IMPACT OF CYBERCRIME ON TOURISM INDUSTRY

Dr. Heramb Nayak
Maharaja Surajmal Institute
GGSIP University, New Delhi, India

ABSTRACT

Cyber crime how it makes globally a challenge to tourism industry and the things how suffered and to overcome from such types of crime in the industry. Net crime is criminal exploitation of the Internet. In other words Cybercrime refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" there are ‘no cyber-borders between countries'. International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. The Purpose of the study is about cybercrime in Tourism Industry. That includes both the major industry under it is Hospitality and Aviation Industry. To analysis the effects of cybercrime on Hospitality and Aviation Industry. To study the methods how to overcome cybercrime/cyber attacks. To analysis financial loss incurred by Hospitality and Aviation Industry. Cybercrime is already a big problem all over the world—and its growing fast. The law enforcement world is scrambling to catch up; legislators are passing new laws to address this new way of committing crime, and police agencies are forming special computer crime units and pushing their officers to become more technically savvy.

However, the cybercrime problem is too big and too widespread to leave to politicians and police to solve. The former often don’t have the technical expertise to pass effective laws, and the latter lack sufficient training, manpower, and time not to mention the confusing issue of jurisdiction to tackle any but the most egregious of Internet crimes.

Cybercrime, like crime in general, is a social problem as well as a legal one. To successfully fight it, we must engage people in the IT community (many of whom might be reluctant to participate) and those in the general population who are affected, directly or indirectly, by the criminal activity that has found a friendly haven in the virtual world.

We can use a number of tactics and techniques, including the legal system, peer pressure, and existing and emerging technologies, to prevent cybercrime.

Failing that, we can develop formal and informal responses that will detect cybercrime more immediately, minimizing the harm done and giving us more information about the incident, maximizing the chances of identifying and successfully prosecuting the cybercriminal.

We’re all in this boat together. The only way to stop cybercrime is to work together and share our knowledge and expertise in different areas to build a Class A cybercrime-fighting team.

Key Word: Cybercrime, Hospitality, Aviation, Tourism, Report, Industry, Networks

I INTRODUCTION

Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Net crime is criminal exploitation of the Internet. In other words Cybercrime refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" there are 'no cyber-borders between countries'. International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. No matters in developing or developed countries, governments and industries have gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale. U.S. China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime

Cybercrime's defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

An Australian nationwide survey conducted in 2006 found that two in three convicted cyber-criminals were between the ages of 15 and 26.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

A report (sponsored by McAfee) estimates the annual damage to the global economy at $445 billion; however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud worldwide.

Purpose of the study

The objective of the study to known about the cyber crime how it makes globally a challenge to tourism industry and the things how suffered and to overcome from such types of crime in the industry.Net crime is criminal exploitation of the Internet. In other words Cybercrime refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" there are 'no cyber-borders between countries'. International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. The author wants to study on the following objectives.

- To Study about cybercrime
- To analysis the effects of cybercrime on Hospitality and Aviation Industry
- To study the methods how to overcome cybercrime/cyber attacks
- To analysis financial loss incurred by Hospitality and Aviation Industry

II Research methodology

Present study is based on secondary data and same has been collected through Internet, Books and Journal, Magazines and websites. Mainly data has been collected from the annually reports of the ministry of tourism. This study used mean value, growth rates etc. are used to analysis the data.

Literature of Review

Sonmez & Graefe 1998 In the study we found the Potential tourists are often exposed to media coverage of international political violence. The volatile relationship between tourism and terrorism is magnified by the media in a manner to cloud actual probabilities of being targeted by terrorists. To date there has been no theory of terrorism and of course its complicity with the media and tourism.

The Federal Bureau of Investigation (FBI) 2003 In the study we found that the 'The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Crenshaw, 1998, 2003. In the study we found that the Terrorism exists because the politically weak and disenfranchised have no other means by which to realize their objectives since they will not be taken seriously by the normal population. Terrorism, therefore, can place political change on the agenda). Violence can also be fuelled by the lack of opportunity for political participation in a society.
Seddighi et al. (2001) and Stafford et al. (2002) state that the effects of terrorist attacks might cause political instability, which leads to the decline or disappearance of tourist arrivals in some tourist destinations The literature and statistics all confirm that terrorist attacks alter tourism demand patterns, indicating an increasing demand to cancel travel or holiday plans particularly just after the 9/11 terrorist attack

III Impact of cybercrime on Hospitality and Airlines Industry

There are two areas of Tourism industry where Cybercrime has its enormous impact. These are:

1. **Hospitality industry**
2. **Airlines Industry**

According to Trust wave's 2012 Global Security Report, the hospitality industry ranked at the top of the list for data breaches and has remained on top for four consecutive years.

