A Review on Cyber Crime

Poonam Gupta[#1], Vikas Sannady[*2]
[#]*Asst.Professor, Department of Computer Science, GTBCPTE, Bilaspur, chhattisgarh, India*
[1]*poonamgupta.90@gmail.com*
[*]*Asst.Professor, Department of Computer Science, GTBCPTE, Bilaspur, chhattisgarh, India*
[2]*vikassannady@gmail.com*

***Abstract*— the growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the World, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. Cyber attacks can come from internal networks, the Internet, or other private or public systems. In this manuscript we deal with the survey reports of India and also statistics of cyber crime in India as well as cyber user in world.**

***Keywords*— cybercrime, Indian cyber-crime statistics, statistics of world cyber users, cyber-attack.**

INTRODUCTION

Cyber criminals around the world lurk on the net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. Headlines of cyber attacks command our attention with increasing frequency [1]. In the current scenario the modern person can steal more with a computer than with a gun. Tomorrow's person may be able to do more damage with a computer than with a missile. Cyber space is broad spectrum including cyber crime, computer, net banking, web engineering, storage media, networking tools. In a current scenario any computer expert able to destroy our cyber legal Frame work means if any people having a computer and internet connection mean it is fully open system for hackers and that why computer experts and hackers hack the any system and perform illegal activities with the help of these weapons and that's why we required legal framework means cyber laws for executing all transaction in smooth way. In a current era cyber experts or hackers are very smart and use the latest technology for hacking they know all the cyber laws and find out the loopholes within that law and perform the illegal activities [2]. A Cybercrime can be considered to be an electronic version of traditional crime. There are variety of Cybercrime and some common type of Cybercrimes are described below in brief –

1. **Hacking:** It is an electronic intrusion, or gaining access to resources like computer, e-mail or social networking accounts such as Face book, Orkut, Gmail, and Hotmail etc. via a computer or network resource without permission.

2. **Spoofing:** It is a technique whereby a fraudster pretends to be someone else's email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster's newly created fraudulent web site.

3. **Phishing:** Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dope the victim into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim, usually via email is provided with a hyperlink that directs hi/her to a fraudster's web site. This fraudulent web site's name closely resembles the true name of the legitimate business.

4. **Cyber Bullying:** Acts of harassment, embarrassment, taunting, insulting or threatening behavior towards a victim by using internet, e-mail or other electronic communication device [3].

5. **Cyber trafficking:** It may be trafficking in weapons, drugs, human beings, which affect the large numbers of persons.

6. **Spreading computer virus:** It is a set of instruction which is able to perform some malicious operations. Viruses stop the normal function of the system programs and also to the whole computer system. They can also ruin/mess up your system and render it unusable without reinstallation of the operating system A computer viruses can be spread through Emails, Cds,Pendrives(secondary storage),Multimedia, Internet[4].

7. **Computer Fraud:** It is one of the most rapidly increasing forms of computer crime. It is also commonly referred to as Internet fraud. Essentially, computer or Internet fraud is "any type of fraud scheme that uses one or more components of the Internet-such as chat rooms, e-mail, message boards, or Web sites to present fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme"

8. **Identity Theft:** When someone appropriates anthers personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

9. **Credit/Debit Card Fraud:** It is the unauthorized use of a credit/debit card to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in an identity theft scheme.

10. **Denial of Service:** A denial of service attack is a targeted effort to disrupt a legitimate user of a Service from having access to the service. Offenders can limit or prevent access to services by overloading the available resources, changing the configuration of the service's data, or physically destroying the available connections to the information [3].

11. **Cross-site Scripting:** Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. Reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc are use for Reflected XSS attack.

12. **Cracking:** It is a dreadful feeling to know that a stranger has broken into user computer systems without user's knowledge and consent and has tampered with precious confidential data and information. Cracker are differ with hacker because hacker are hired by companies to audit network security or test software but cracker do same work for their own profit or to harm others[5].

RELATED WORK

Hemraj Saini et.al proposed the current manuscript provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes [6].

