CYBER CRIME
ADVANCES & BOTTLENECKS

PRESENTED BY

DR. HAROLD D'COSTA

CEO - Intelligent Quotient Security System,

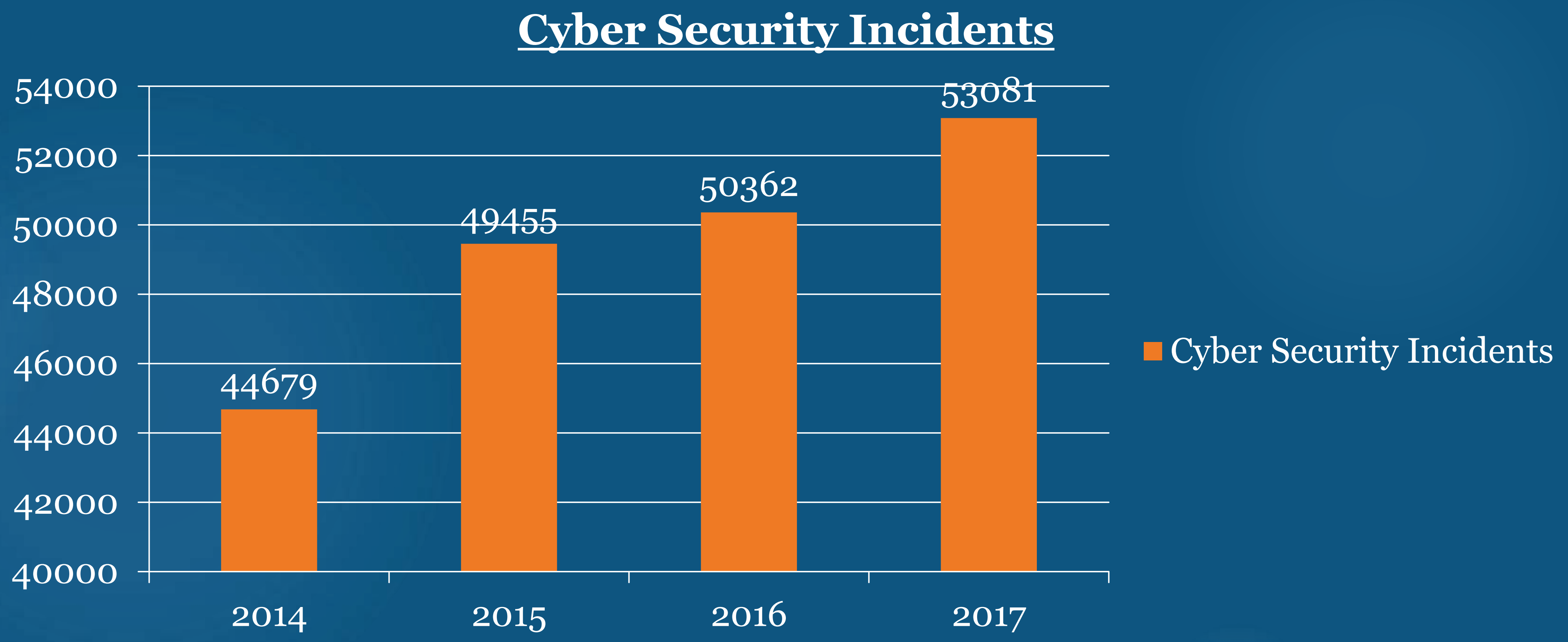
President - Cyber Security Corporation,

Advisor (Law Enforcement Agencies - Cyber Crime),

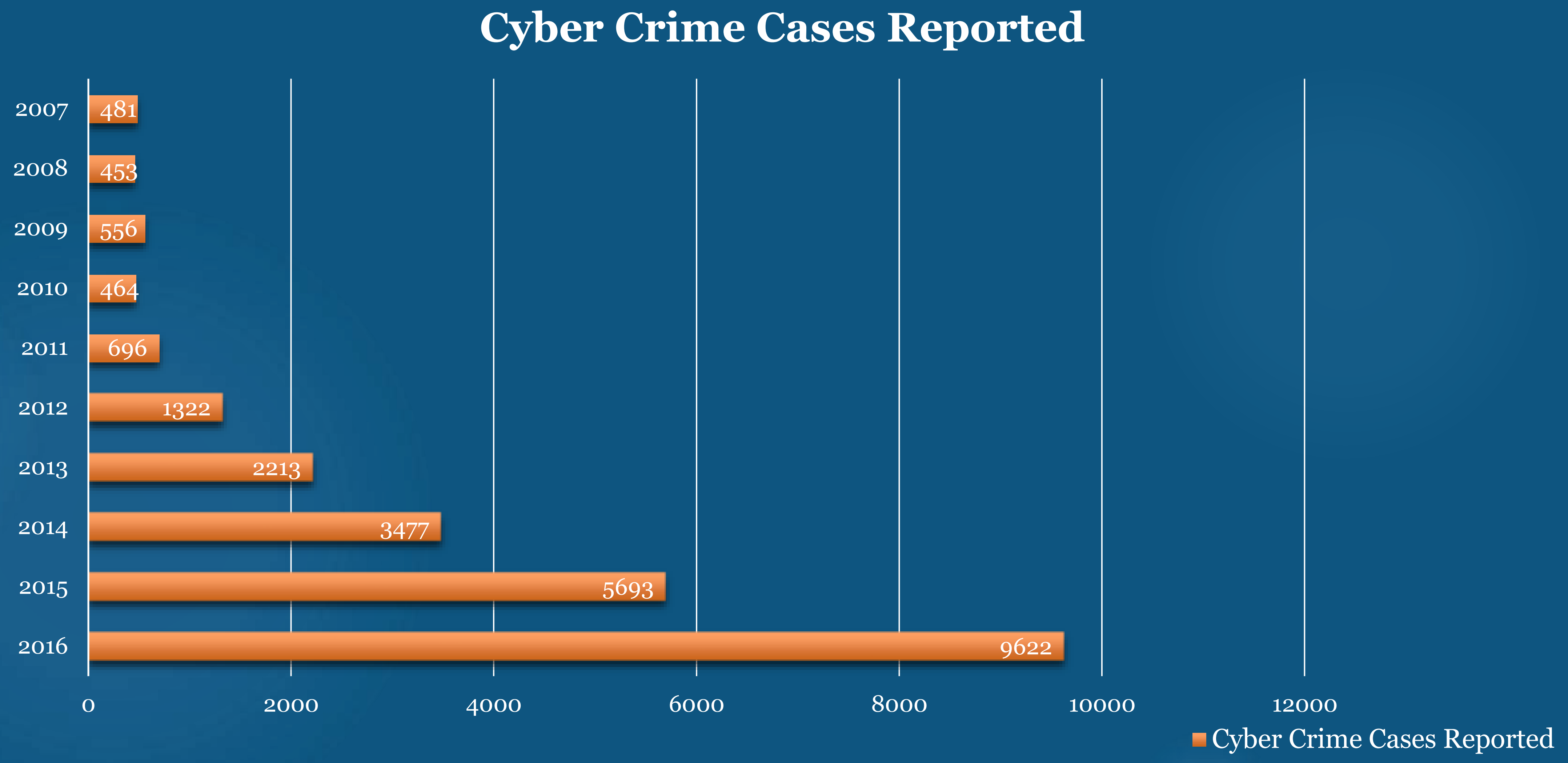
Sr. Trainer (Judges & Public Prosecutors),

Office No 5, 3rd Floor, Anandi Gopal Building,
Fergusson College Road, Pune - 411005, India
Email: hld@rediffmail.com
Cell: +91-9637612097
Website: https://cybersecuritycorp.in

