Impact Factor (SJIF): 2.125

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 1, January-2016

CYBER-CRIMES AND CYBER -ESPIONAGE: A WEB OF AN EVIL

CS Shaifali Bhatia
Assistant Professor- NGI Junagadh (Gujarat)
Vaishali Bhatia
Panjab University, Chandigarh (Punjab)

ABSTRACT

The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education. There're two sides to a coin. Internet also has its own disadvantages is Cybercrime- illegal activity committed on the internet. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. The research comes at growing public awareness of the issue but the study's authors say their findings show that people are still not doing enough to protect themselves. However, it should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to the society. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals Restriction of cyber-crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cybercrimes and cyber espionage as a web of evil.

INDEX TERMS— Cyber-crimes, Cyber espionage, crime pays, web of evil, types, case study and secondary surveys

INTRODUCTION

Cyber-crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime. Crime committed using a computer and the internet to steal data or information. ♣ Illegal imports. ♣ Malicious programs. Cyber-crime is nothing but where the computer used as an object or subject of crime. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber-crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds

Cyber espionage describes the stealing of secrets stored in digital formats or on computers and IT networks. It is the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization:

The Components of Malicious Cyber Activity In this initial report we start by asking what we should count in estimating losses from cybercrime and cyber espionage. We can break malicious cyber activity into **six** parts:

• The loss of intellectual property and business confidential information

• Cybercrime, which costs the world hundreds of millions of dollars every year

• The loss of sensitive business information, including possible stock market manipulation

• Opportunity costs, including service and employment disruptions, and reduced trust for online activities

• The additional cost of securing networks, insurance, and recovery from cyber attacks

• Reputational damage to the hacked company

CRIME PAYS—BUT HOW WELL?

Extracting value from the computers of unsuspecting companies and government agencies is a big business. The size of any loss, however, is the subject of intense dispute. Is this what one senior official called “the greatest transfer of wealth in human history,” or is it what a leading economist called a “rounding error in a fourteen trillion dollar economy?”

Cyber-crimes against banks and other financial institutions probably cost many hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information probably costs developed economies billions of dollars—how many billions is an open question. These losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage.

The cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. There are opportunity costs, damage to brand and reputation, consumer losses from fraud, the opportunity costs of service disruptions “cleaning up” after cyber incidents and the cost of increased spending on cyber security. Each of these categories must be approached carefully, but in combination, they help us gauge the cost to societies.

Some previous estimates of the cost of cybercrime relied on surveys, which are notoriously imprecise unless very carefully constructed. Surveying a few companies or even a few hundred companies and then extrapolating costs from their responses is a dangerous methodology. There are significant differences among economic sectors in vulnerability. There are rules for deciding on sample size and selection, but imperfect samples are a common flaw in surveys. Many previous studies use a sample population that is too small for us to feel confident in the results. One common problem in cyber security surveys is that those who answer the questions “self-select” and we do not know if their experience is the same as those who chose not to respond. Companies that have concealed large losses, for example, might choose to not respond, introducing a possible source of distortion into the survey.

CRIME AS AN EVIL FACTOR OF SOCIETY

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritate by the question, ‘Why there is too much ado about crime? 'No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behavior! However, it should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to the society. In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes.

CYBER CRIME: TYPES

- **Spam and Phishing**

Spamming and phishing are two very common forms of cybercrimes. There is not much you can do to control them. Spam is basically unwanted emails and messages. They use Spambots. Phishing is a method where cyber criminals offer a bait so that you take it and give out the information they want. The bait can be in form of a business proposal, announcement of a lottery to which you never subscribed, and anything that promises you money for nothing or a small favor. There are online loans companies too, making claims that you can get insecure loans irrespective of your location. Doing business with such claims, you are sure to suffer both financially and mentally. **Phishing** has its variants too – notably among them are Tab nabbing, Tab jacking and vishing and smishing

Such spamming and phishing attempts are mostly emails sent by random people whom you did not ever hear of. You should stay away from any such offers especially when you feel that the offer is too good. The US Cybercrime Center says – do not get into any kind of agreements that promise something too good to be true. In most cases, they are fake offers aiming to get your information and to get your money directly or indirectly.

