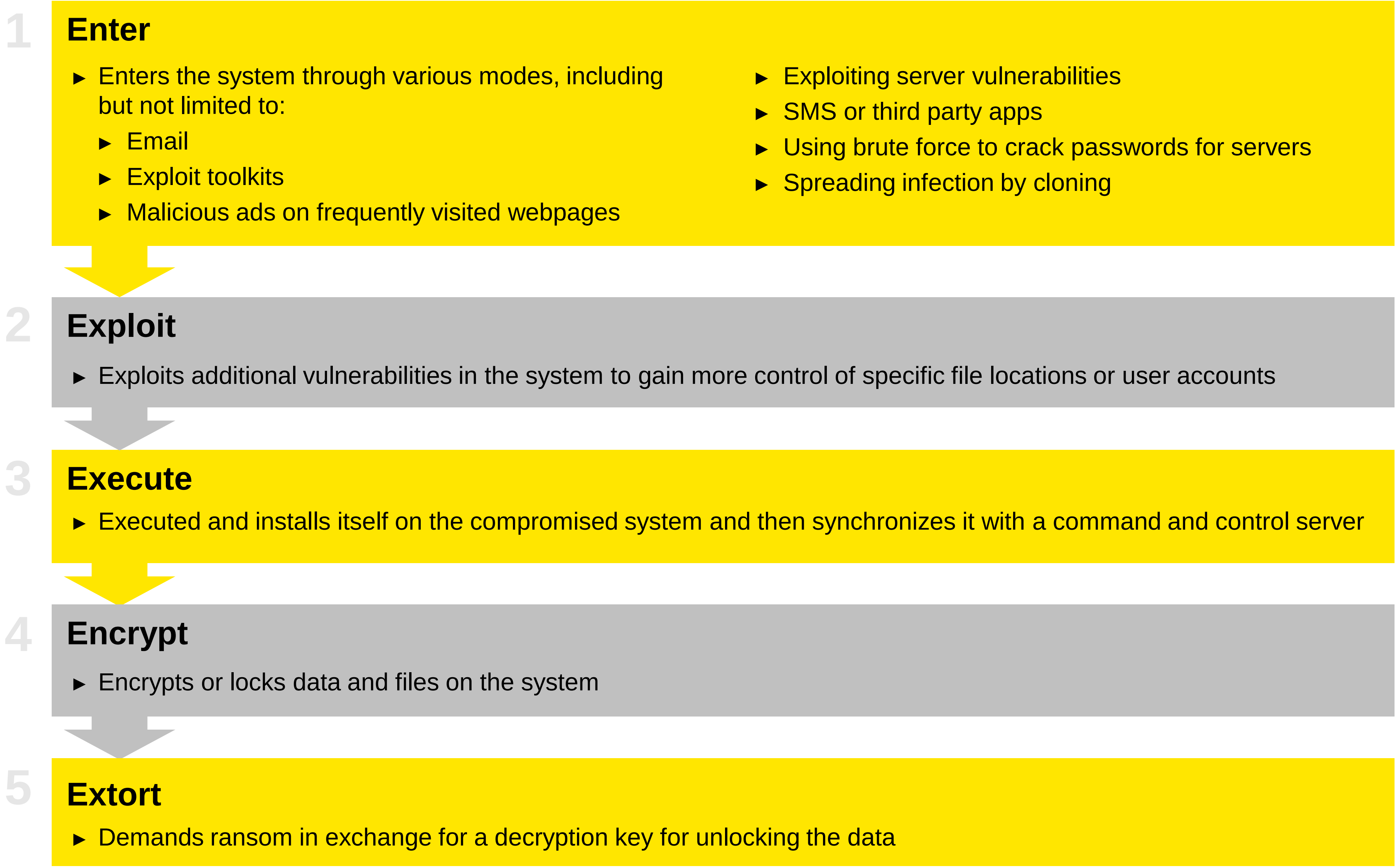
Lockerpin
CryptoWall 3.0
TeslaCrypt

2016

LeChiffre
Locky
Mamba

Data collated from various sources

Modus Operandi



1

Enter

- Enters the system through various modes, including but not limited to:
  - Email
  - Exploit toolkits
  - Malicious ads on frequently visited webpages
- Exploiting server vulnerabilities
- SMS or third party apps
- Using brute force to crack passwords for servers
- Spreading infection by cloning

