Cyber crime
Indian legal system
& International Co-operation

NAVNEET RAJAN WASAN

Paytm ‘fraud’: This big money manager lost Rs 5,000 from mobile wallet, here’s how he got it back

By: Sushruth Sunder | Updated: **November 13, 2019** 12:01:13 PM

A prominent investment manager got a rude shock this morning, when he discovered that Rs 5,000 from his Paytm wallet got automatically transferred to a juice vendor. Notably, Vikaas M Sachdeva, CEO of a reputed AMC, was hit by fraud and his entire balance of Rs 5,520.93 got transferred to Shree Balaji Juice centre at about 12.15 am on Tuesday morning. Sharing the incident of Twitter, Sachdeva said that the fraud took place when he was asleep at home. “Just flagging off a fraud which happened to me. My entire paytm balance of over 5k got transferred to an entity called Balaji juice center at 12.15 am today while I was asleep at home. Reported it to @Paytmcare but am surprised how vulnerable paytm is to cyber fraud.’

Vikaas M Sachdeva @vikaasmsachdeva
Just flagging off a fraud which happened to me. My entire paytm balance of over 5k got transferred to an entity called Balaji juice centre at 12.15 am today while I was asleep at home. Reported it to @Paytmcare but am surprised how vulnerable paytm is to cyberfraud @vijayshekhar
563
5:25 AM - Nov 12, 2019

CYBER CRIME

Cybercrime, also called **computer crime**, the use of a computer resource and computer network as an instrument to further illegal ends, such as committing fraud (financial or commercial) , trafficking in child pornography and intellectual property, stealing identities, stealing or manipulating data, violating privacy or providing anonymous platform to terrorists.

Cybercrime, especially through the Internet, has grown in importance, dimension and sophistication as the computer/s has become central to commerce, entertainment, and government.

Cost of Data Breach

- According to figures revealed by a research, the average total cost of a data breach for the 350 companies participating in that research increased from $3.52 to $3.79 million in one year.
- The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $145 in 2014 to $154 in this year's study.

Cost of Data Breach

Data breaches cost the most in the US and Germany and the lowest in Brazil and India. The average per capita cost of data breach is $217 in the US and $211 in Germany. The lowest cost is in Brazil ($78) and India ($56). The average total organizational cost in the US is $6.5 million and in Germany $4.9 million. The lowest organizational cost is in Brazil ($1.8 million) and India ($1.5 million).

Cost of Data Breach

The cost of data breach varies by industry. The average global cost of data breach per lost or stolen record is $154. However, if a healthcare organization has a breach the average cost could be as high as $363 and in education the average cost could be as high as $300. The lowest cost per lost or stolen record is in transportation ($121) and public sector ($68). **The retail industry's average cost increased dramatically from $105 in one year to $165.**

CYBER CRIME & LAW

Information Technology Act, 2000 was passed on 17th October, 2000 & amended to deal with the technology in the field of e-commerce, e-governance, e-banking as well as provide penalties and punishments in the field of cyber crimes.

The Act was amended by IT (Amendment) Act 2008.

CYBER CRIME

- **COMMITTED THROUGH USE OF COMPUTING DEVICES**
  - (ELECTRONIC MANIPULATION OF DATA)
- **DIRECTED TOWARDS COMPUTING DEVICES**
  - (HACKING, VANDALISM, COMPUTER VIRUSES)
- **COMMUTING IS INCIDENTAL TO CRIME**
  - (PNB LoU FRAUD)

DEFINITION IN INFORMATION TECHNOLOGY ACT 2000

- (i) "**Computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
- (ha) "**Communication Device**" means Cell Phones, Personal Digital Assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)

DEFINITIONS IN INFORMATION TECHNOLOGY ACT 2000

(j) "**Computer Network**" means the inter-connection of one or more Computers or **Computer systems** or Communication device through;

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

DEFINITIONS IN INFORMATION TECHNOLOGY ACT 2000

(k) "**Computer Resource**" means computer, communication device, computer system, computer network, data, computer database or software;

(l) "**Computer System**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

Penalty and Compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, -

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

Penalty and Compensation for damage to computer, computer system, etc.

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;
he shall be liable to pay damages by way of compensation to the person so affected.

Penalty and Compensation for damage to computer, computer system, etc.