- **Botnets**

Botnets are networks of compromised computers, controlled by remote attackers in order to perform such illicit tasks as sending spam or attacking other computers. Computer Bots can also be used act like malware and carry out malicious tasks. Then can be used to assemble a network of computers and then compromise them.

- **Identity theft**

Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains. When this is done online on the Internet, its is called Online Identity Theft. The most common source to steal identity information of others, are data breaches affecting government or federal websites. It can be data breaches of private websites too, that contain important information such as – credit card information, address, email ID's, etc.

- **Social Engineering**

Social engineering is a method where the cyber criminals make a direct contact with you using emails or phones – mostly the latter. They try to gain your confidence and once they succeed at it, they get the information they need. This information can be about you, your money, your company where you work or anything that can be of interest to the cyber criminals.

- **PUPs**

PUPs, commonly known as Potentially Unwanted Programs are less harmful but more annoying malware. It installs unwanted software in your system including search agents and toolbars. They include spyware, adware, as well as dialers. Bit coin miner was one of the most commonly noticed PUPs in 2013.

- **Drive-By-Downloads**

Drive By Downloads too, come close to malvertising. You visit a website and it triggers a download of malicious code to your computer. These computers are then used to aggregate data and to manipulate other computers as well.

The websites may or may not know that they have been compromised. Mostly, the cyber criminals use vulnerable software such as Java and Adobe Flash and Microsoft Silverlight to inject malicious codes as soon as a browser visits the infected website. The user does not even know that there is a download in progress.

- **Exploit Kits**

A vulnerability means some problem in the coding of a software that enables cyber criminals to gain control of your computer. There are ready to use tools (exploit kits) in the Internet market which people can buy and use it against you. These exploit kits are upgraded just like normal software. Only difference is these are illegal. They are available mostly in hacking forums as well as on the Dark net.

- **Scams**

Notable among Internet scams are, scams which misuse the Microsoft name and other general tech support scams. Scamsters phone computer users randomly and offer to fix their computer for a fee. Every single day, scores of innocent

people are trapped by scam artists into Online Tech Support Scams and forced to shell out hundreds of dollars for non-existent computer problems.

- **Telecommunications Piracy**

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many. This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement (United States, Information Infrastructure Task Force 1995, 131).When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss.

- **Electronic Funds Transfer Fraud**

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy.1 Computer-related crime may be compound in nature, combining two or more of the generic forms outlined above.

- **Malvertising**

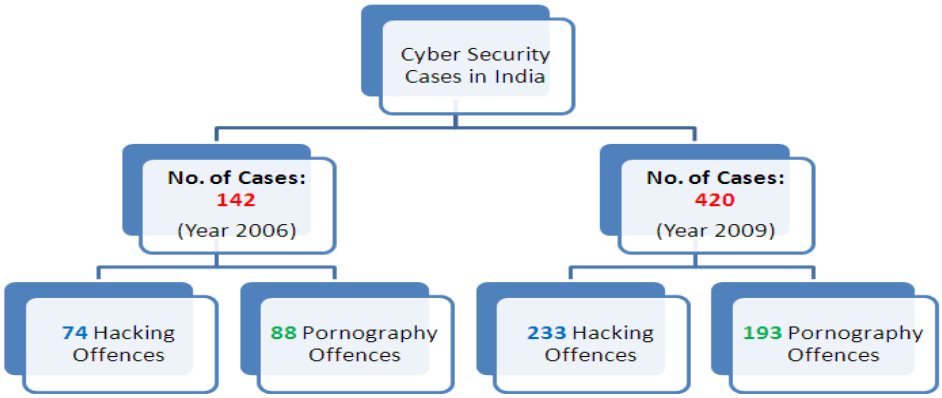
Malvertising is a method whereby users download malicious code by simply clicking at some advertisement on any website that is infected. In most cases, the websites are innocent. It is the cyber criminals who insert malicious advertisements on the websites without the knowledge of the latter. It is the work of advert companies to check out if an advertisement is malicious but given the number of advertisements they have to deal with, the malverts easily pass off as genuine ads.