CYBER SECURITY INCIDENTS – CERT IN



Cyber Crimes Over a Decade in India

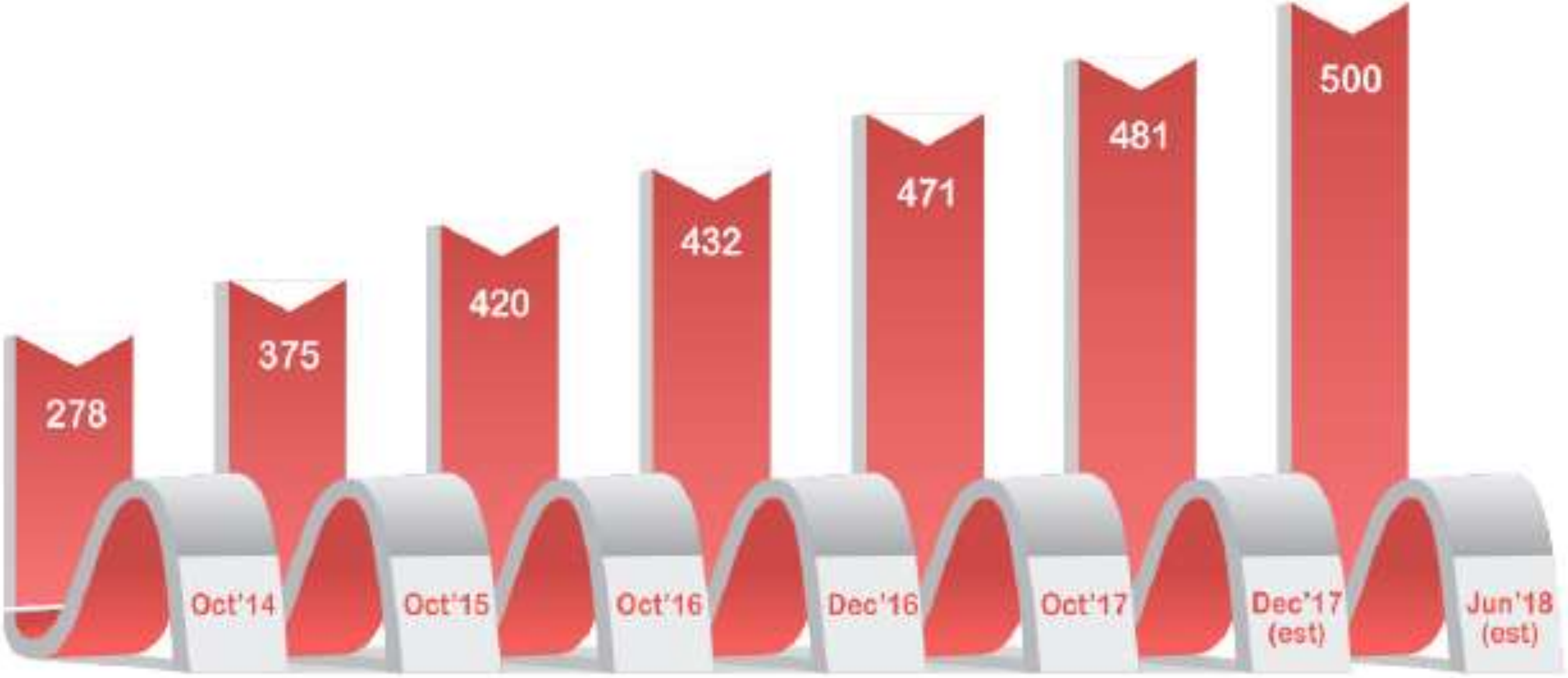


Increased use of Internet

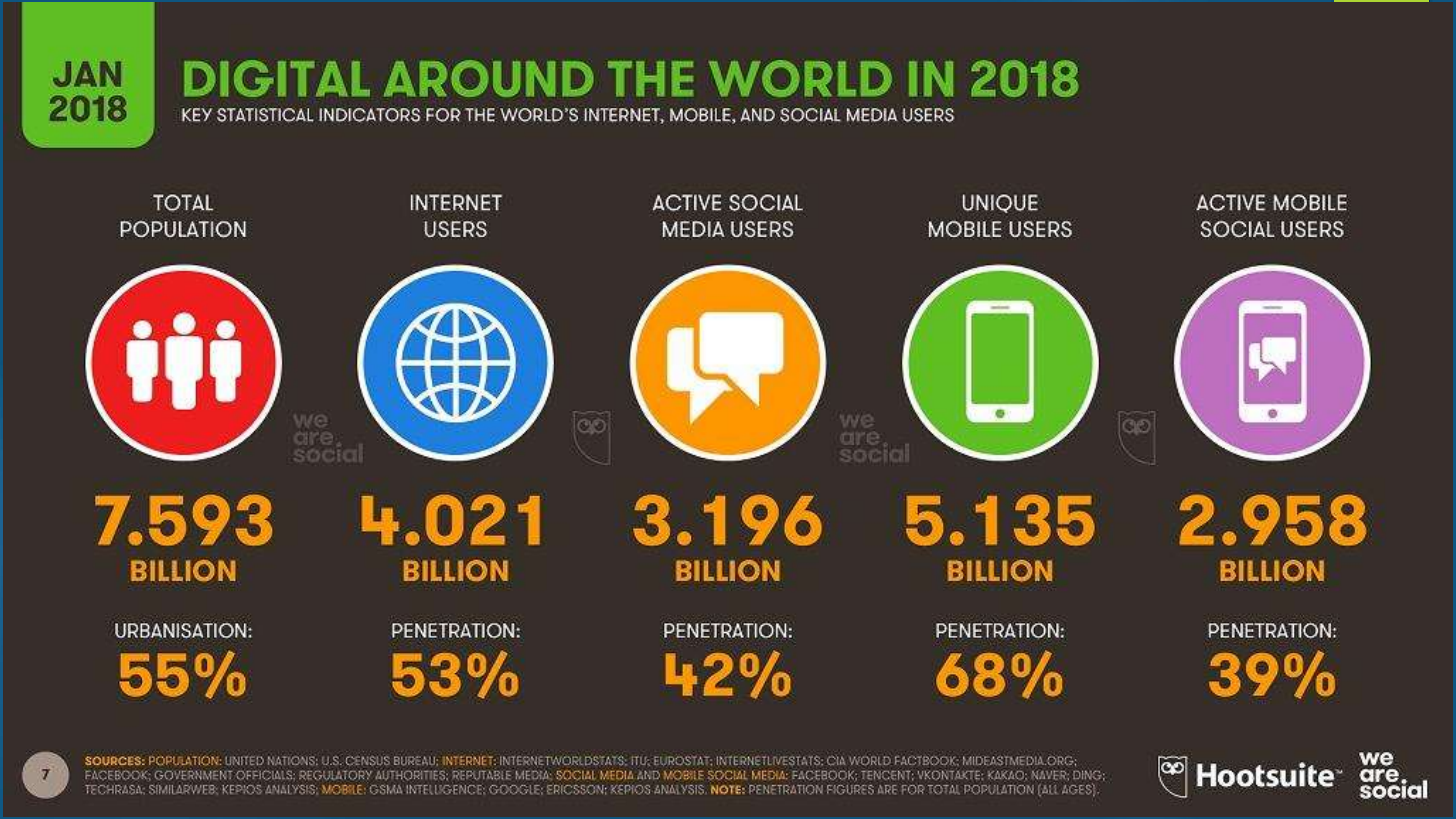
With increasing mobile and internet penetration in the country, cyber crimes have also increased proportionately. Between 2012 and 2016, more than 32,000 cyber crimes were reported across the country.