SECTION 43 A

Where a **body corporate**, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

INFORMATION TECHNOLOGY ACT 2000
PENAL OFFENCES

CHAPTER XI

SECTION 65: TAMPERING WITH COMPUTER SOURCE DOCUMENTS

- Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Explanation.--For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

SECTION 66: COMPUTER RELATED OFFENCES

(TO BE READ WITH SECTION 43)

66. Computer Related Offences. -
If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both.

Explanation: For the purpose of this section,-

a) The word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

24. “Dishonestly”.—Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing “dishonestly”.

25. “Fraudulently”.—A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

SECTION 66A (SINCE STRUCK DOWN BY APEX COURT)*

SECTION 66B PUNISHMENT FOR RECEIVING STOLEN COMPUTER RESOURCE OR COMMUNICATION DEVICE

SECTION 66C PUNISHMENT FOR IDENTITY THEFT

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

SECTION 66D PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER RESOURCE

Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

SECTION 66E PUNISHMENT FOR VIOLATION OF PRIVACY

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation. -For the purposes of this section-(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;
(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
(d) "publishes" means reproduction in the printed or electronic form and making it available for public; e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that;-(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

SECTION 66F PUNISHMENT FOR CYBER TERRORISM

(1) Whoever,—
(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—
(*i*) denying or cause the denial of access to any person authorised to access computer resource; or
(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(*iii*) introducing or causing to introduce any computer contaminant,
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

SECTION 67 PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

SECTION 67B PUNISHMENT FOR PUBLISHING/ TRANSMITTING MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT FORM

67-B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.-

Whoever,-
(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
(d) Facilitates abusing children online; or
(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,
shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Section 72-A. Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Section 75. Act to apply for offence or contraventions committed outside India

75. Act to apply for offence or contraventions committed outside India.-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 80. Power of Police Officer and Other Officers to Enter, Search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

Protection of Children from Sexual Offences Act, 2012

13. Use of child for pornographic purposes.-
Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes-

a. representation of the sexual organs of a child;

b. usage of a child engaged in real or simulated sexual acts (with or without penetration);

c. the indecent or obscene representation of a child, shall be guilty of the offence of using a child for pornographic purposes.

Explanation.- For the purposes of this section, the expression "use a child" shall include involving a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation and distribution of the pornographic material.