In other cases, the cyber criminals show clean ads for a period of time and then replace it with malverts so that the websites and advertisements do not suspect. They display the malverts for a while and remove it from the site after meeting their targets. All this is so fast that the website does not even know they were used as a tool for cybercrime. Malvertising is one of the fastest, increasing types of cybercrime.

- **Ransom ware**

This is one of the detestable malware-based attacks. Ransom ware enters your computer network and encrypts your files using public-key encryption, and unlike other malware this encryption key remains on the hacker's server. Attacked users are then asked to pay huge ransoms to receive this private key.

CYBER CRIME: CASE STUDY



- **ONLINE CREDIT CARD FRAUD ON E-BAY**
  Bhubaneswar: Rourkela police busted a racket involving an online fraud worth Rs 12.5 lakh. The modus operandi of the accused was to hack into the eBay India website and make purchases in the names of credit cardholders.

Two persons, including alleged mastermind Debasis Pandit, a BCA student, were arrested and forwarded to the court of the sub divisional judicial magistrate, Rourkela. The other arrested person is Rabi Narayan Sahu.

Superintendent of police D.S. Kutty said the duo was later remanded in judicial custody but four other persons allegedly involved in the racket were untraceable. A case has been registered against the accused under Sections 420 and 34 of the Indian Penal Code and Section 66 of the IT Act and further investigation is on, he said. While Pandit, son of a retired employee of Rourkela Steel Plant, was arrested from his Sector VII residence last night, Sahu, his associate and a constable, was nabbed at his house in Uditnagar.

Pandit allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. He then made purchases by using their passwords. The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London, said V. Naini, deputy manager of eBay.

The company brought the matter to the notice of Rourkela police after some customers lodged complaints.Pandit used the address of Sahu for delivery of the purchased goods, said police. The gang was involved in train, flight and hotel reservations. The hand of one Satya Samal, recently arrested in Bangalore, is suspected in the crime. Samal had booked a room in a Bangalore hotel for three months.

The hotel and transport bills rose to Rs 5 lakh, which he did not pay. Samal was arrested for non-payment of bills, following which Pandit rushed to Bangalore and stood guarantor for his release on bail, police sources said.

- **BAAZEE.COM CASE**

CEO of Baazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber-crime cases and a lot of education is required.

- **WIPRO SPECTRAMIND CASE**

Wipro Spectra mind lost the telemarketing contract from Capital one due to an organized crime. The telemarketing executives offered fake discounts, free gifts to the Americans in order to boost the sales of the Capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarketers were also involved in the whole scenario

- **ONLINE GAMBLING CASE**

Recent Indian case about cyber lotto was very interesting. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the internet with the address of eurolottery@usa.net. Whenever accessed, the site would name him as the beneficiary of 12.5 million pound. After confirmation a telgu newspaper published this as a news. He collected huge sums from the public as well from the banks. However the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs. 1.73 million bounced.

- **EMAIL SPOOFING CASE**

Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this information proved to be true in the next few days.

- **CYBER-CRIMES NEWS**

With the increase in use of information technology/internet, there is a big increase in Cyber-crimes. This ranges from theft of bank account PIN to theft of personal information. On account of such cyber-crimes, annually there is a loss of Rs. 30,000 crores in the world. Like Edward Snowden, there are so many hackers in the world. As per Julius Assange, Internet is the biggest medium of spying. Over and above the spying, it is a platform of economic/financial cheating. It is advisable to limit uploading personal information/photographs on social sites. These views were expressed by Triveni Singh (Director, Special Task Force, Cyber Cell) at Chartered Accountants' Conference at Rajkot. Gujarat Samachar (20 Dec., 2015)

CYBER EXPIONAGE: CASE STUDY

- *Security experts at Fire Eye uncovered a cyber-espionage campaign that targeted organizations in India and the Tibetan activists.*

A. Security firm Fire Eye revealed an intense activity of hackers based in China particularly interested in entities and organization linked to the Indian Government as well as information on Tibetan activists. Also in this case we are dealing with a cyber espionage campaign conducted by an Alleged Chinese APT. The Chinese hackers run spear phishing attacks against their targets, the malicious email have an attachment containing a script called Water main. When victims open it the malicious code creates backdoors on target machines.