The hospitality sector consisting of hotels, resorts, country clubs, transportation companies, and destination marketing organizations, convention centres, tour companies, cruise lines, theme parks, and restaurants is a multi-billion dollar industry and has become one the major revenue contributors to the global economy and employment sector. It is estimated that security breaches in the hospitality industry are far higher than even the financial services or retail sectors. The 2012 Verizon Communications Report also revealed that the accommodations and food service industries accounted for half of all breaches in 2011.

It is widely acknowledged that hotels and resorts of all sizes face a storm of factors making them vulnerable to breaches. What it really comes down to it is most hotels and resorts do not have data privacy and security as priority. According to the "Hospitality Industry Risks: Data Privacy and Security" article, "hospitality businesses often prove to be an easy target for criminals who are looking for high transaction volume, a large database of customer records, a low barriers to entry. Unfortunately, many hospitality companies have not upgraded their risk management plans to address the inherent exposures associated with today's sophisticated data management." Furthermore, the "Data Breaches Make the Hospitality Industry Less Hospitable" article also points out that "while hotels ride out the recession, security maintenance, implementation, and upgrades fall lower in the priority checklist, creating an easy welcome mat for fraudsters." CBS News also reported that hackers target hotels because they are easy prey and it can take a long time on average, about five months–until hackers are discovered.

Wi-Fi Threats

As hotels become dependent upon wireless communications, security vulnerabilities of such an adoption continue to rise. Wi-Fi now has the potential to open doors to cyber criminals, allow unauthorized entry of privacy hackers and just about every other security nightmare imaginable. Even though a router may provide advanced security features, it still doesn't translate into protection of the hotel's or guests' confidential/personal information.

Spear-phishing & backdoor attacks: The Dark hotel malware is one of the leading examples of these attacks. Hackers who conducted the attack waited for hotel guests to check-in and connect to the Wi-Fi network by submitting their surname and room number to login. The attackers use the hotel's compromised network to send bogus software update messages to trick guests into downloading a backdoor that appears as a legitimate software update (for Adobe Flash or Google Toolbar). The guests download this new update, only to infect their machine with a backdoor that may be used to download further software such as Trojans and advanced stealing key loggers.

Man-in-the-middle (MITM) attacks: This involves the hackers placing their malicious code between the victim and a valuable resource, such as a login page presented by the hotel body. The most sophisticated MITM attack type is conducted via browsers. In this case, the malware silently records the data transferred between the user's browser and the hotel login page that has been hardcoded into the malware. Such attacks don't require the attacker to be in close proximity to the victims, and can be used to target a large group of victims with less effort. Hackers may also use packet sniffers to intercept the information.

ARP (Address Resolution Protocol) spoofing: ARP spoofing or flooding is a technique that can be used to attack hotel networks. It allows hackers to sniff traffic on a hotel network and modify the exchange of data. Criminals send fake ARP messages to a LAN to associate the MAC address of an attacker to an IP address of a victim. As a result, any data meant to be transferred to the victim's IP address is transferred to the criminal instead. The attacker can also launch denial-of-service attacks against victims by forming a connection of a nonexistent MAC address to the victim's IP address.

- What can Hospitality industry do to protect themselves from the cyber attacks?

Only Antivirus software and firewalls will not shield and protect hotels and resorts from hackers performing security breaches inside and outside of their premises. Both management and owners should invest in a capable Intrusion Detection System (IDS) that can help monitor their network system for any suspicious traffic. IDS will help hotels quickly discover if someone is trying to hack their network security system.

For larger hotel chains and resorts, a SIEM solution would also be very effective in managing, monitoring, and securing a large network. Security experts believe that SIEM solutions that interface with a successful IDS is most suited to monitor network traffic, deliver real-time alerts, and provide effective threat management which can result in a greater security posture For example, Tactical FLEX, Inc. is among SIEM-leading suppliers that provides a very strong focus on intrusion detection for successful threat management. Aanval's unique approach to security threat management helps organizations proactively seek out potential problems before they actualize, instead of operating in a reactive mode after attacks have occurred.