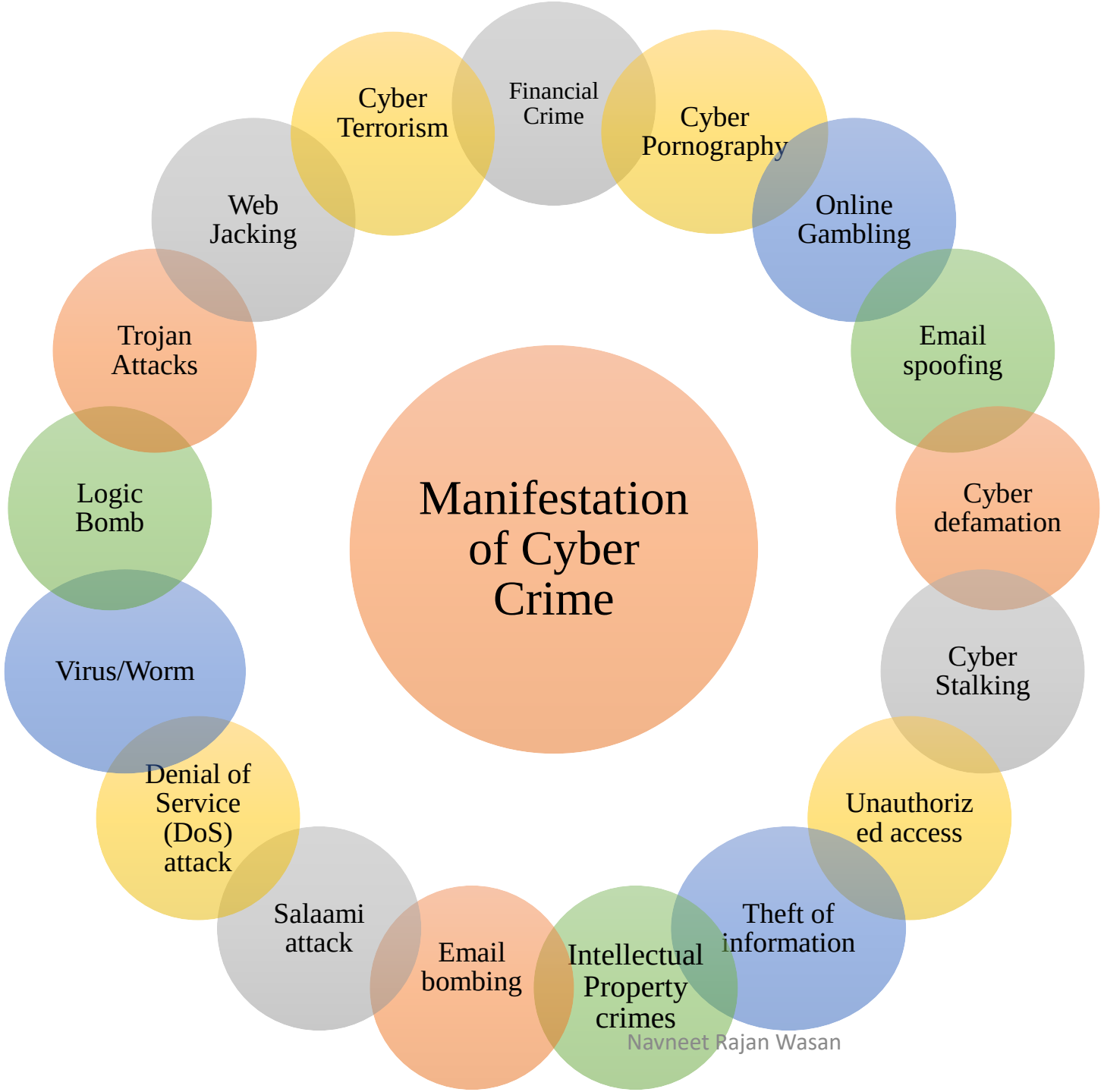
Protection of Children from Sexual Offences Act, 2012

14. Punishment for using child for pornographic purposes.-

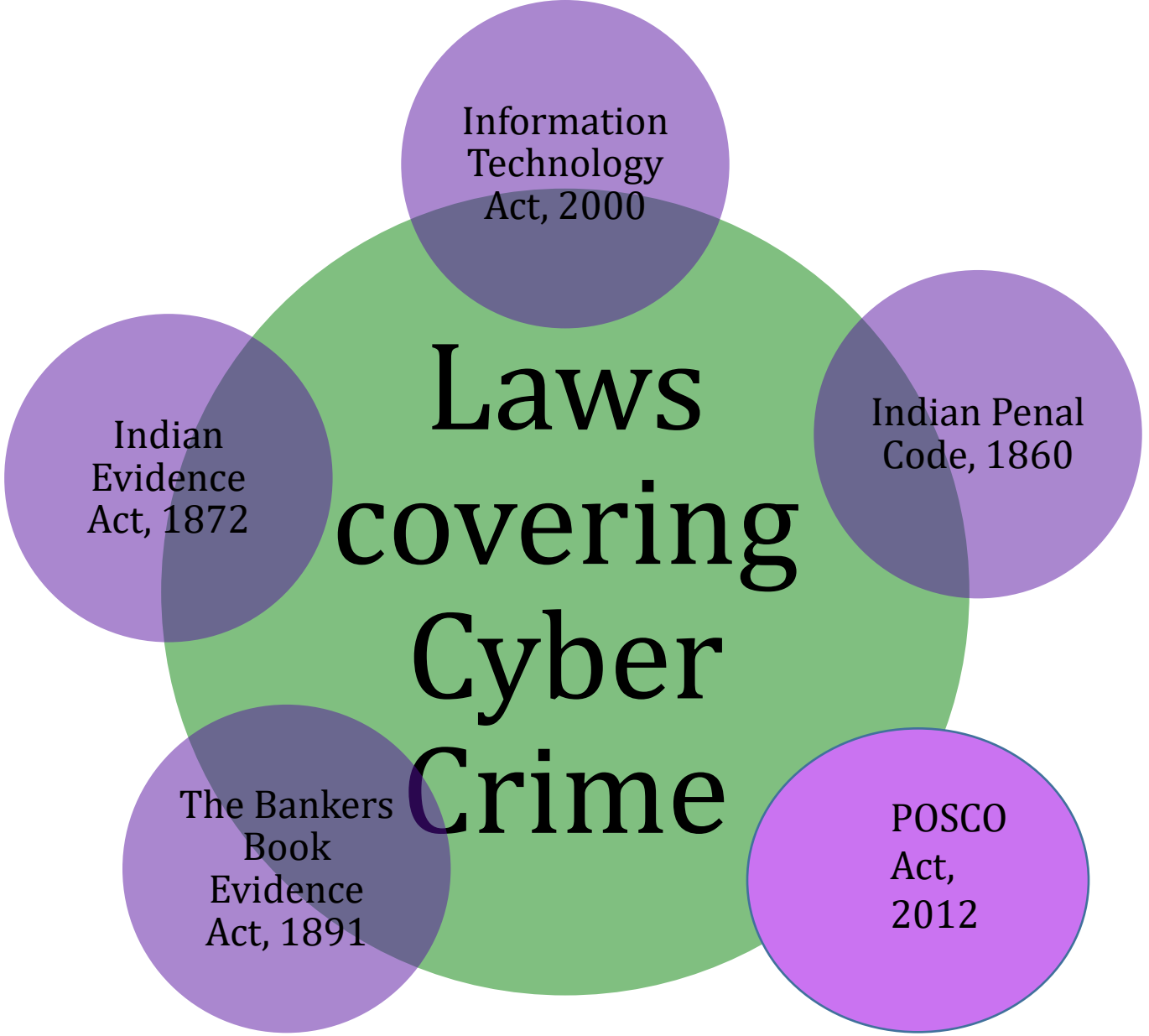
1. Whoever, uses a child or children for pornographic purposes shall be punished with imprisonment of either description which may extend to five years and shall also be liable to fine and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also be liable to fine.