Experts at Fire Eye are monitoring the Waterman's activity since 2011, the APT targeted more than 100 entities since now, and about 70% of them are from India.

"Collecting intelligence on India remains a key strategic goal for China-based APT groups, and these attacks on India and its neighboring countries reflect growing interest in its foreign affairs," said Bryce Boland, Fire Eye chief technology officer for Asia Pacific.

"Organizations should redouble their cyber security efforts and ensure they can prevent, detect and respond to attacks in order to protect themselves."

Fire Eye detected the same APT group in April 2015, one month before Indian Prime Minister Narendra Modi's first visit to China.

Fire Eye has already reported cyber espionage conducted by other APT groups, in April the security firm revealed the details of APT30 which targeted aerospace and defense company in India among others.

"Advanced threat group like APT 30 illustrate that state-sponsored cyber espionage affects a variety of governments and corporations across the world," explained Dan McWhorter, VP of threat intelligence at Fire Eye. "Given the consistency and success of APT 30 in Southeast Asia and India, the threat intelligence on APT 30 we are sharing will empower the region's governments and businesses to quickly begin to detect, prevent, analyze and respond to this established threat."

According to Fire Eye, the majority of targeted organizations in India have already patched the flaws exploited in the attacks.

At the time I was writing the Government of Beijing hasn't commented the findings of the Fire Eye experts.

India and China have long been involved in a dispute over their border, for this reason, the government of Beijing could have arranged a cyber-espionage campaign searching for information related to the Indian diplomacy.

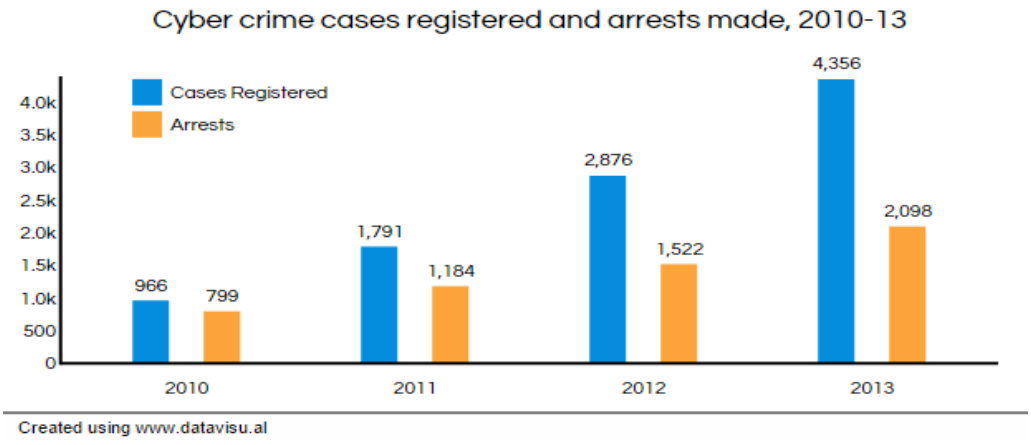
India has also been wary of China influence in Sri Lanka and Nepal.

II. INDIAN CYBER CRIME SOARS 350% IN 3 YEARS

A. In the three years up to 2013, registered cases of cyber crime were up 350%, from 966 to 4,356

With Internet usage soaring in India, so is cyber-crime, but India's laws do not appear to be adequate to tackle the surge.