More than 24,000 of these cases are registered under the IT Act 2000 and the remaining under the various sections of IPC and other State Level Legislations (SLL).

Internet Users (in MN)



Source: IAMAI & Kantar IMRB I-CUBE 207, All India Users Estimates, October 2017



JAN 2018

DIGITAL AROUND THE WORLD IN 2018

KEY STATISTICAL INDICATORS FOR THE WORLD'S INTERNET, MOBILE, AND SOCIAL MEDIA USERS

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
7.593 BILLION	4.021 BILLION	3.196 BILLION	5.135 BILLION	2.958 BILLION
URBANISATION: 55%	PENETRATION: 53%	PENETRATION: 42%	PENETRATION: 68%	PENETRATION: 39%

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; MOBILE: GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. **NOTE:** PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).

Types of Cyber Crime

Cyber Stalking

Cyber Contraband

Cyber Trespassing

Cyber Laundering

Cyber Vandalism

Cyber Defamation

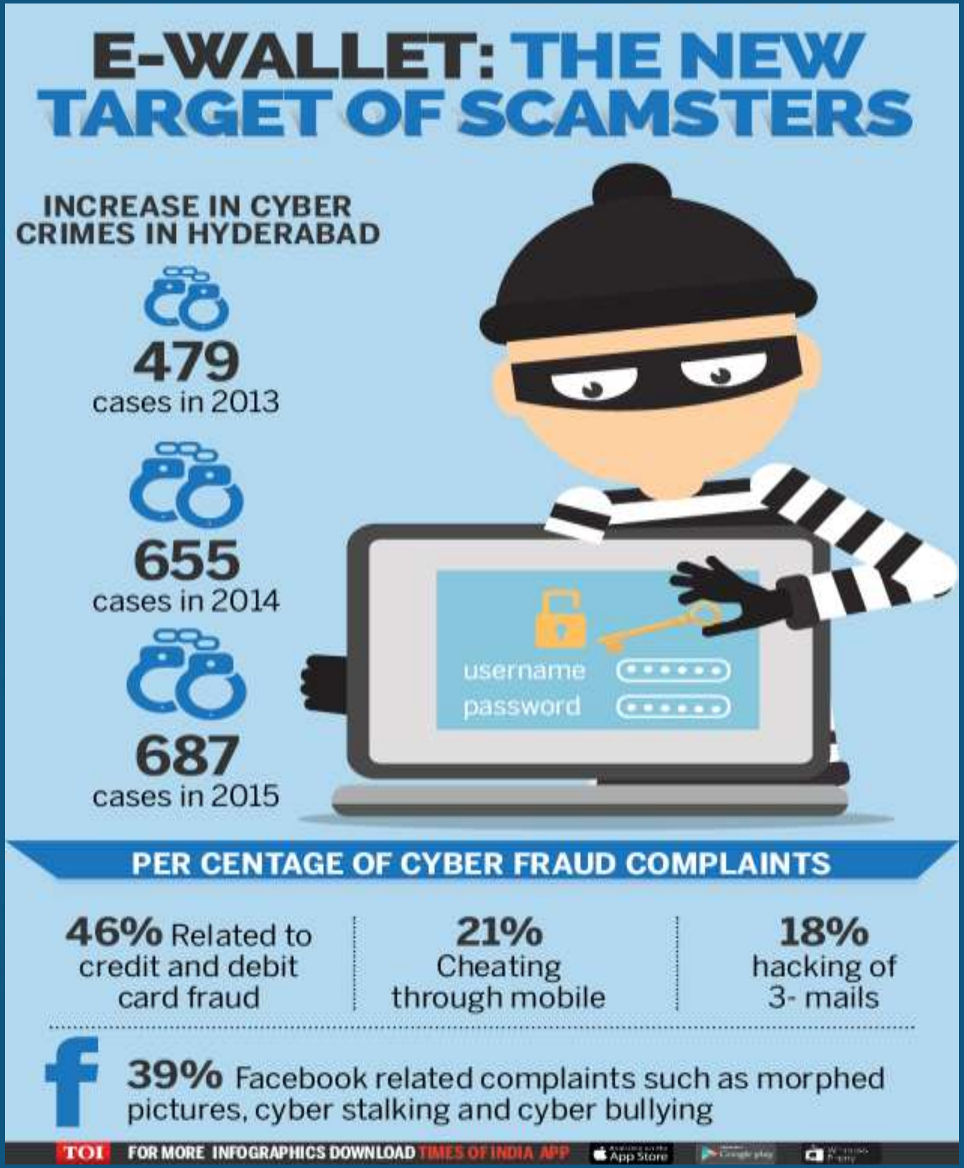
Cyber Theft

Cyber Terrorism

Cyber Pornography