- What can Aviation Industry do to protect themselves against cyber-attacks?

The airline industry relies on computer systems extensively in their ground and flight operations. Some systems are directly relevant to the safety of aircraft in flight, others are operationally important, and many directly impact the service, reputation and financial health of the industry.

Many airlines and airports have robust systems in place to address common hacking threats, but have not taken a holistic view to all of their IT infrastructure nor considered the broader threat to the aviation system.

IATA has put in place a three-pillar strategy, including work to understand, define and assess the threats and risk of cyber-attack, advocacy for appropriate regulation and mechanisms for increased cooperation throughout the industry and with Governments.

In 2013, IATA developed the first iteration of a toolkit to assist airlines in understanding and better defining the risks to their organizations. This includes a situational assessment of cyber security in the industry, an introduction to cyber threats, a framework for assessing risk, and guidance material for setting up a cyber security management system. The toolkit was published in July 2014.

IATA presented a paper to the ICAO AVSEC Panel in 2014 to highlight the threats to cyber security, call on regulators to work with industry, and take an outcome-focused approach to cyber security in their regulation.

A group has been created including IATA, ICAO, CANSO, ICCAIA and ACI to coordinate activities and provide a common framework for the industry. A Memorandum of Cooperation was created to provide a roadmap for the future of cyber security for aviation. The Civil Aviation Cyber Security Action Plan was signed 5 December 2014 at ICAO Headquarters. Looking forward, work will continue to further define the threats and devise strategies to combat them, both within the airlines and across the industry.

IATA will continue to work with regulators to advocate for coordinated and outcome-focused regulation, and with industry partners to agree on a common framework.

Mechanisms for data and intelligence sharing will be sought in conjunction with industry partners.

WHAT IS CYBERCRIME?

Computer Crime is a new form of crimes which involves the use of a computer as the primary instrument to facilitate the crime and targets computer networks themselves. Included in this category are such crimes as hacking, releasing computer contaminant viruses, disrupting and denying computer services to an authorized user , shutting down computers by flooding them with unwanted information (so-called ''denial of service'' attacks), and taking copying, altering, deleting, or destroying computer data, and software or programs. Computer crimes require a much higher degree of technical knowledge than computer-related crimes.

Cyber-crime by definition is any harmful act committed from or against a computer or network, it differs according to McConnell International, “from most terrestrial crimes in four ways: they are easy to learn how to commit, they require few resources relative to the potential damages caused, they can be committed in a jurisdiction without being physically present in it and fourthly, they are often not clearly illegal.

Another definition given by the Director of Computer Crime Research Centre (CCRC) during an interview is that “cyber-crime is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. In essence, cyber-crime is crime committed in a virtual space and a virtual space is fashioned in a way that information about persons, objects, facts, events, phenomena or processes are represented in mathematical, symbol or any other way and transferred through local and global networks.

From the above, we can deduce that cyber crime has to do with wrecking of havoc on computer data or networks through interception, interference or destruction of such data or systems. It involves committing crime against computer systems or the use of the computer in committing crimes.

Cybercrime is crime that is enabled by, or that targets computers. Some argue there is no agreed-upon definition for “cybercrime” because “cyberspace” is just a new specific instrument used to help commit crimes that are not new at all. Cybercrime can involve theft of intellectual property, a violation of patent, trade secret, or copyright laws. However, cybercrime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data. If a terrorist group were to launch a cyber attack to cause harm, such an act also fits within the definition of a cybercrime. The primary difference between a cyber attack to commit a crime or to commit terror is found in the intent of the attacker, and it is possible for actions under both labels to overlap.

CATEGORIES OF CYBER CRIME

Cybercrimes can be divided into four major categories:

1. Cybercrime against persons.
2. Cybercrime against property.
3. Cybercrime against the organization.
4. Cyber crime against the society

Cybercrime against persons:

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation and also leave irreparable scars and injury on the younger generation, if not controlled.

It includes:

- Harassment via e-mails.
- Cyber-stalking.
- Dissemination of obscene material.
- Defamation.
- Unauthorized control/access over computer system.
- Indecent exposure.
- Email spoofing.
- Cheating & Fraud

Cybercrime against property:

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism i.e. destruction of others' property and the transmission of harmful programmes.