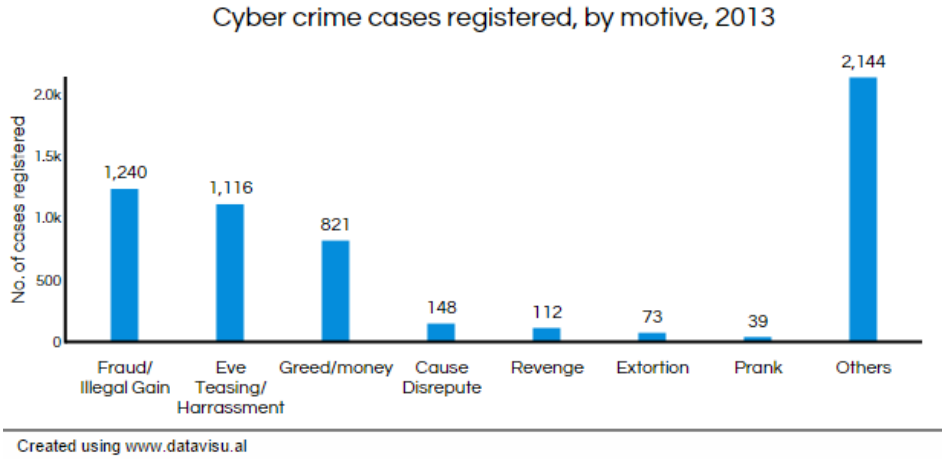
In the three years up to 2013, registered cases of crime were up 350%, from 966 to 4,356, according to statistics from the National Crime Records Bureau (NCRB).



Source: NCRB

India was projected to have 302 million internet users by the end of 2014, and will, this year, overtake the United States as the second largest number of internet users after China. About 24% of the population will then be online. As cyber-crime rises, there are indications that the criminal-justice system is unable to cope, with a minuscule percentage of convictions reported, although there is no reliable, nationwide data.

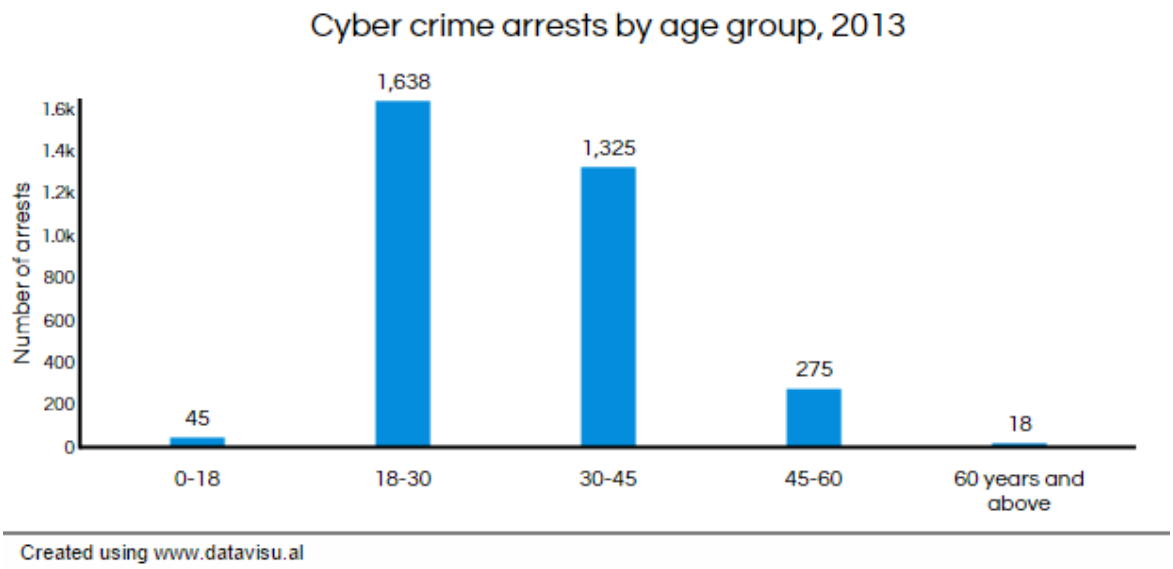
TOP MOTIVES FOR CYBER CRIME: ILLEGAL GAIN AND HARASSMENT



Source: NCRB

"Illegal gains" and "harassment" are the top cyber-crime motives, the data reveal. The majority of crimes are registered under "others"; 2,144 cases were registered in this category in 2013. Such a high number of cases registered in "others" implies that the current laws and regulations aren't detailed enough to tackle cyber-crime. Instead of bunching cyber-crime in the "others" category, they should be specifically classified, said Sunil Abraham, founder-director of Bangalore's Centre for Internet & Society.