Cyber Fraud

Indian States And Cyber Crime Incidences



E-WALLET: THE NEW TARGET OF SCAMSTERS

INCREASE IN CYBER CRIMES IN HYDERABAD

479 cases in 2013

655 cases in 2014

687 cases in 2015

PER CENTAGE OF CYBER FRAUD COMPLAINTS

46% Related to credit and debit card fraud

21% Cheating through mobile

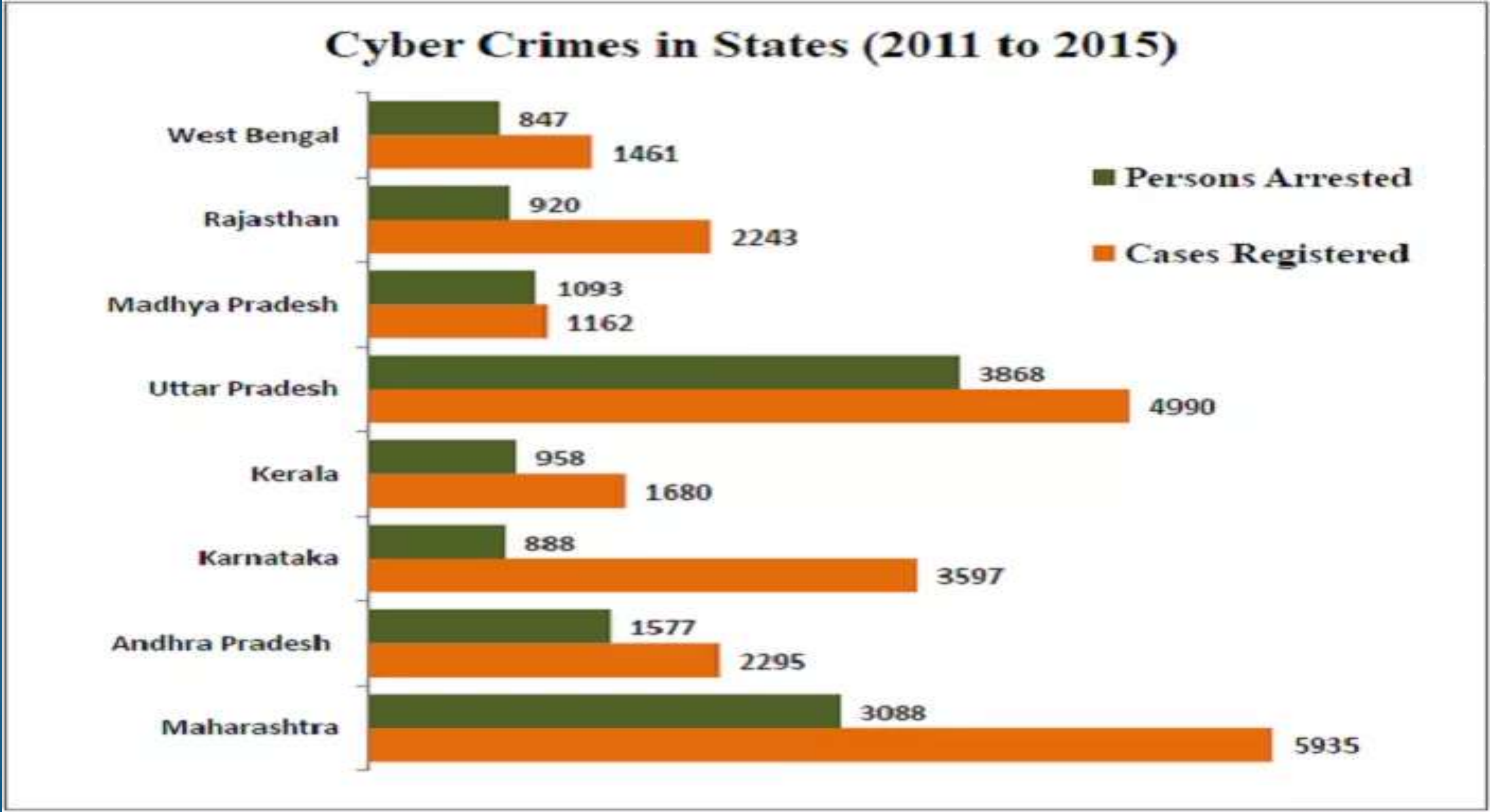
18% hacking of 3- mails

39% Facebook related complaints such as morphed pictures, cyber stalking and cyber bullying

TOI FOR MORE INFOGRAPHICS DOWNLOAD TIMES OF INDIA APP

As of December 2016

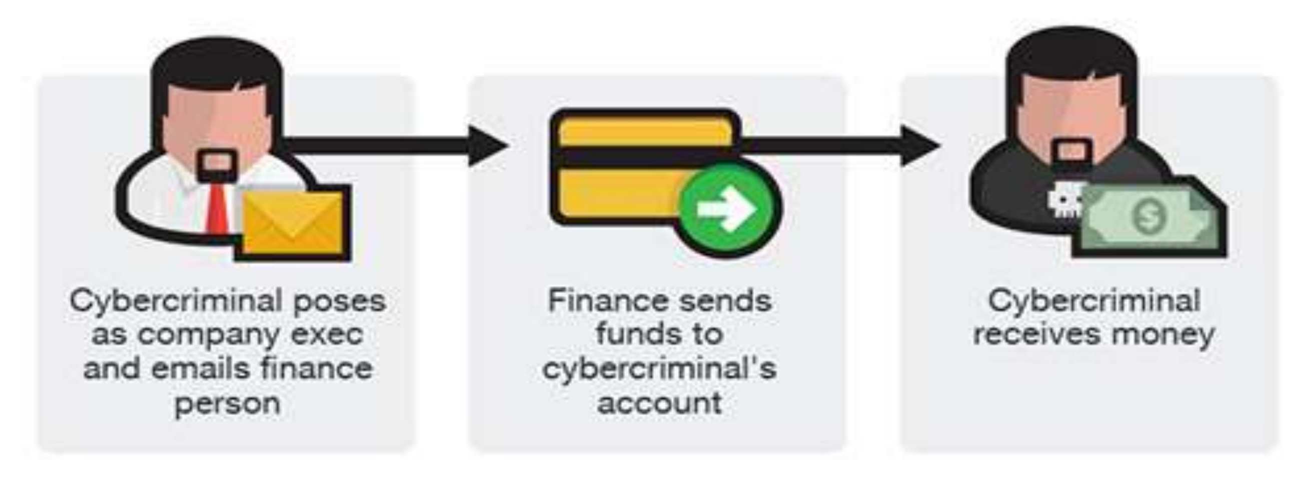
Indian Statistics

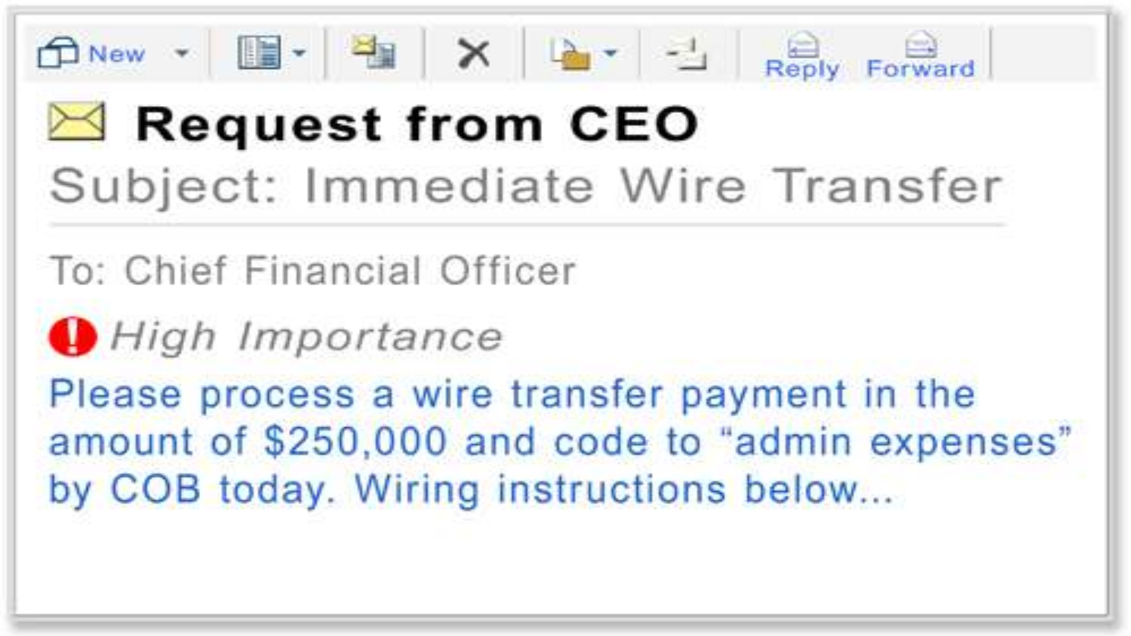


Business E-mail Compromise

- Cyber-criminals are like every businessman:

They want maximum profit for minimum investment. A recent trend amongst hackers to help achieve this goal is Business Email Compromise (BEC) also known as "CEO Fraud". This type of scam is very profitable since it only needs to be successful a few times to be highly cost-effective for the criminals.