2

Exploit

- Exploits additional vulnerabilities in the system to gain more control of specific file locations or user accounts

3

Execute

- Executed and installs itself on the compromised system and then synchronizes it with a command and control server

4

Encrypt

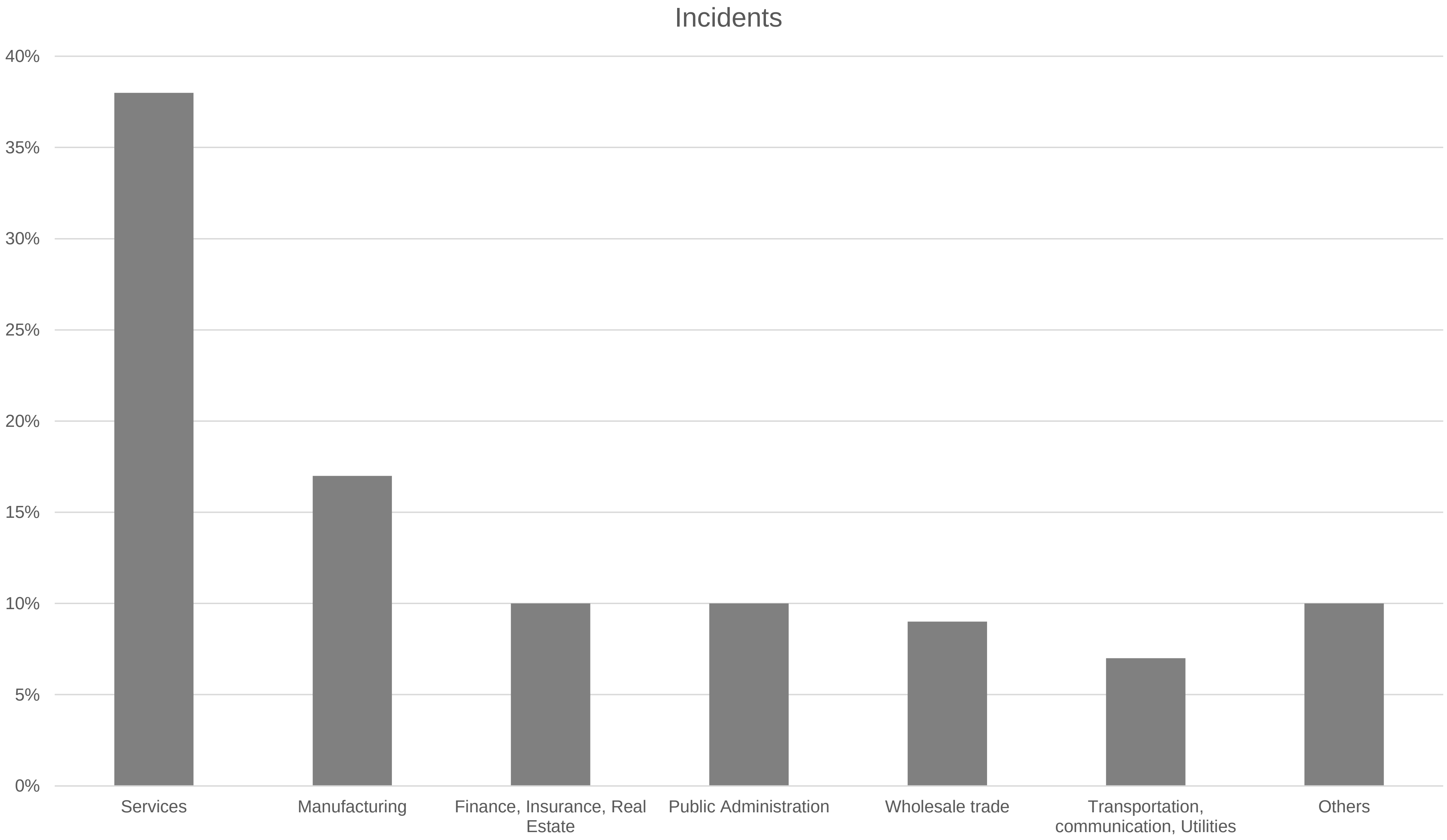
- Encrypts or locks data and files on the system