Ravikumar S.Patel et.al describes the The main reason behind the increasing this types of activities is vulnerabilities of Indiancyber laws and procedure of handling the cybercrime related cases [2].

Shubham Kumar et.al discussed various categories and cases of cyber-crime which is committed due to lack of knowledge or sometimes due to intention behind. I also, suggested various preventive measures against these unlawful acts in day to day life[4].

Mohit Goyal has discussed in his article is an attempt to provide a glimpse on cyber crime in India. This article is based on various reports from news media and news portal [7].

V.Karamchand Gandhi proposed in this paper is based on various reports from news media and news portal. [8].

Er. Harpreet Singh Dalla et.al has suggested various preventive measures to be taken to snub the cyber crime [9].

Rupinder Pal Kaur discussed statistics of crime cases which were happened in last few years and compared crimes happened in 2012 with previous years and also discussed what type of crimes are on increase and decrease [10].

CURRENT CYBERCRIME SCENARIO IN INDIA

Given the growth of cybercrime incidents in India, boards and CXOs are forced to take cognizance of this menace. With confidential strategic data, operational information at stake and reputation on the line, organizations are now beginning to realize the need for building their cyber defenses to limit the damage from cyber attacks. As managements work on building a cyber defense strategy, it is vital for organizations to have an understanding of the looming cyber threat and knowledge of how the business community as a whole is responding. Our survey report provides corporate India's perspective on cybercrime which is summarized as under:

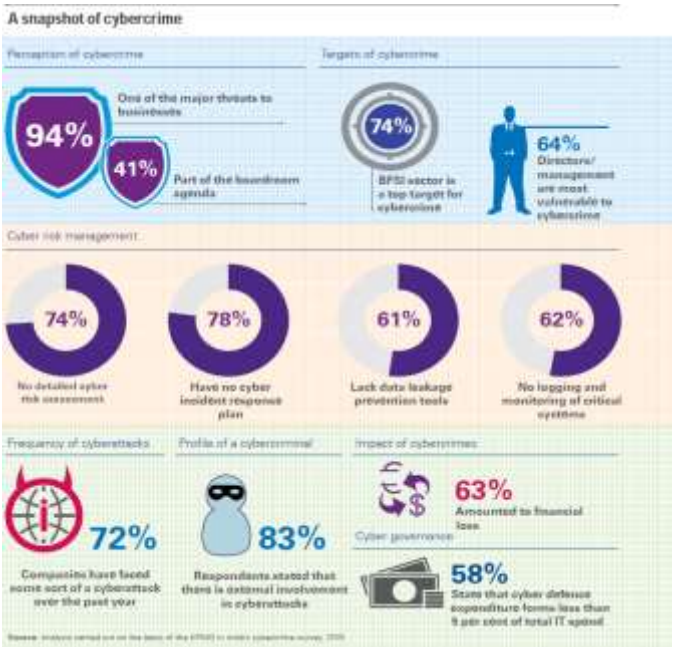


FIGURE I

IMPACT OF CYBERCRIME IN INDIA

Given the growth witnessed by Indian companies and internet penetration, India is now becoming a more integrated part of the global cyber village. Due to this, the number of companies and individuals having online presence has grown phenomenally as technology platforms provide the ease of leveraging the internet for conducting business and financial transactions. As businesses open themselves up to technology, They are exposed to the risk of cybercrime, which Can have far-reaching damages including:

— financial loss,
— loss of reputation,
— operational loss, i.e. impact on physical safety of
Employees and assets, closure of factory/plant Operations. While cybercrime may have the aforementioned direct impacts, it can also have an indirect impact such as large regulatory fines, contractual penalties and litigation.