Cybercriminal poses as company exec and emails finance person
Finance sends funds to cybercriminal's account
Cybercriminal receives money



Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

❗ *High Importance*

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

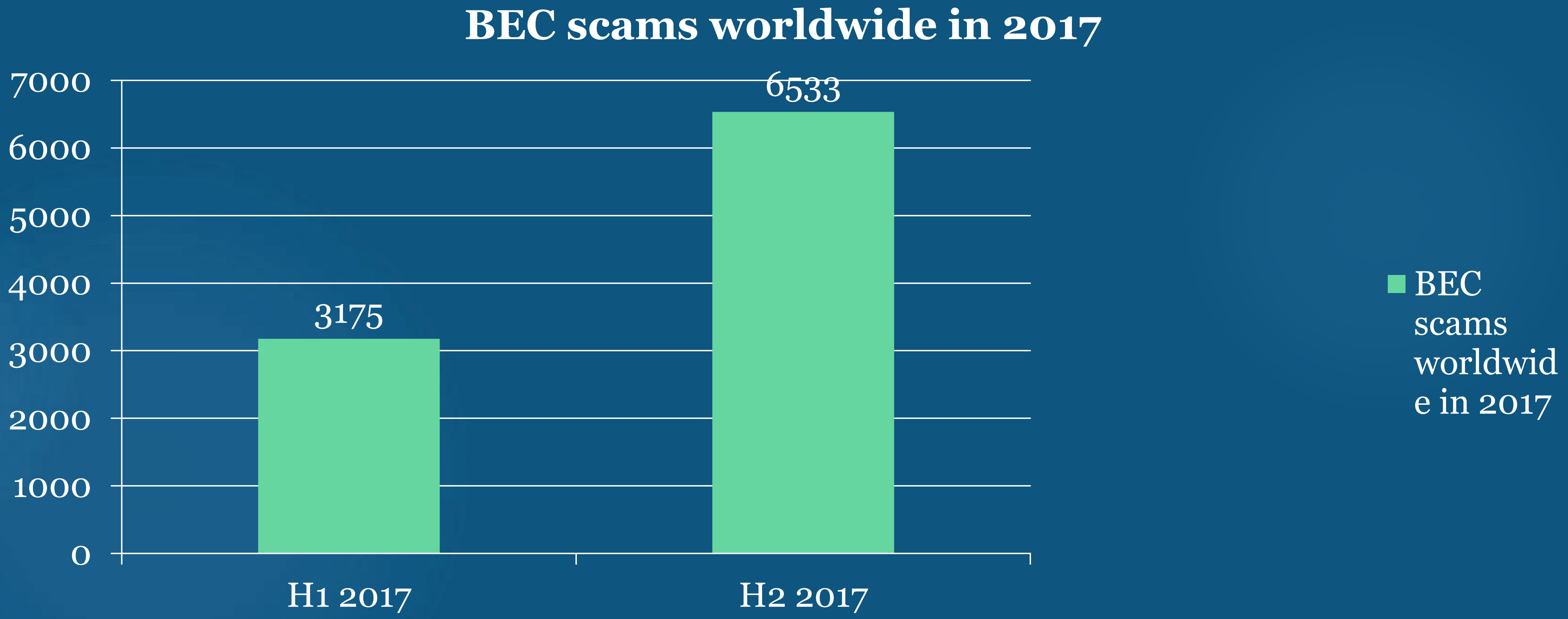
Cyber Security Cor

Data of Number of Cases Affected by BEC in India - 2017

- Over 180 Indian Companies were affected with Business Email Compromise (BEC) Schemes.

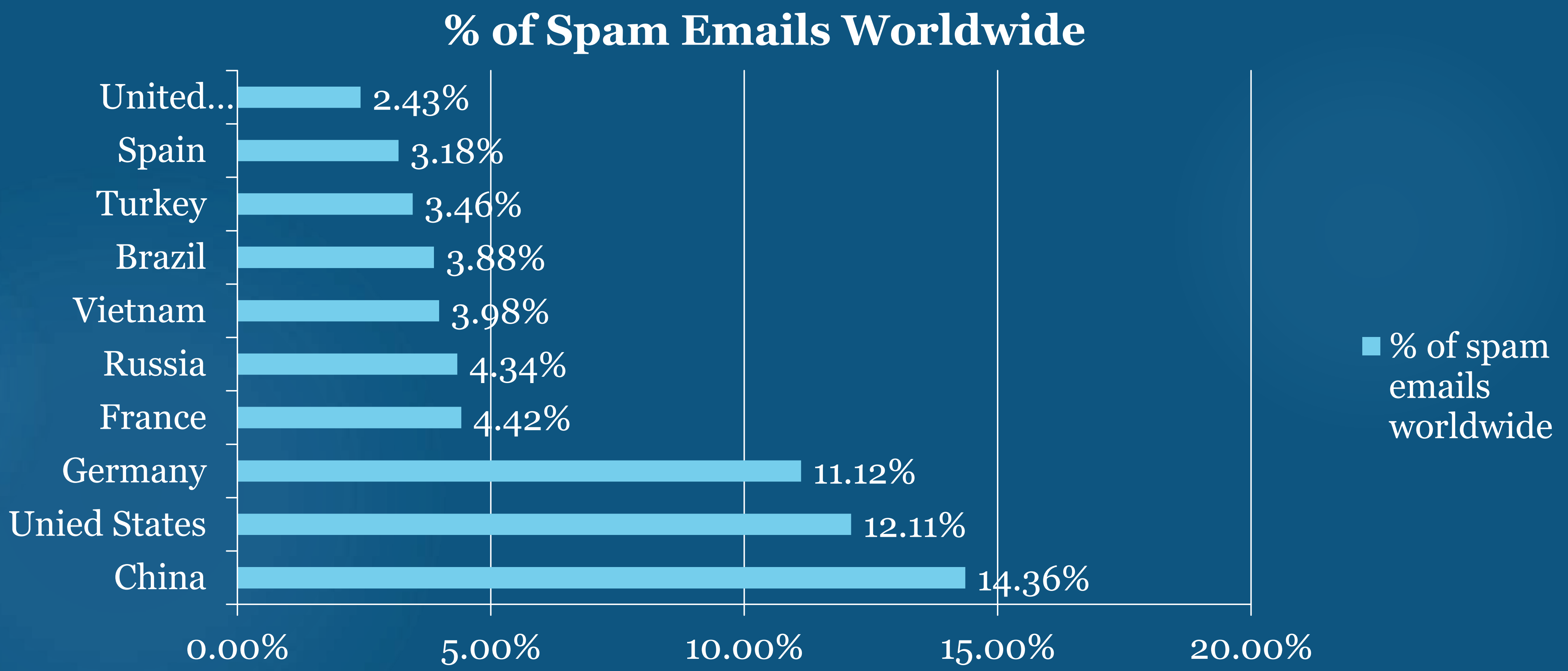
- Globally, Business Email Compromise (BEC) scams targeted over 400 businesses per day in 2017, draining $3 million over the last 3 years.