- Computer vandalism.
- Transmitting virus.
- Netrespass
- Unauthorized control/access over computer system.
- Intellectual Property crimes
- Internet time thefts

Cybercrime against the government:

The third category of cyber-crimes relate to Cybercrimes against government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments and cracking is amongst the greatest cyber-crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this the actuality is that no computer system in the world is cracking proof. It is unanimously agreed that any and every system in the world can be cracked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, Amazon and others are a new category of cyber-crimes which are slowly emerging as being extremely dangerous and also to terrorize the citizens of a country.

- Unauthorized control/access over computer system
- Possession of unauthorized information.
- Cyber terrorism against the government organization.
- Distribution of pirated software etc.

Against Society at large

- Pornography (basically child pornography).
- Polluting the youth through indecent exposure.
- Trafficking
- Financial crimes
- Sale of illegal articles
- Online gambling
- Forgery

The above mentioned offences may discuss in brief as follows:

1. Harassment via e-mails

Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Recently a lady complained about the same. Her former boy friend was sending her mails constantly sometimes emotionally blackmailing her and also threatening her. This is a very common type of harassment via e-mails.

2. Cyber-stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc

3. Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography) /Polluting through indecent exposure-

Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing these obscene materials. Downloading through the Internet, obscene materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

4. Defamation

It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium. E.g. the mail account of Rohit was hacked and some mails were sent from his account to some of his batch mates regarding his affair with a girl with intent to defame him.

5. E mail spoofing

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

Rajesh Manyar, a graduate student at Purdue University in Indiana, was arrested for threatening to detonate a nuclear device in the college campus. The alleged e- mail was sent from the account of another student to the vice president for student services. However the mail was traced to be sent from the account of Rajesh Manyar.

6. Computer vandalism

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

7. Intellectual Property crimes / Distribution of pirated software-

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.

8. Cyber terrorism against the government organization

There is a compelling need to distinguish between cyber crimes and cyber terrorism. Both are criminal acts. A cyber crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of Osama Bin Laden, the LTTE, attack on America's army deployment system during Iraq war.

Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives"

Another definition may be attempted to cover within its ambit every act of cyber terrorism.

A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to

(1) Putting the public or any section of the public in fear; or

(2) Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

(3) Coercing or overawing the government established by law; or

(4) Endangering the sovereignty and integrity of the nation

And a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

9. Trafficking

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey.

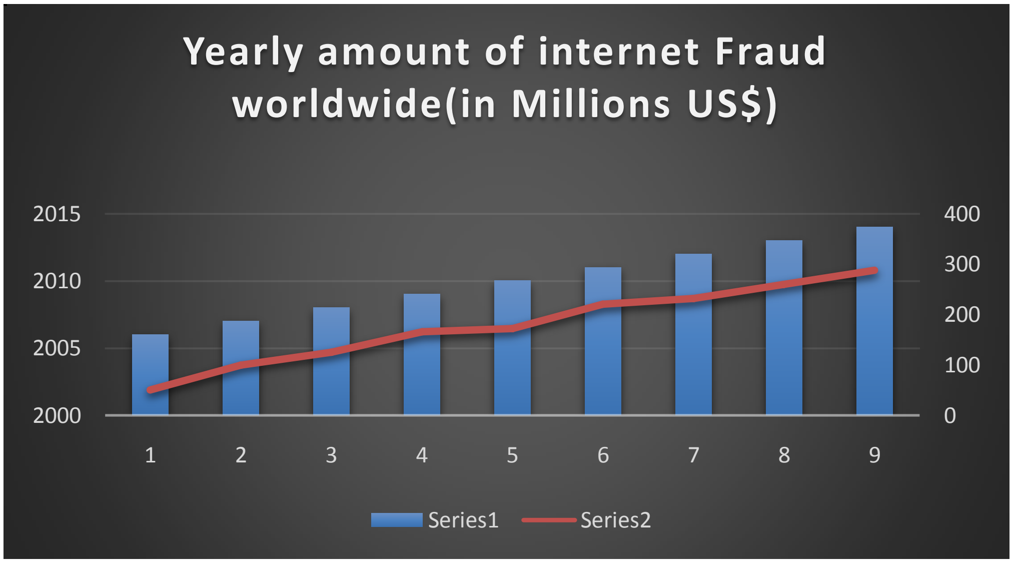
10. Fraud & Cheating

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

III DATA ANALYSIS AND FINDINGS

Yearly amount of cyber internet fraud worldwide

S.no	Year	Amount(in Million US $)
1.	2006	50
2.	2007	100
3.	2008	125
4.	2009	165
5.	2010	172
6.	2011	220
7.	2012	231
8.	2013	260
9.	2014	287