5

Extort

- Demands ransom in exchange for a decryption key for unlocking the data

Statistics – Ransomware incidents



Impact of ransomware

- **Financial and operational losses**
  - Downtime cost
  - Financial cost (often demanded in Cryptocurrencies)
  - Data loss
  - Loss of life (especially in case of healthcare)
- **Reputational damage**
- **Employee stress**
- **Data breach**
- **Disruption of business continuity**

Case Study

Company

- A global medical equipment manufacturer

What went wrong

- Critical data on company computers and main ERP server was infected by the LeChiffre Ransomware
- A ransom of US$1,000 in virtual currency was demanded per computer for the release of data

Findings

- The hacker conducted port scan on all the IP addresses belonging to the company
- A vulnerability was exploited on an internet facing server and on another server brute force was used to crack remote desktop password. This server was stand alone.
- After gaining access the hacker deployed the malware on both servers.

Cryptocurrencies

Cryptocurrencies

- Virtual currencies, stored in “e-wallets” and traded virtually peer to peer or person to person
- These currencies can provide anonymity, meaning there is no easy way of tracking the parties when a transfer is made using this currency
- **Examples:** Bitcoin, Litecoins, Dogecoins, etc.

Key features:

1 **Virtual currency**

2 **Works on the concept of blockchain**

3 **Decentralised**

4 **Transactions are irreversible**

5 **Ultimate cap on total amount of currency to be issued**

6 **Offers anonymity to users**

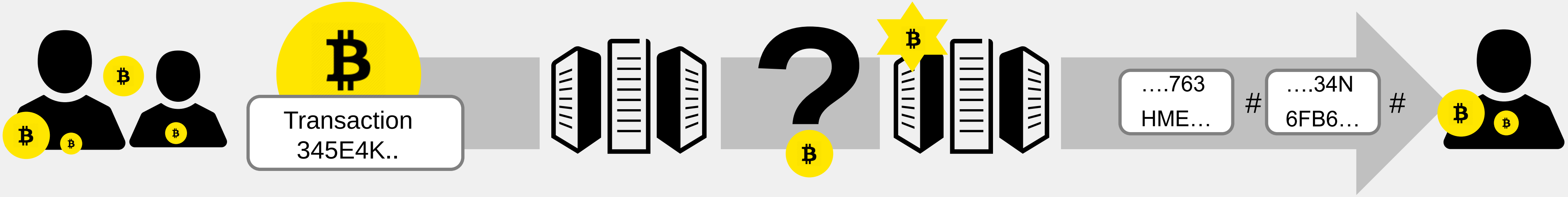
7 **Can be permanently lost**

8 **No consumer protection from frauds**

9 **Value is volatile**

How Cryptocurrencies work – Bitcoin example

How a cryptocurrency transaction is processed



1 Payers initiate a cryptocurrency payment through a wallet application

2 This transaction is broadcasted on the global Bitcoin network

3 Every ten minutes or so, specialised computers on this network, known as “miners”, collects a few hundred transactions and combine them in a “block”.

4 Miners process the block, reaching a consensus on what the new “blockchain” should look like

5 Miners are rewarded with newly minted cryptocurrency for providing vast amounts of computing power- giving them a stake in the smooth functioning of the currency.