BEC Scams Worldwide in 2017



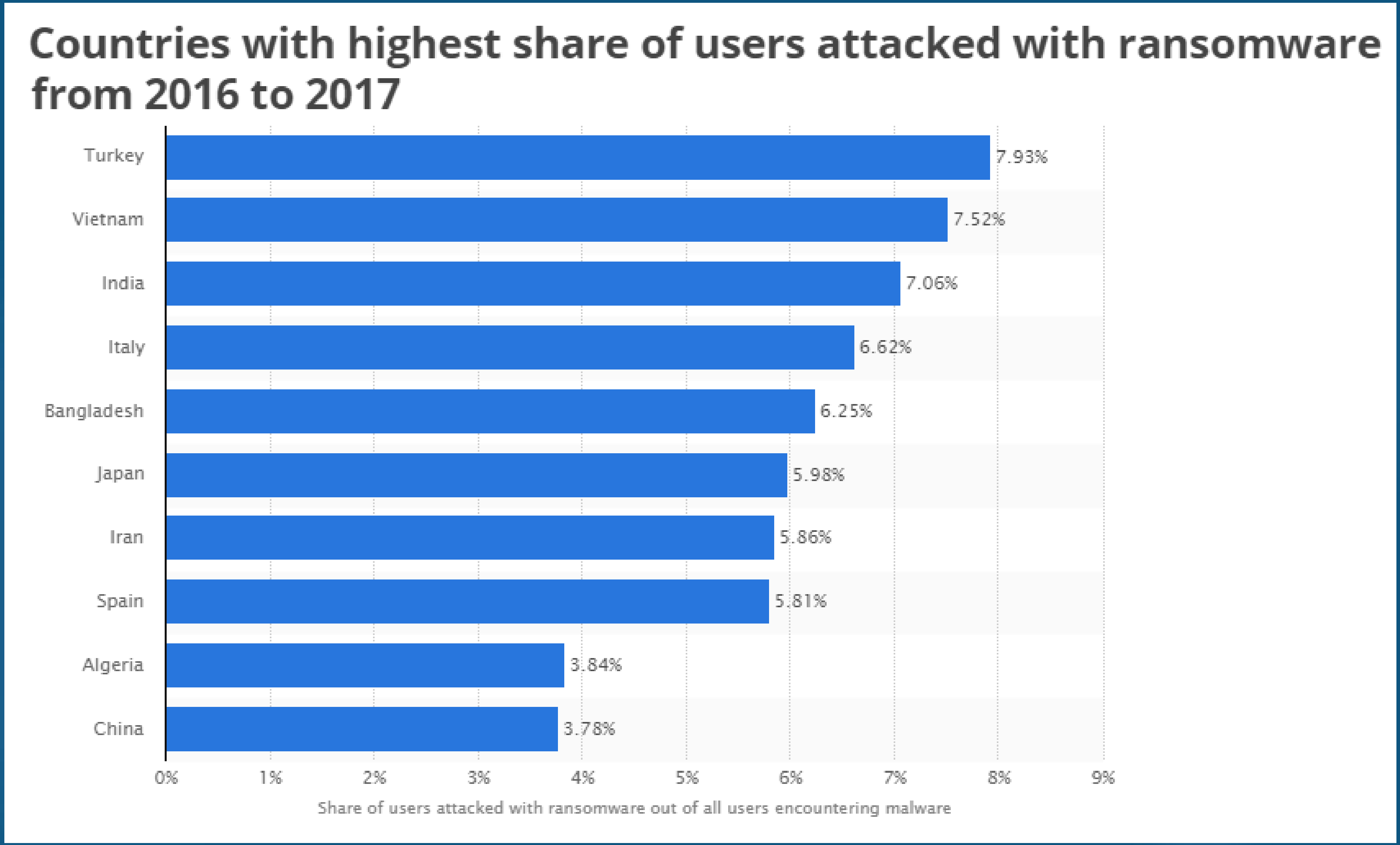
Source: https://www.statista.com/statistics/820912/number-of-attempts-of-bec-scams-ceo-fraud/

Unsolicited Commercial Email in Q2-2018



Source: https://www.statista.com/statistics/263086/countries-of-origin-of-spam/

Ransomware Attacks

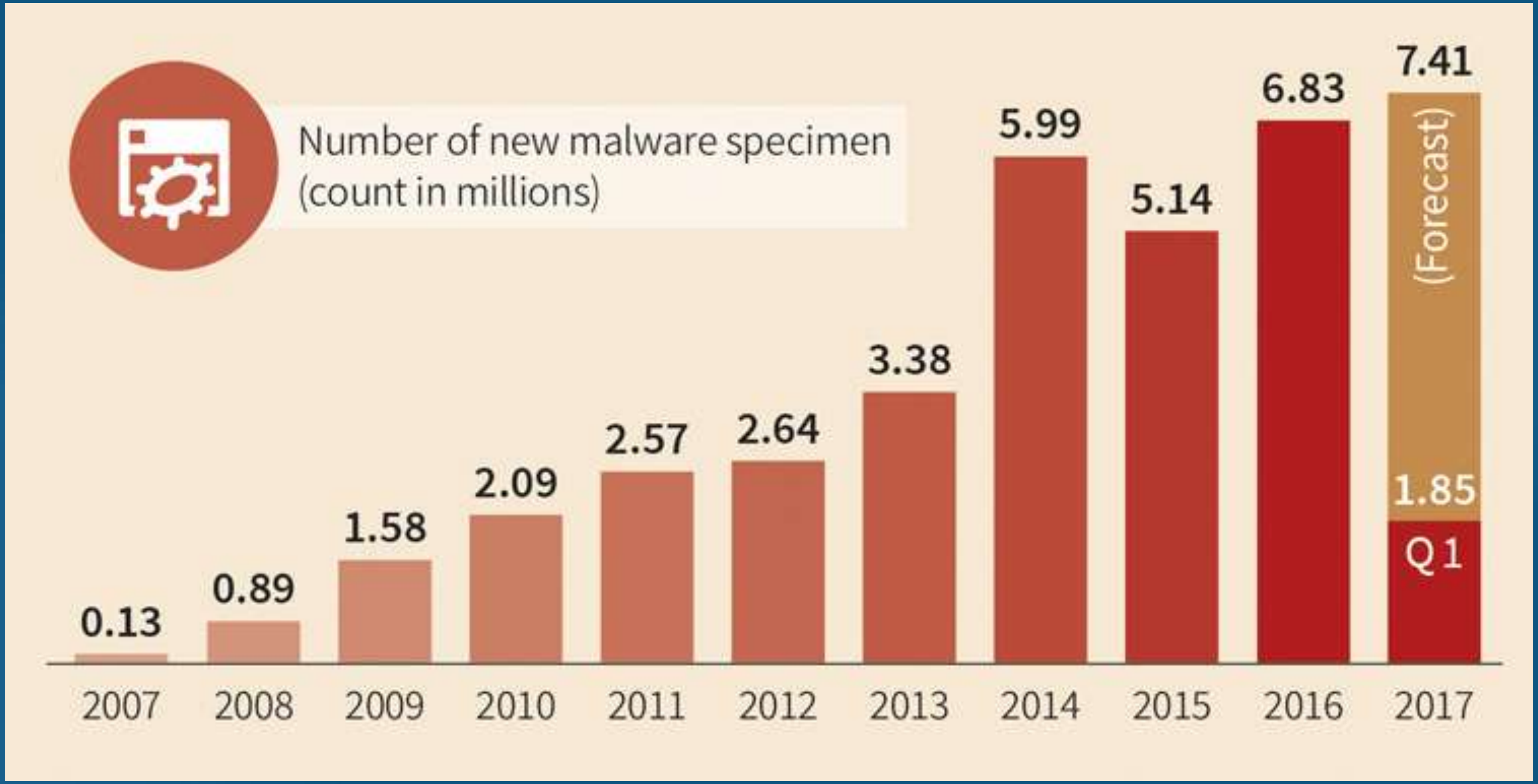


Countries with highest share of users attacked with ransomware from 2016 to 2017

Ransomware

Both new and old variants caused a total of US $209 million in monetary losses to enterprises. Ransomware attacks found in the first half of 2016, like BEC scams, originated from emails 58 percent of the time.

Number of New Malware Specimen



Source: https://file.gdatasoftware.com/_processed_/c/9/GDATA_Infographic_New_Malware_Types_Years_EN_RGB_78643w753h3

Cyber Security Corporation | Pune © 2019

Modus Operandi - Targeted Victims

- Victims are not limited to a certain business type:

Hackers are targeting medium and large corporations, small businesses, not-for-profit organizations, etc... They always have one characteristic in common: the victim's business must work with foreign suppliers and/or regularly use wire transfer payments.

Other Modus Operandi

- The business email compromise (BEC) scams are also referred to as “whaling” because they send spear-phishing emails to senior (usually C-level) employees. In the majority of emails which researchers have observed, the attackers send the message to the chief financial officer (CFO).