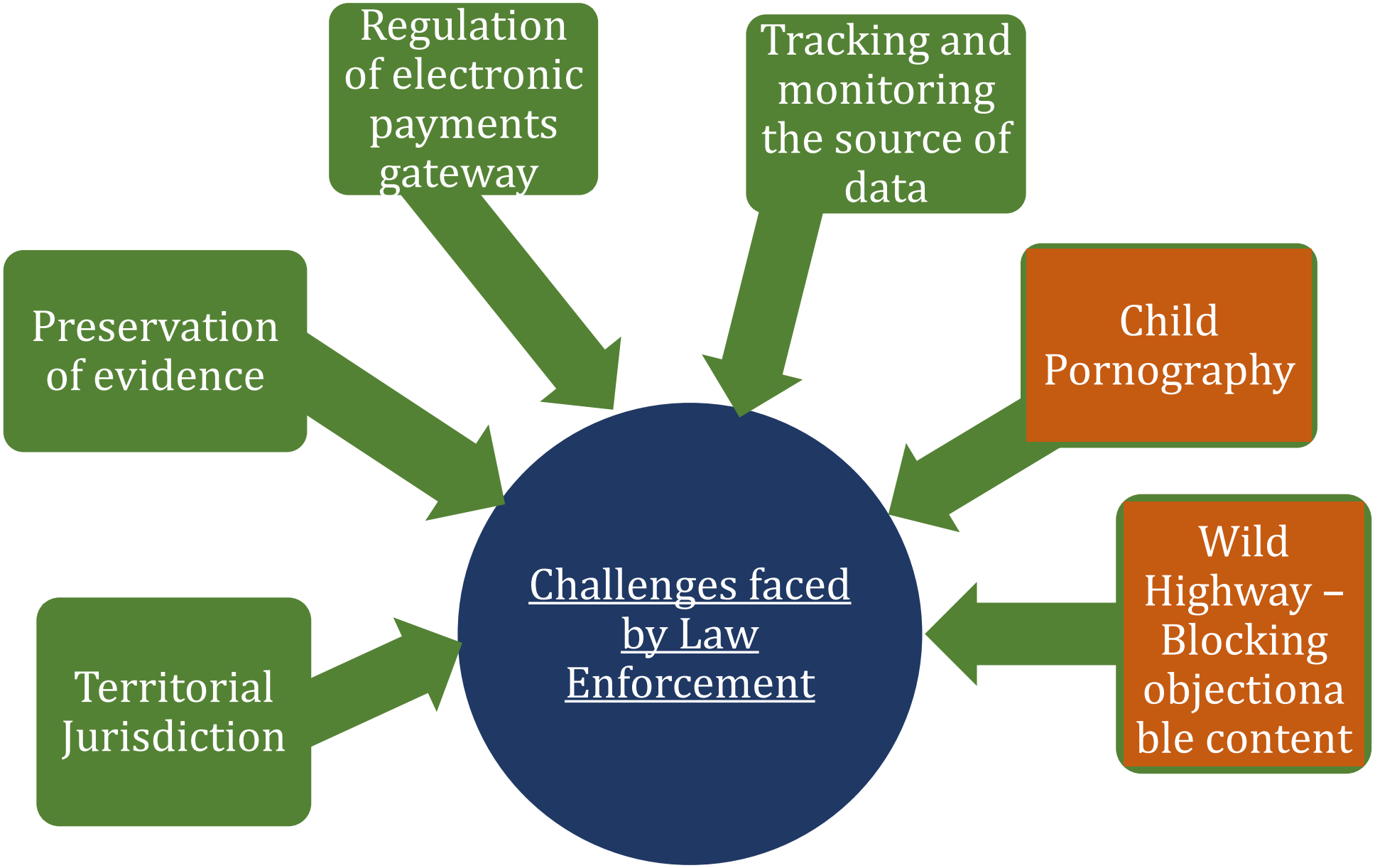
15. Punishment for storage of pornographic material involving child.-