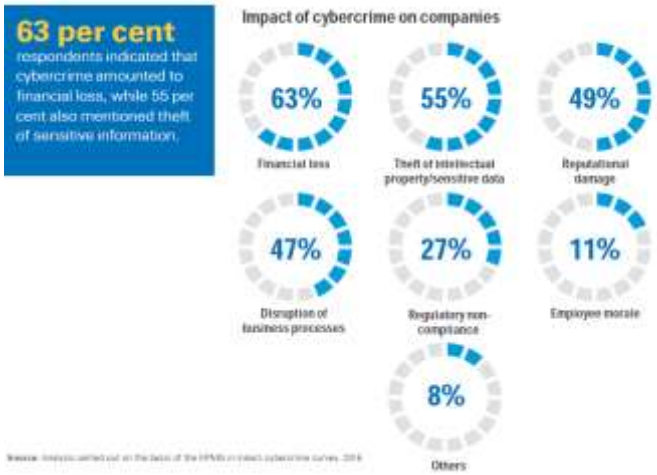


FIGURE II

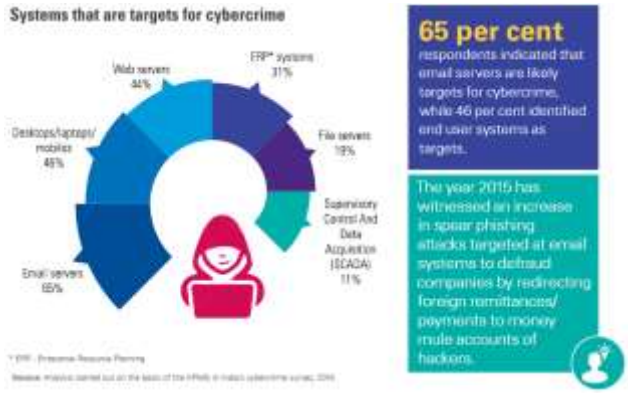


FIGURE III

INDUSTRIES THAT ARE TARGETS FOR CYBERCRIME

The type of industries that are most prone to cyber attacks Depend on multiple factors, such as:

- Profile of the attacker
- Motivation of the attacker, Strength of cyber laws
- Cyber security culture at an industry level
- Efficiency of law enforcement agencies to track cybercriminals
- Efficiency of the judiciary to evaluate the nature of the

Crime and deliver judgments/ conviction. Apart from the aforesaid external factors, a key aspect that also determines the susceptibility to cybercrime of a particular

Industry is the nature of data it holds, as well as the value of the data that can be fetched by the cybercriminal, if they were to sell it on the dark net.

FIGURE IV

TYPE OF PERSONNEL PRONE TO CYBER ATTACKS

With the growing ease of transacting technology, people extensively use their computers and mobile phones to carry out banking transactions, to avoid the hassle of long queues and travel. While people leverage on technology to a large extent, the same cannot be said about them using technology in a secure manner. From sharing passwords, to working on malware infected devices, to banking transactions; people make silly yet serious follies that make them vulnerable to cybercriminals. Cybercriminals thrive on three key elements people in general ignore. Firstly, not securing their digital devices; secondly, sharing/insecurely storing access credentials; and lastly, willingness to share personal data with unknown people. Due to these aspects, cybercriminals are able to successfully pull off socially engineered attacks, website spoofing and phishing attacks.

FIGURE V

PROBABLE INTENTIONS BEHIND CYBERATTACKS

As mentioned earlier, cybercriminals operate with different motives in their mind. In order to effectively manage cyber threats, it is vital for organizations to understand the motives behind cyber attacks due to the following reasons:

- Motives of the attack have a critical bearing on the technique used in the attack, which can at times give clues on the potential perpetrators.

• Motives of the attack also help affected companies design their cyber defenses. Some of the typical motives cyber criminals have for carrying out the attacks are as under:
• Financial fraud and embezzlement & Business disruption
• Theft of intellectual property/ sensitive information
• Skill testing for new hackers
• Cyber terrorism to cause grievous damage to a country's Strategic assets/general public safety
• Social causes, Political causes [11].