Source: - UN's Website (year 2015)

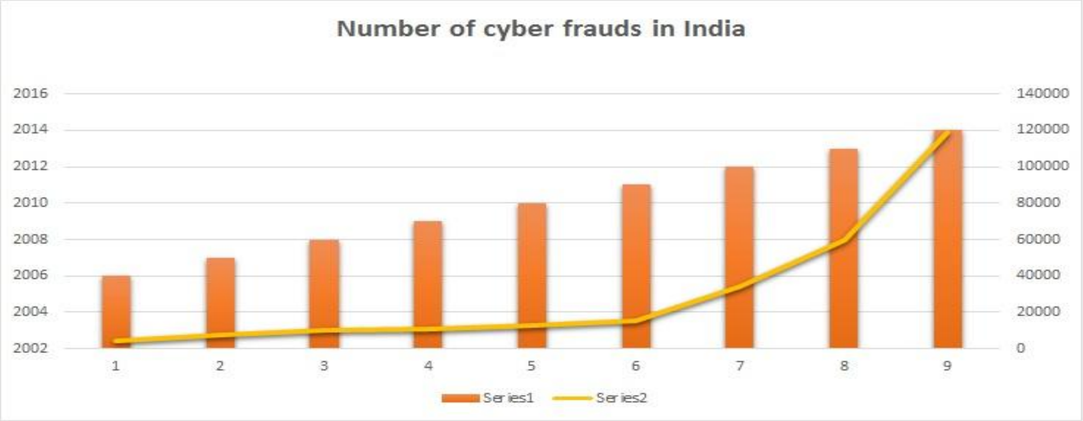
(http://www.un.org/en/development/desa/news/ecosoc/cybercrime-report-global-approach.html)

Interpretation:

Cybercrime is rising enormously year by year. In the year 2006 the amount or loss incurred by businesses due to cyber fraud was $50 million and it kept on rising and by the year 2014, it rose to $287 Million. As we can see there is 500% increase in the cybercrime worldwide from 2006 to 2014. Cybercrime is increasing day by day and people will have to be more smart and cautious while using computers or any smart phone or gadgets that have Internet in it.

Number of Cyber Fraud cases in India

S.No	Year	Total number of cases registered
1	2006	4214
2	2007	7756
3	2008	9912
4	2009	10927
5	2010	12831
6	2011	15625
7	2012	34456
8	2013	59854
9	2014	118917



Source: ASSOCHAM- Mahindra SSG Report, Jan 2015

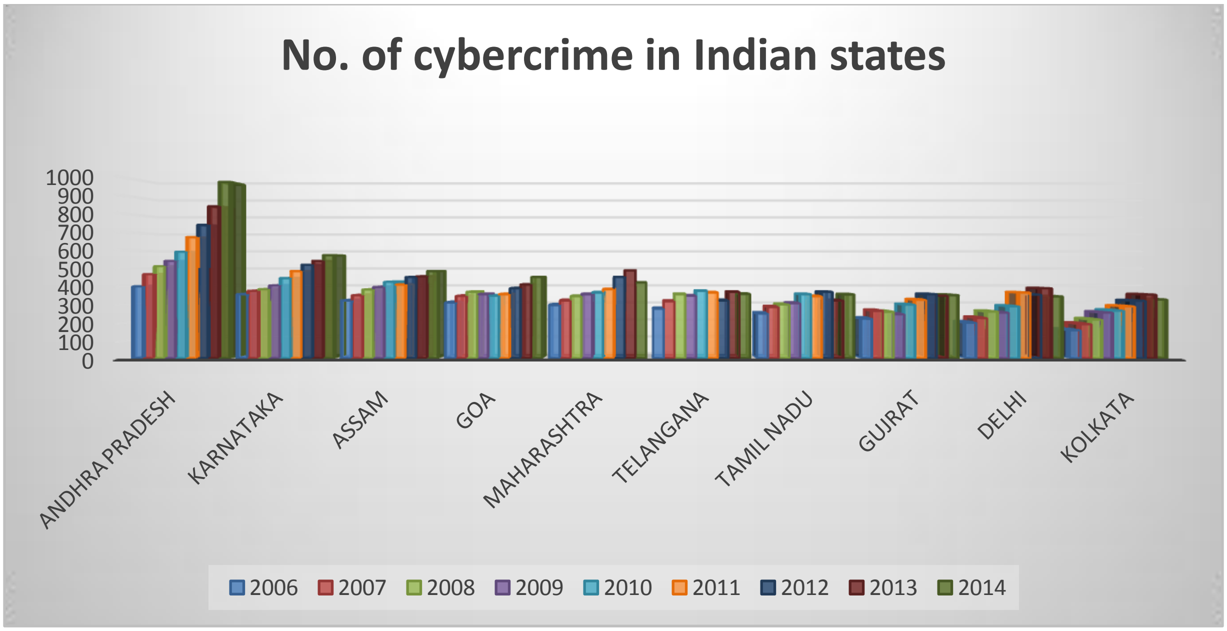
Source: ASSOCHAM's Website
(http://www.assocham.org/newsdetail/Report/cyberfraud/2015.php?id=482)