Any person, who stores, for commercial purposes any pornographic material in any form involving a child shall be punished with imprisonment of either description which may extend to three years or with fine or with both.


Manifestation of Cyber Crime
Financial Crime
Cyber Pornography
Online Gambling
Email spoofing
Cyber defamation
Cyber Stalking
Unauthoriz ed access
Theft of information
Intellectual Property crimes
Email bombing
Salaami attack
Denial of Service (DoS) attack
Virus/Worm
Logic Bomb
Trojan Attacks
Web Jacking
Cyber Terrorism


INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008
The Information Technology (Certifying Authorities) Rules, 2000
The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000
The Information Technology (Use of Electronic Records and Digital Signature)Rules 2004
The Information Technology (Security Procedure) Rules,2004
The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public)Rules 2009
The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
The Information Technology (Intermediary Guidelines) Rules, 2011
Milestone Amendments/ Rules to Information Technology Act, 2000


Information Technology Act, 2000
Indian Evidence Act, 1872
Laws covering Cyber Crime
Indian Penal Code, 1860
The Bankers Book Evidence Act, 1891
POSCO Act, 2012


Regulation of electronic payments gateway
Tracking and monitoring the source of data
Preservation of evidence
Child Pornography
Challenges faced by Law Enforcement
Territorial Jurisdiction
Wild Highway – Blocking objectionable content

DIFFICULTIES FACED BY INVESTIGATORS

- **QUESTION OF JURISDICTION-BOTH NATIONAL & INTERNATIONAL**
  - INVESTIGATION IS STATE SUBJECT- CYBER CRIME RELATED CASE CAN BE REGISTERED BY LOCAL POLICE
  - THERE IS NO CENTRAL INVESTIGATION AGENCY WHICH CAN *SUO MOTU* REGISTER CASES HAVING INTERSTATE OR INTERNATIONAL RAMIFICATIONS
  - EXCEPTION BEING OFFENCES UNDER SECTION 66F OF INFORMATION TECHNOLOGY ACT
  - POWER GIVEN TO NIA TO REGISTER AND INVESTIGATE CASES OF CYBER TERRORISM
  - OTHER CASES CAN BE REGISTERED ONLY ON CONSENT OF THE STATE CONCERNED BY DSPE
  - COULD LEAD TO CRUCIAL DELAY LEADING TO LOSS OF EVIDENCE

DIFFICULTIES FACED BY INVESTIGATORS ON ACCOUNT OF JURISDICTION

- Cyber space being globally network of computers give rise to trans-jurisdictional barriers – the national boundaries have lost their meaning
- There is no consensus on sharing of information & evidence
- Information is difficult to get even for prevention
- Despite extra-territorial legal provision in IT ACT for criminal acts perpetrated in foreign jurisdictions, the practical application of this provision is almost impossible. Whilst an offender may be apprehended in one jurisdiction, the digital evidence required to progress an investigation may reside in another country