- The scammers send the first email, asking the CFO if they can carry out an urgent wire transfer. If the recipient responds, the attackers send a follow-up email with the necessary details for the wire transfer. If there’s no response, the scammers may send a second email to the CFO or they may try to target another member of the finance organization. Information about these individuals can be easily gleaned from LinkedIn.

CONTINUED...

- The cyber criminals may also pretend to be a business partner and ask the company to send funds to a new bank account (the fraudulent bank account) by indicating that due to administrative need or tax or audit purposes, they have used a new bank account to receive money for business transactions.

- Upon reaching the criminals' bank account, the funds are quickly transferred through a number of additional bank accounts to frustrate any attempts to freeze or trace the funds.

Company Email ID gets Hacked leading to Massive Monetary Loss

- A chemical company in India was trading with neighbouring companies for the raw materials they needed for the production of metals. the trading was going on with the same suppliers for a number of years. The supplier would release the order on payment of 20% of the total amount and the remaining 80% was paid after the delivery of the resources. communication used to take place on e-mails.
- After a span of time the companies used to take money but not send the material giving very acceptable reasons to the Indian party for the same. In this way the company paid around rupees 2 crores but never received their delivery. The Indian company tried contacting them but they never responded.
- On investigating it was found that the email Id of the trading partner of the Indian company from which conversations used to take place was hacked and was conversing with the company with a wrong intention of extorting money.
- It was found that as soon as the message used to come in the traders inbox it was directed to the hacker and get deleted from the original inbox. The hacker used to make changes and talk to the company as the trader.

Online Job Scam referring as the CEO of an International Company

- An Indian citizen residing and working with a reputed organization in Baroda , a city in India applied for a job on an online job portal. Shortlisted for the job in a company in Australia he was sent offer letter and contract letter from the company CEO and HR with the exact same logo and name of the company.
- The company then asked the victim to pay money for different purposes like Visa Processing fees, Anti Terrorist Certificate, Joining amount, etc which summed up to a massive amount of around 2,75,80,210 INR.
- A doubt in mind he contacted the investigation agency and found out that it was a pure online job scam and he was cheated and lost his hard earned money.

Recent Trends in Cyber Security

Biometric Hacking, an increase in phishing attacks and sophisticated use of artificial intelligence (AI) are among the top cyber security threats to be expected in 2019, as attackers stop at nothing to steal identities and evade detection through new techniques.

CONTINUED...

Attacks through Theft of Biometric Data

- As more biometric systems for user identification and authentication are being implemented by various financial institutions in META (Middle East, Turkey and Africa), 2019 will see criminals exposing vulnerabilities in passcodes, touch ID sensors and facial recognition.

CONTINUED…

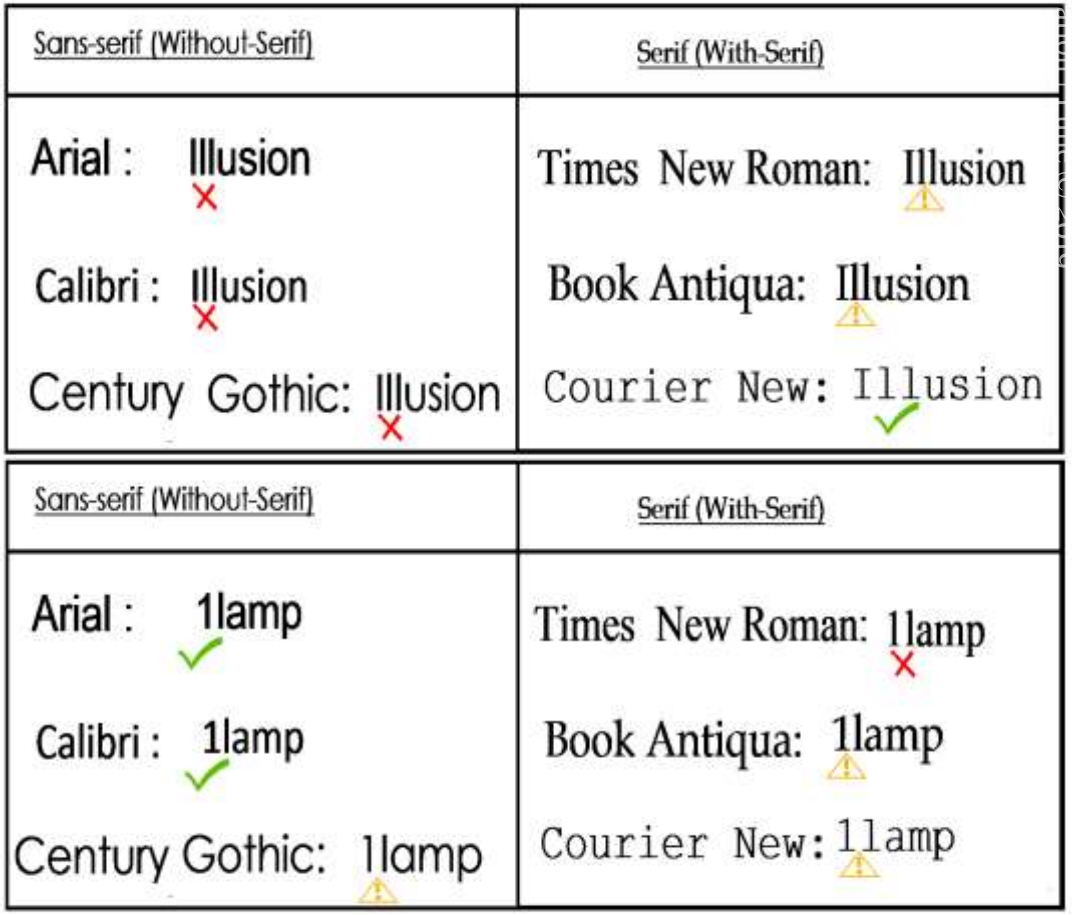
- **AI and Machine Learning make Attacks Harder to Detect**

  - AI and machine learning will play a more prominent role as the velocity and variety of attacks makes conventional approaches - such as blacklists - outdated and ill-equipped to deal with modern cyber threats.

CONTINUED...

Phishing Scams to Soar

- Phishing techniques like the use of homoglyphs (similar characters for e.g. 0 and O, number 1 and lower case alphabet l), elongated URLs, legitimate certifications (green lock), and credential-harvesting sites will increase. Flawless phishes will continue to prey on the gap in human firewalls, pivoting internally around organisations and intensifying efforts to better educate all staff.



Sans-serif (Without-Serif)	Serif (With-Serif)
Arial : Illusion ✗	Times New Roman: Illusion ⚠
Calibri : Illusion ✗	Book Antiqua: Illusion ⚠
Century Gothic: Illusion ✗	Courier New: Illusion ✓

Sans-serif (Without-Serif)	Serif (With-Serif)
Arial : 1lamp ✓	Times New Roman: 1lamp ✗
Calibri : 1lamp ✓	Book Antiqua: 1lamp ⚠
Century Gothic: 1lamp ⚠	Courier New: 1lamp ⚠

CONTINUED…

Fake Videos Bring A New Era of Fake News

- Lifelike computer-generated graphics - appearing to show video footage of events that never really happened - will be used to mislead the public.

CONTINUED...

- Improved Execution of Existing Attack Types
    - Better social engineering, increases in credential stuffing attacks, and more complicated malware with multiple stages and different form factors for transmission will make threats incredibly tricky to detect.

CONTINUED…

Mobile, In-the-app Malware

- Users of mobile devices are increasingly subject to malicious activity that pushes malware apps to their phones, tablets, or other devices running Android and iOS.

CONTINUED...