YOUNG AND SAVVY: WHO'S ARRESTED FOR CYBER CRIME



Source: NCRB

Those who are arrested under these laws are overwhelmingly young. Data show that the age group of 18-30 accounts for the highest percentage of cyber-crime with 1,638 persons arrested in the age bracket out of a total arrests of 3,301 in 2013.

Some cyber laws are considered too draconian for a modern, democratic society, being forced open by the spread of the Internet. These laws are now being opposed by various experts, lawyers and free-speech activists.

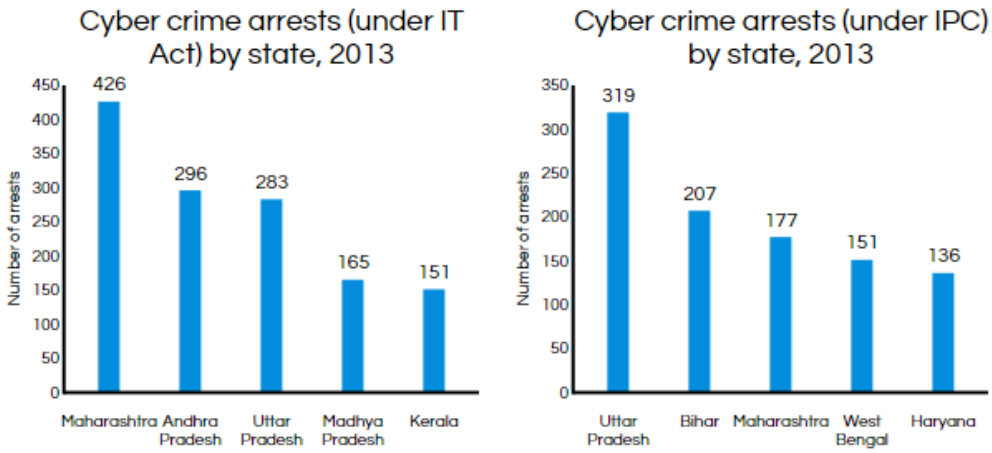
Consider the particularly contentious section 66A, which deals with "offensive" messages sent through a computer or other personal communication devices. Anyone found guilty can be imprisoned for up to three years and fined.

In 2012, two girls were even arrested under section 66A in Mumbai for questioning the shutdown of Mumbai over Bal Thackeray's death on Facebook, with one of them being arrested for just "liking" her friend's post. To prevent such abuses, the Supreme Court has ruled that arrests can only be made after clearance from an Inspector General of Police in cities and a Superintendent of Police in the districts.

"Recently certain incidents have been reported wherein section 66A of the Information Technology Act, 2000, has been invoked solely as well as with other sections of Indian Penal Code against certain persons for posting/communicating certain content which was considered by the police to be harmful," the Supreme Court judgment said. "Due diligence and care may be exercised while dealing with cases arising out of the alleged misuse of cyberspace. The Supreme Court is now examining the constitutional validity of section 66A.

Abraham said the problem is various sections of the Information Technology (IT) Act, 2000, such as Section 66A and section 69 (power to issue directions to block public access through any computer resource) are "deeply flawed". He said these laws were "copy-paste jobs" from British and American laws.

MAHARASHTRA TOPS THE CYBER CRIME LIST



Source: NCRB

Cybercrime appears to be concentrated in states with major cities, indicating that urbanisation–and so internet penetration–is a factor. Maharashtra accounts for the most persons arrested under the IT Act, 2000, and Uttar Pradesh reported the most arrests under the older Indian Penal Code (IPC).

WEB OF EVIL: ONE IN FIVE OF US FELL VICTIM TO CYBERCRIME IN PAST YEARS

MORE than 12 million Britons fell victim to cybercrime in the past year, a wide-ranging new study has revealed. One in five people were hit by ID theft, computer hacking or other online crimes in 2014 suffering a total loss of £1.6bn, according to the survey.

Dealing with the aftermath of the crime took victims about one working day - nine hours, the internet security giants Norton found.

The research comes amid growing public awareness of the issue but the study's authors say their findings show that people are still not doing enough to protect themselves.

The first official figures for the crime category, published by the Office for National Statistics earlier this year, showed that there were 7.6million cases of fraud and computer misuse last year.