DIFFICULTIES FACED BY INVESTIGATORS ON ACCOUNT OF JURISDICTION

- Without a universal cyber crime convention, cross-jurisdictional conflict of criminal laws raises the unavoidable dilemma of “what law should be applied to determine the legal effect of a person's conduct when he does an act in one state which produces harmful effects in another”
- The inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime
- Rapid advancements in the functionality of information communication technologies (ICTs) are challenges for first responders, investigating authorities, forensic interrogators, prosecuting agencies, and administrators of criminal justice

DIFFICULTIES FACED BY INVESTIGATORS ON ACCOUNT OF JURISDICTION

- Managing dual criminality provisions for extradition, processing requests for mutual legal assistance (MLA), and balancing sensitive diplomatic relations are all significant encumbrances for investigations into cyber crime offending
- Maintaining evidence continuity can be complex as both stored and transmitted data may be retrieved from disparate points of origin within cloud computing infrastructures (i.e., trans-border data-flows, distributed file systems, data backup and replication/synchronization, etc.) which affects the legal provisions governing data access and disclosure.
- Public cloud deployment within multi-tenanted infrastructure can present a minefield of privacy and technical issues for investigators

DIFFICULTIES FACED BY INVESTIGATORS ON ACCOUNT OF JURISDICTION

- **Budapest Convention on Cybercrime or Convention on Cybercrime is not universally accepted- India is not a signatory to the convention**
- *United Nations Convention against Transnational Organized Crime* (2000) and its three protocols
- *Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism* (1999)
- In order to address trans-jurisdictional cyber crime offending, international legal frameworks must be harmonized. However, enacting legislation and ratifying treaties is a slow process compared to the rapid uptake of new technologies by nations globally
- Many cyber crimes are sophisticated and well-conceived, requiring police to apply technological expertise and deductive reasoning to unravel complex *'modus operandi'* and substantiate elements of an offence

DIFFICULTIES FACED BY INVESTIGATORS ON ACCOUNT OF JURISDICTION

- LOGISTICAL & PRACTICAL BARRIERS
  - DIFFERENT TIME ZONES
  - NO AGENCY TO AGENCY CONTACT POSSIBLE – INTERPOL CHANNELS MAY NOT WORK
  - LANGUAGE DIFFICULTY
  - DIPLOMATIC REQUIREMENTS MAY CREATE HURDLE
- IDENTIFYING SUSPECTS- A DIFFICULT PROCESS
  - COMPUTING RESOURCE USED FOR COMMITTING CRIME MAY BE DIFFERENT OR LOCATED IN DIFFERENT PLACE
  - COULD HAVE BEEN ACCESSIBLE TO ANYONE
  - IDENTITY CAN BE EASILY DISGUISED

DIFFICULTIES FACED BY INVESTIGATORS ON ACCOUNT OF JURISDICTION

- SEARCH & SEIZURE- A DIFFICULT TASK
  - TIMELY PHYSICAL SEARCH OFTEN NOT POSSIBLE
  - INTERCEPTION/ MONITORING OF DATA FOR THE PURPOSE OF SEARCH IS DIFFICULT IN CASE THE COMPUTING RESOURCE IS LOCATED OUTSIDE THE JURISDICTION
  - STRONG ENCRYPTION OF DATA/ INFORMATION BY CRIMINALS POSES A BIG CHALLENGE IN DECIPHERING THE SEIZED INFORMATION
  - INTERCEPTING NETWORK TRAFFIC AND SEIZING DEVICES IS OFTEN A FRUITLESS EXERCISE WHEN A SUSPECT HAS IMPLEMENTED ROBUST ENCRYPTION ON DISKS AND HANDSETS FOR DATA AT REST, IN CONJUNCTION WITH ENCRYPTED CHANNELS OF COMMUNICATION FOR DATA IN TRANSIT

NEED OF THE HOUR

- United Nations globally accepted Convention/ Protocols for sharing information & evidence
- Only tools available to investigator to gather information in through a tedious route of Letters Rogatory-either under MLAT or based on principals of reciprocity
- India does not have a law governing Mutual Legal Assistance in Criminal Matters