- IIoT attacks not slowing down
  - Three elements expected to play a significant role in the increase of IIoT attacks, according to the report, are:

1. increasing network connectivity to edge computing;
2. the difficulty in securing devices as more compute moves out to the edge; and
3. the exponential number of devices connecting to the cloud for updates and maintenance.

Kuva 1. Internet of Things. Lähde: Huffington Post

CONTINUED...

- The rise of **SaaS** (Software as a Service)

  - SaaS' greatest advantage is also its greatest weakness. With SaaS, you need much less IT. This is a benefit at first glance, but upon inspection, it becomes a problem - you don't control the access, or the data. Therefore, you don't know you were hacked, nor do you have the tools to know.

App Server
Mobiles
SaaS
Networks
Database
PCs
Codes

CONTINUED...

Ransomware Evolution

- Ransomware is the bane of cybersecurity, IT, data professionals, and executives. Perhaps nothing is worse than a spreading virus that latches onto customer and business information that can only be removed if you meet the cybercriminal's egregious demands. And usually, those demands land in the hundreds of thousands (if not millions) of dollars.

CONTINUED...

- **AI Expansion**

  - Robots might be able to help defend against incoming cyber-attacks. Between 2016 and 2025, businesses will spend almost $2.5 billion on artificial intelligence to prevent cyber attacks.

CONTINUED…

IoT Threats

- The Internet of Things (IOT) is making sure that every single device you own is connected. The problem is that all of that interconnectedness makes consumers highly susceptible to cyber attacks. Specifically, insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge leave users open to attacks.

CONTINUED…

- Attackers will Continue to Target Consumer Devices

  - In 2019 and beyond, will we start to see consumers being targeted across a range of connected objects. This is a likely scenario, with examples coming out of child predators targeting IoT devices in toys (designed for children).

CONTINUED…

- Attackers will become bolder, more commercial less traceable

  - Attackers will look to base themselves in countries where cybercrime is barely regarded as a crime and thereby placing themselves outside their victims' police jurisdictions.

CONTINUED...

- Attackers will get Smarter
  - Attackers capability to write customer specific targeted code will continue to improve faster than the defenders ability to counter or get ahead of it.

CONTINUED...

- **Breaches will get More Complicated and Harder to Beat**

  - Cybercriminals will look to grow their malicious activities using malicious code in ever more devious ways.

CONTINUED…

- Cyber Risk Insurance will become more common
  - As the industry evolves we might see cyber insurance covering for loss of reputation and trust with their customers, loss of future revenue from negative media or other exposure, and improvement costs for security infrastructure or system upgrades.

CONTINUED...

- Cybercrimes in Banking Sector
  - Cosmos Bank Fraud
  - Seva Vikas Bank Fraud

CONTINUED...

- Cosmos Bank Fraud
  - There was a malware attack on a switch operative as payment gateways for Visa and Rupay cards.
  - Core Banking System (CBS) receives debit card payment requests via switching system.
  - During malware attack a proxy switch was created and all fraudulent payment approvals were passed by this proxy switching system.
  - Cloning of bank's debit cards was used for the fraudulent fake transactions using fake debit cards.

CONTINUED...

- Seva Vikas Bank fraud

  - KYC was not done of its customers who took loan of more than rupees 50,00,000.
  - Loans disbursed without verification of documents.

CONTINUED...

- Contactless cards misuse
  - A device used to copy details from RFID-enabled contactless debit cards, if held as close as eight centimetres away from a victim's card.
  - It can copy up to 15 bank cards per second.
  - This data is stored on devices internal storage system, and thieves can connect the device to their PC using USB cables and transfer it using special software.

CONTINUED…

- <u>Aadhaar Breach</u>
  - Demographic Data – Name, Address, Aadhaar number was leaked from the dealers and distributors section in the website of Indian Oil Corporation-owned LPG brand, Indane.
  - The leak was due to lack of authentication in the local dealers portal.
  - Biometric data was safe.

CONTINUED...

- AnyDesk App
  - The Reserve Bank of India has warned banks of an emerging digital banking fraud that can wipe out a customer's bank balance by using the Unified Payment Interface (UPI) route.
  - The modus operandi is simple: fraudsters get victims to download an app called AnyDesk. Hackers get remote access to the mobile through a nine-digit code generated on the victim's device. "Once a fraudster inserts this app code on his device, he will ask the victim to grant certain permissions, which are similar to what are required while using other apps," RBI said in an advisory.
  - This enables the imposter to gain access to the victim's device and carry out transaction fraudulently. The modus operandi, according to RBI, can be used to carry out transactions through any mobile banking app or payment-related apps, including UPI or wallets.

Bottleneck faced by Law Enforcement Agency

- Lack of Sharing.

- Blame it on enemy-of-the-day.

- Ensuring adequate analytical and technical capabilities for law enforcement agencies.

- Generally go around in circles with sparse conclusions.

CONTINUED...

- Lack of capability , skills, resources.
- Reporting of crimes.
- Implementing information security practices and raising awareness.
- Working in a borderless environmEnt with laws of multiple jurisdictions.

Role of Government

- According to Indian government use of social media has also emerged as a key tool for committing cyber crimes and attacks that affect nation and society and is conscious of increase in cyber crimes. It has taken various steps in the form of awareness, training, legal framework, emergency response and implementation of best practices to prevent occurrence of such cyber crimes

Following Measures are taken by the Government

- The State Governments have been advised to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes.

- A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyze the digital evidence and present them in Courts.

- Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI.
- In addition, Government has set up cyber forensic training and investigation labs in the States of Maharashtra, Delhi, Karnataka, Tamil Nadu, Uttar Pradesh, Rajasthan Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

- The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

certin
Handling Computer Security Incidents

Tools Used for Investigation

Some of the tools to investigate cyber crimes:

- Email Tracer
- Forensic Tool Kits
- Call Directory Records
- IP Tracker
- Forensic Duplicators
- Android/IOS Data Extractors
- Data Recovery Tools

Cases Registered Under The IT Act 2000 Include

- Tampering computer source documents (Section 65 IT Act)
- Loss /damage to computer resource/utility (Section 66 (1) IT Act)
- Hacking (Section 66 (2) IT Act)
- Obscene publication/transmission in electronic form (Section 67 IT Act)
- Failure of compliance/orders of Certifying Authority (Section 68 I T Act)
- Failure to assist in decrypting the information intercepted by Govt Agency (Section 69 IT Act)

CONTINUED...

- Un-authorized access/attempt to access to protected computer system (Section 70 IT Act)
- Obtaining license or Digital Signature Certificate by misrepresentation / suppression of fact (Section 71 IT Act)
- Publishing false Digital Signature Certificate (Section 73 IT Act)
- Fraud Digital Signature Certificate (Section 74 IT Act)
- Breach of confidentiality/privacy (Section 72 IT Act)

Cyber Crime Cases Also Registered Under The IPC

- Offences by/against Public Servant (Section 167, 172, 173, 175 IPC)
- False electronic evidence (Section 193 IPC)
- Destruction of electronic evidence (Section 204, 477 IPC)
- Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476,
- Criminal Breach of Trust (Section 405, 406, 408, 409 IPC)
- Counterfeiting Property Mark (Section 482, 183, 483, 484, 485 IPC)
- Tampering (Section 489 IPC)

Your friend and partner in all training and consultancy related to:

- ✓ Cyber Security
- ✓ Cyber Forensics
- ✓ Cyber Crime Investigation
- ✓ Cyber Law
- ✓ Cyber Policy Guidelines
- ✓ Cyber Audit

Thank You

DR. HAROLD D'COSTA

+91-96376 12097