People using dating websites were cheated out of more than £33million last year by lonely-hearts con artists.

And in one of the most high-profile computer hacking cases this year, 160,000 customers of phone company Talk Talk had their details stolen by cyber criminals in an online attack last month.

Findings from the Norton Cyber security Insights Report, published today, revealed that concern about online crime is so widespread; nearly 90 percent worry about falling victim to cyber criminals and only one in ten feel they have control of their internet security.

Nearly half of Britons, 44 percent have been hit by cybercrime in their lifetime and one in five or 22 percent in the last year.

The average loss for each person was £134, giving an estimated total loss across the nation of £1.6bn.

One in six people have been hit by the rising crime of online extortion, where hackers use so-called 'ransom ware' to take over computers and deletes files unless a ransom is paid.

And even after paying the extortionists, half of those still lost their documents and photos.

The report found that one in ten had their identity stolen and one in seven saw their financial details compromised after internet shopping.

The survey of more than 1,000 people in the UK found that 45 percent pointed the finger of blame for the cyber-attacks at foreign governments such as Russia and China.

While one in ten think the primary culprits are teenage hackers doing it for fun.

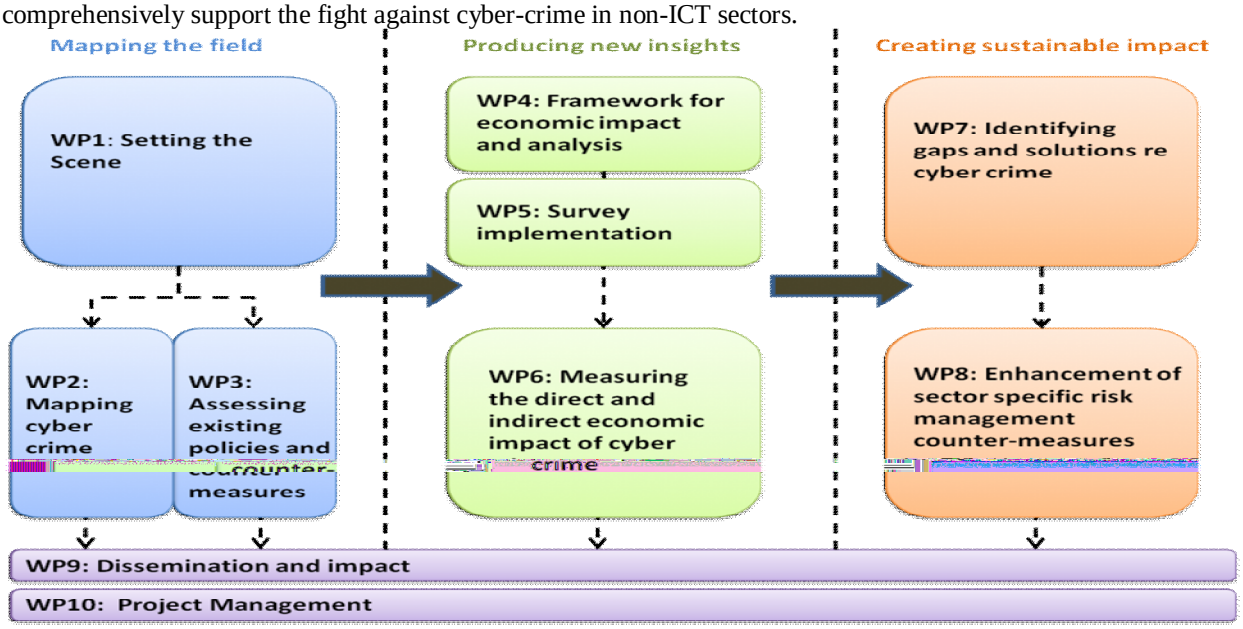
Despite falling victim to cyber criminals, two in five do not bother changing their passwords.

CYBER-CRIME UNFOLDS IN THREE PHASES.

A first mapping preparatory phase in which the research questions are refined and existing knowledge in the different disciplines and stakeholders' views are synthesized and compared.

The second new insight phase is devoted to the collection of new insights and the development of the model on the economic impact of cyber-crime on the selected non- ICT sectors.