NEED OF THE HOUR

- In order to bring in professionalism and improve the collection of evidence from outside India and to cut down delays, there is an urgent need to revamp the Central Authority to be manned by experts.
- Concept of **Joint Investigation** may be introduced in Code of Criminal Procedure
- Set up national mission in cyber forensics to facilitate collection of evidence against cyber criminals and cyber terrorists
- Training of law enforcement personnel/ prosecutors/ judicial officers

WHO: Mphasis BPO Fraud: 2005

- **What**
  - Four call center employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.

When

- In December 2004

How

- These employees were not authorized to obtain the PINs. In association with others, the call Centre employees opened new accounts at Indian banks using false identities.

Impact

- The Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen.

Who: Major Telecom Firms Worldwide

What

- State-backed Chinese hacker group APT41
- Retrieved call records and intercepted text messages from telecom carriers' customers, including "high value" targets

When

- Disclosed on August 07, 2019
- Published on October 31, 2019

How

- A malware named MESSAGETAP was installed on Short Message Service Center (SMSC) servers at telecom operators, allowing monitoring of all network connections. SMSC are typically Linux servers that route, store and forward SMS
- 64-bit data miner uses libpcap to listen to all traffic on Ethernet and IP protocols, using parsers to extract SMS data from protocols such as SCTP, SCCP and TCAP
- Using ISMI and other filters, the malware dumps data of interest to a local CSV file
- Queries Call Detail Record (CDR) to pull details about calls of interest

Impact

- MESSAGETAP can intercept all SMS messaging traffic, which includes the content of the messages; their cellphones' unique identifiers, known as international mobile subscriber identity (IMSI) number; and the source and destination phone numbers.
- Malware filtered keywords and names of high value targets, especially high-ranking officers and government officials
- APT41 has been persistent in establishing access to telecom carriers worldwide since 2017, treating such access as a crucial first step to establish foothold in targeting a region

Who: Facebook

What

- 419 million records over several databases on users across geographies (US, UK, Vietnam and others)
- Affects all Android and iOS game users who installed the game prior to September 2, 2019

When

- Reported on September 04, 2019
- Data may have been older since data dump included phone numbers and Facebook imposed limitations to public access to phone numbers a year ago

How

- Initial data exfiltration source unknown, possibly data scrapping attacks similar to what were previously used
- Server databases did not require authentication, so the databases were open to access by anybody

Impact

- Stolen information includes the PII such as
  - Phone numbers
  - UIDs
  - Location, Country
  - Name
  - Gender
- Exfiltrating phone numbers and their associated user IDs is particularly useful for executing SIM swapping attacks, which enables attackers to then force password resets for that user / identity across many internet accounts associated with that number, including financial accounts.

Who: Nuclear Power Corporation of India Ltd

What

- Administrative network at Kudankulam Nuclear Power Plant operated by NPCIL infected by DTrack RAT virus
- The DTrack RAT is a malware that originated from the North Korean backed Lazarus Group, supposedly also responsible for cyber crimes such as WannaCry ransomware