6 Miners disseminate the new blockchain to the entire network, recording the transactions in the latest block

7 The payee can use his wallet software to see whether the cryptocurrency has arrived.

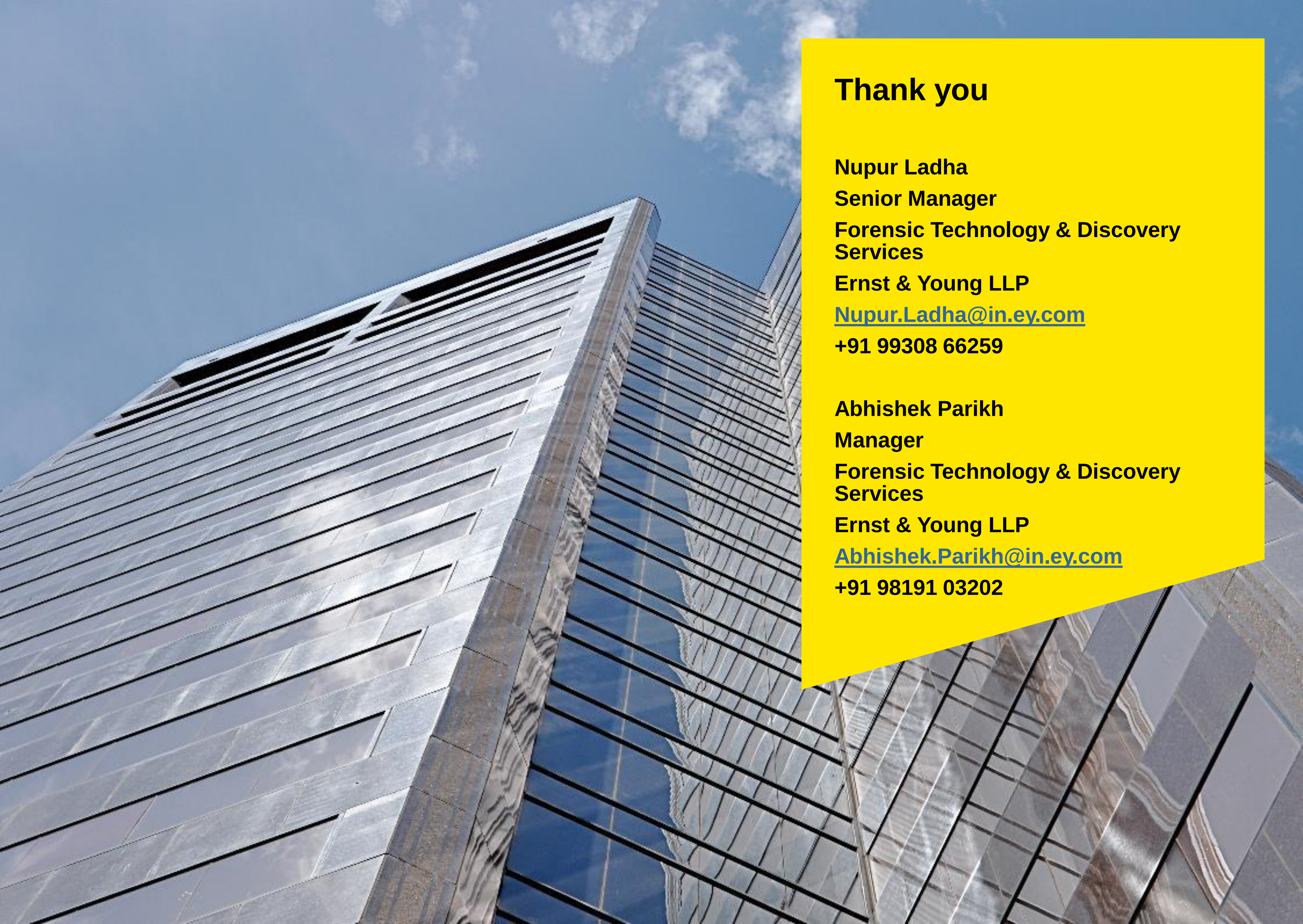
Why Cryptocurrencies

Pros:

- Transparency
- Virtually impossible to counterfeit
- Cost savings
- Faster speed of execution
- New opportunities for business models
- Scalable divisible down to 8 decimals
- Global

Cons:

- Open source
- Potential for loss
- Money supply is not controlled by economists or monetary experts, but technology experts and programmers
- Irreversible transactions
- Offers anonymity



Thank you

Nupur Ladha
Senior Manager
Forensic Technology & Discovery Services
Ernst & Young LLP
Nupur.Ladha@in.ey.com
+91 99308 66259

Abhishek Parikh
Manager
Forensic Technology & Discovery Services
Ernst & Young LLP
Abhishek.Parikh@in.ey.com
+91 98191 03202