The third solution phase focuses on sustainable impact by the cross-analysis and integration of the research results from the various strands of investigation, and the development of concrete and diverse measures, which can systematically and comprehensively support the fight against cyber-crime in non-ICT sectors.



The work is broken up into 10 work packages:

WP1, Setting the scene, sets up the necessary stakeholder and expert engagement mechanisms necessary to support the project's participatory and multi-actor research strategy. This work package conducts the stakeholder and expert analysis identifying key stakeholder groups and sets up the E-CRIME Stakeholder Forum. It also incorporates the definition of the project's methodological framework as a guide to all partners and participants, and conducts initial research to confirm the representative non-ICT sectors and Member States for the analysis.

WP2, Mapping cyber-crime, maps cyber-crime activities, in the form of cyber-crime taxonomy, inventory, structures, economies and journeys, and validate its findings with stakeholders and experts. Initially, it develops taxonomy of cyber-crime. It then investigates the key factors and drivers behind cyber-crime networks, their modus operandi and economies, while producing selected criminal journeys from a perpetrator and victim perspective.

WP3, Assessing existing policies and counter-measures, produces a detailed assessment of existing cyber-crime counter-measures, including policies, regulatory and enforcement frameworks, business best practices and technologies. This work package also includes the on-going monitoring of these counter-measures through the lifespan of the project.

WP4, Framework for economic impact and analysis, develops a theoretical framework and hypotheses about the impact of cyber-crime on non-ICT sectors, conducts new data collection with industries and integrates these new data with various viewpoints to generate new insights.

WP5, Survey implementation, focuses on collecting data from citizens. The work package contains a large scale citizen survey to understand citizens' experiences of victimization, awareness of cyber-crime, economic impacts at different level of European society and value network participants, and issues of trust, confidence and societal values and individual rights (e.g., privacy, cohesiveness).

WP6, Measuring the direct and indirect economic impact of cyber-crime, produces a multi-layer and integrated model of the economic impact of cyber-crime on the selected non-ICT sectors, assessing the impact for the different levels of the European society (i.e., individual, industry players, sectors, states, society) and for different participants in the value network (i.e., software vendors, network operators, ISPs, industry players, cyber security providers, end users).

WP7, Identifying gaps and solutions re cyber-crime, uses the findings and results from preceding work packages to identify inter-sector, common solutions. These solutions identify concrete and measurable opportunities for deterring possible criminals and managing cyber-crime.

WP8, Enhancement of sector specific risk management counter-measures, builds on the opportunities map in WP7, while developing sector specific methods, tools and measures for managing and deterring cyber-crime in the selected non-ICT sectors, while creating portfolios of solutions. These comprehensive intra-sector portfolios of responses include risk management tools, sector specific requirements for the development of crime-proofed applications, enhancing regulatory innovation and development, sector specific best practices, and awareness, trust and confidence initiatives.

WP9, Dissemination and impact, contains the project dissemination and impact activities, and involves setting out and managing the project's dissemination strategy.

WP10, Project management, is the project management work package and contains all the administration, management and reporting and co-ordination activity necessary to support the E-CRIME.

CONCLUSION

This manuscript concludes that despite crimeless society is myth, crime is omnipresent phenomenon. Though internet makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality. It is the biggest evil for all sectors of economy. The research comes at growing public awareness of the issue but the study's authors say their findings show that people are still not doing enough to protect themselves.

REFRENCES

1. http://www.mcafee.com/in/resources/reports/rp-economic-impact-cybercrime.pdf
2. http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
3. http://www.slideshare.net/lipsita3/cyber-crime-and-security-ppt
4. http://www.thewindowsclub.com/types-cybercrime
5. http://www.cyberlawclinic.org/casestudy.asp
6. http://www.cyberlawsindia.net/cases2.html
7. http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html

8. http://securityaffairs.co/wordpress/39535/hacking/cyber-espionage-on-india.html

9. http://www.business-standard.com/article/current-affairs/indian-cyber-crime-soars-350-in-3-years-115011900329_1.html

10. https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf

11. http://www.express.co.uk/news/uk/619841/One-in-five-victim-to-cybercrime