When

- Discovered on September 4, 2019
- Confirmed on October 31, 2019

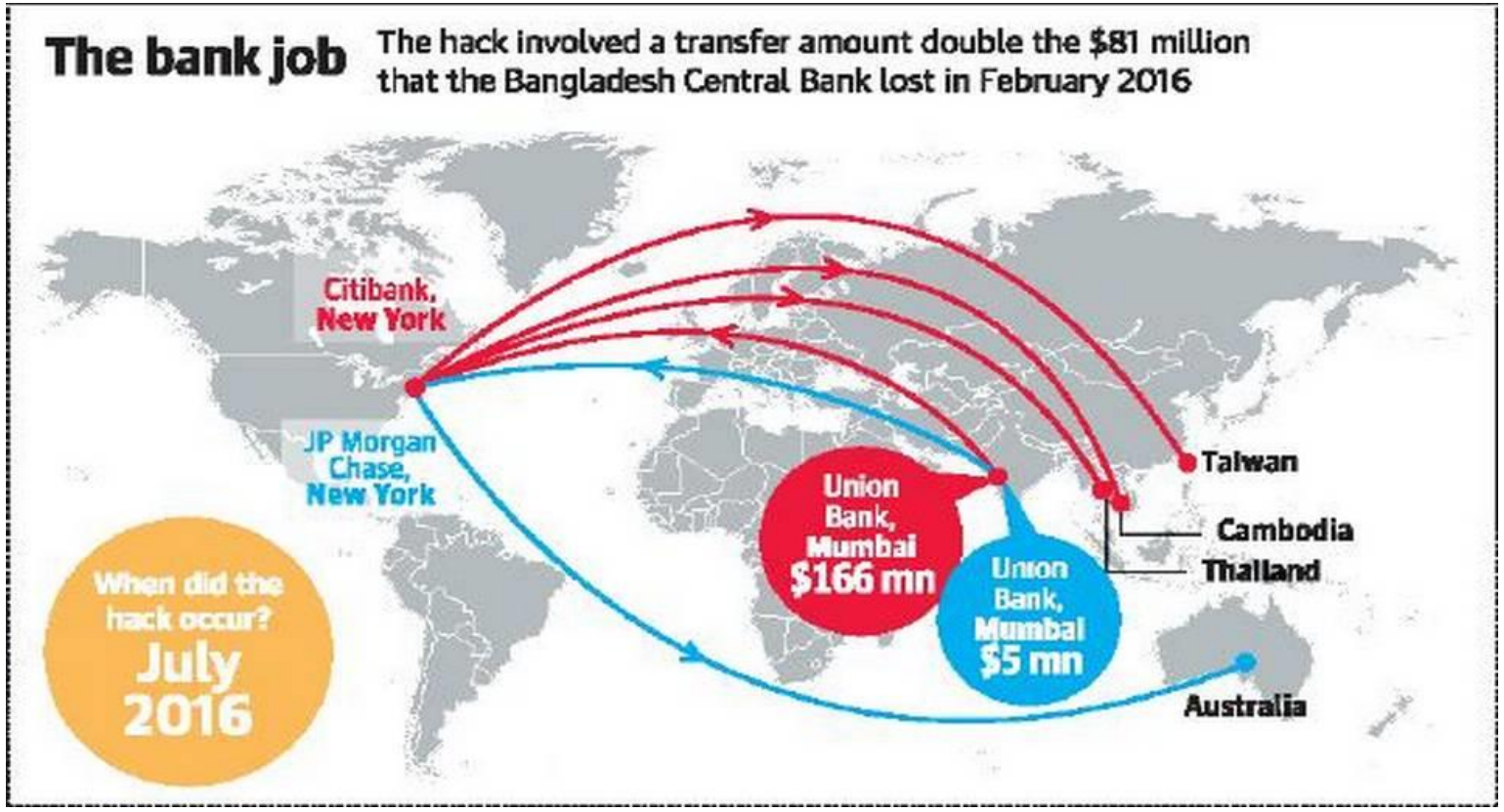
How

- Preliminary investigation indicates that “the infected PC belonged to a user who was connected to the Internet-connected network used for administrative purposes.”
- Critical network reported to be isolated and not currently impacted

Impact

- The e-Procurement portal of the government has been suspended for six days which impacted rolling out of new tenders and issuance of refunds for legitimate tenders which was successfully functioning for the eight years.

Who: Union Bank of India



Courtesy : The Hindu

What

- One of the “not-so-tech-savvy" Union Bank officials fell prey to the phishing email and clicked on the link which released the malware that went viral on the bank’s servers.

When

- Discovered on July 21, 2017

How

- An unidentified hacker was attempting to swindle us of $171 million (about Rs1,100 crore at today’s rates) from our Nostro account." A Nostro account is an account that a bank holds in a foreign currency in another bank.
- The money had found its way to accounts in two banks in Cambodia—the Canadia Bank Plc and RHB IndoChina Bank Ltd, besides the Siam Commercial Bank in Thailand, Bank Sinopac in Taiwan, and a bank in Australia. These funds were routed by Citibank New York and JP Morgan Chase New York, which hold UBI’s foreign exchange accounts.

Impact

- The e-Procurement portal of the government has been suspended for six days which impacted rolling out of new tenders and issuance of refunds for legitimate tenders which was successfully functioning for the eight years.