Interpretation

Cybercrime cases in India are rising at an alarming rate. As we can see, the number of cases registered every year is almost double that of the previous year. In 2006, the number of cases registered all over India was near to 4000 whereas if we compare this data with 2014, the number of cases registered is near to 1 lakh and 20 thousand. This drastic increase in the cases shows less cyber security amongst Indians. There is rise of 3000% cases registered from 2006 to 2014.

Number of Cybercrime in Indian states

no.	States	2006	2007	2008	2009	2010	2011	2012	2013	2014
1	Andhra Pradesh	400	468	512	542	593	674	742	846	981
2	Karnataka	356	375	384	405	446	485	520	542	574
3	Assam	321	350	382	396	425	410	452	456	485
4	Goa	310	346	369	356	348	356	389	410	452
5	Maharashtra	296	321	345	356	365	384	452	489	421
6	Telangana	275	317	356	348	374	365	321	369	357
7	Tamil Nadu	249	285	299	306	356	345	369	321	355
8	Gujrat	220	264	258	245	298	325	356	348	351
9	Delhi	198	224	259	254	289	365	354	389	344
10	Kolkata	156	190	215	254	265	289	320	354	327



Source: -Home ministry's Website (year 2015)

(http://ijecs.in/issue/cybercrime/states/reportv2-i8/41%20ijecs.pdf)

Interpretation: The highest Cybercrime is in Andhra Pradesh as we can see. The least cybercrime state is Kolkata. As we can see the number of cases registered in every state is rising year by year. In 2006 the number of cases registered in Andhra Pradesh was 400 and in the year 2014 it rose to 914. This clearly states that the cyber security is less in India as compared to other countries.

The state with the least cybercrime is Kolkata. The numbers of cases registered in 2006 were 156 and in 2014 are 327.

Total loss incurred by Hospitality industry and Aviation industry from 2006 to 2014 due to cyber attacks

Industry	Financial Loss	Cost of recovery	Loss of Business	Total Cost/ Lost	Number of total Incidents per Industry	Average cost Per Attack
Telecom Technology	$943724	$547299	$397097	$1882120	796	$2364
Airlines	$492755	$263410	$524509	$1280674	765	$1674
Financial	$388437	$257248	$263642	$909327	2039	
Utilities/ Infrastructure	$154599	$403349	$11199	$569147	625	$911
Hospitality	$398556	$70096	$145396	$614048	1424	$431
Aerospace and defence	$104600	$67200	$1800	$173600	217	$800
Total Loss/ Cost	$2482671	$1608602	$2237643	$5328916		

Interpretation

Total Loss Incurred by telecom industry Worldwide annually

- One Million and eight hundred thousand Dollars was the financial loss which telecom industry incurred due to cyber attacks.
- Cost of recovery was $547299. I.e. this is the cost which was recovered by the telecom industry.
- Average cost per cyber-attack was $2364

Total Loss Incurred by Airline Worldwide annually

- One Million and Two hundred thousand Dollars was the financial loss which Airline/Shipping industry incurred due to cyber attacks.
- Cost of recovery was $263410. I.e. this is the cost which was recovered by the Airline industry.
- Average cost per cyber attack was $800

Total Loss Incurred by Hospitality Industry Worldwide annually

- Six hundred and fourteen thousand Dollars was the financial loss which Hospitality industry incurred due to cyber attacks.
- Cost of recovery was $70096. I.e. this is the cost which was recovered by the telecom industry.
- Average cost per cyber attack was $800

Total Loss Incurred by Aerospace and defence Worldwide annually

- One hundred and seventy three thousand Dollars was the financial loss which Aerospace industry incurred due to cyber attacks.
- Cost of recovery was $67200. I.e. this is the cost which was recovered by the telecom industry.
- Average cost per cyber attack was $2364
-

IV Conclusion

Cybercrime is already a big problem all over the world—and its growing fast. The law enforcement world is scrambling to catch up; legislators are passing new laws to address this new way of committing crime, and police agencies are forming special computer crime units and pushing their officers to become more technically savvy.

However, the cybercrime problem is too big and too widespread to leave to politicians and police to solve. The former often don't have the technical expertise to pass effective laws, and the latter lack sufficient training, manpower, and time—not to mention the confusing issue of jurisdiction—to tackle any but the most egregious of Internet crimes.

Cybercrime, like crime in general, is a social problem as well as a legal one. To successfully fight it, we must engage people in the IT community (many of whom might be reluctant to participate) and those in the general population who are affected, directly or indirectly, by the criminal activity that has found a friendly haven in the virtual world.

We can use a number of tactics and techniques, including the legal system, peer pressure, and existing and emerging technologies, to prevent cybercrime.

Failing that, we can develop formal and informal responses that will detect cybercrime more immediately, minimizing the harm done and giving us more information about the incident, maximizing the chances of identifying and successfully prosecuting the cybercriminal.

We're all in this boat together. The only way to stop cybercrime is to work

together and share our knowledge and expertise in different areas to build a Class A cybercrime-fighting team.

References

Barker, M., S. Page, and D. Meyer (2002). "Modelling Tourism Crime: The 2000 America's Cup." *Annals of Tourism Research* 29(3):762–782.
Brunt, P., and Z. Hambly (1999). "Tourism and Crime: A Research Agenda." *Crime Prevention and Community Safety: An International Journal* 1(2):25–36.
Chesney-Lind, M., and I. Lind (1986). "Visitors as Victims: Crimes Against Tourists in Hawaii." *Annals of Tourism Research* 13:167–191.
Crotts, J. (1996). "Theoretical Perspectives on Tourist Criminal Victimization." *Journal of Tourism Studies* 7(1):2–9.
DeAlbuquerque, K., and J. McElroy (1999). "Tourism and Crime in the Caribbean." *Annals of Tourism Research* 26(1):968–984.
Ferreira, S., and A. Harmse (2000). "Crime and Tourism in South Africa: International Tourists' Perception and Risk." *South African Geographical Journal* 82(2):80–85.
Florida Department of Law Enforcement (1996). *Visitor Crime in Florida: The Perception vs. the Reality*. Tallahassee: Florida Department of Law Enforcement.
Flynn, D. (1998). *Defining the "Community" in Community Policing*. Washington, D.C.: Police Executive Research Forum.
Fujii, E., and J. Mak (1980). "Tourism and Crime: Implications for Regional Development Policy." *Regional Studies* 14:27–36.

Harper, D. (2001). "Comparing Tourists Crime Victimization." *Annals of Tourism Research* 28(4):1053–1056.

Honolulu Police Department (1998). "Herman Goldstein Award Nomination: District 4." Submission to the Herman Goldstein Award for Excellence in Problem-Oriented Policing.

Ishikawa, S. (2002). "Theft Poses Challenge for Hawaii's Tourism*."Honolulu Advertiser*, November 18.

McIntosh, R., and C. Goeldner (1986). *Tourism Principles, Practices, Philosophies.* New York: Wiley.

McPheters, L., and W. Stronge (1974). "Crime as an Environmental Externality of Tourism: Miami, Florida." *Land Economics* 50(2):288–292.

Metro-Dade Police Department (1996). "Tourist-Oriented Police Program." Submission for the Herman Goldstein Award for Excellence in Problem-Oriented Policing.

Pelfrey, W. (1998). "Tourism and Crime: A Preliminary Assessment of the Relationship of Crime to the Number of Visitors at Selected Sites." *International Journal of Comparative and Applied Criminal Justice* 22(2):293–304.