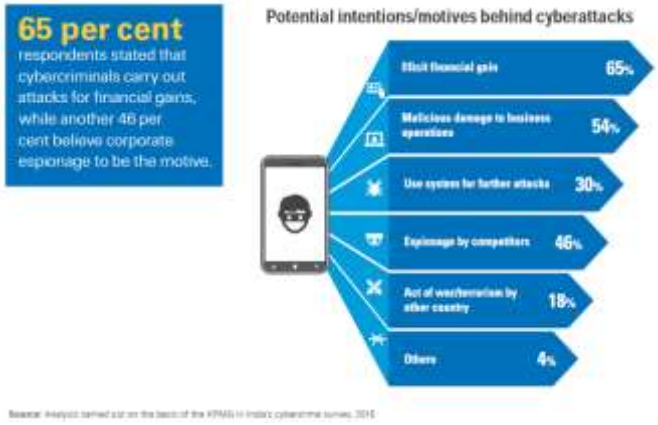


FIGURE VI

TABLE I
STATISTICS OF CYBERCRIMES IN INDIA

Cases Reported and Persons Arrested under Cyber Crime And Their Percentage Variation in 2014 Over 2013

S.No.	State/UT	Cases Reported under Total Cyber Crimes			Persons Arrested under Total Cyber Crimes			Percentage Share of Cases Reported under Cyber Crimes during 2014
		2013	2014	% Variation	2013	2014	% Variation	
(1)	(2)	(4)	(4)	(5)	(6)	(7)	(8)	(9)
STATES:								
1	Andhra Pradesh	651	282	-	515	298	-	2.9
2	Arunachal Pradesh	10	18	80.0	5	2	-60.0	0.2
3	Assam	154	379	146.1	2	351	17450.0	3.9
4	Bihar	139	114	-18.0	229	111	-51.5	1.2
5	Chhattisgarh	101	123	21.8	50	105	110.0	1.3
6	Goa	58	62	6.9	11	14	27.3	0.6
7	Gujarat	77	227	194.8	65	178	167.7	2.4
8	Haryana	323	151	-53.3	194	121	-37.6	1.6
9	Himachal Pradesh	28	38	35.7	13	16	23.1	0.4
10	Jammu & Kashmir	46	37	-19.6	16	4	-75.0	0.4
11	Jharkhand	26	93	257.7	20	57	185.0	1.0
12	Karnataka	533	1020	91.4	104	372	257.7	10.6
13	Kerala	383	450	17.5	169	283	67.5	4.7
14	Madhya Pradesh	342	289	-15.5	177	386	118.1	3.0
15	Maharashtra	907	1879	107.2	603	942	56.2	19.5
16	Manipur	1	13	1200.0	0	3	-	0.1
17	Meghalaya	17	60	252.9	0	12	-	0.6
18	Mizoram	0	22	-	0	4	-	0.2
19	Nagaland	0	0	-	0	0	-	0.0
20	Odisha	104	124	19.2	62	17	-72.6	1.3
21	Punjab	156	226	44.9	133	159	19.5	2.3
22	Rajasthan	297	697	134.7	151	248	64.2	7.2
23	Sikkim	0	4	-	0	2	-	0.0
24	Tamil Nadu	90	172	91.1	97	120	23.7	1.8
25	Telangana	-	703	-	-	429	-	7.3
26	Tripura	14	5	-64.3	13	1	-92.3	0.1
27	Uttar Pradesh	682	1737	154.7	602	1223	103.2	18.1
28	Uttarakhand	27	42	55.6	6	39	550.0	0.4
29	West Bengal	342	355	3.8	209	212	1.4	3.7
	TOTAL STATE(S)	5508	9322	69.2	3144	5643	74.0	96.9
UNION TERRITORIES:								
30	A & N Islands	18	13	-27.8	3	5	66.7	0.1
31	Chandigarh	11	55	400.0	9	45	400.0	0.6
32	D&N Haveli	0	3	-	0	1	-	0.0
33	Daman & Diu	1	1	0.0	2	2	0.0	0.0
34	Delhi UT	150	226	50.7	41	56	36.6	2.3
35	Lakshadweep	0	1	-	0	0	-	0.0
36	Puducherry	5	1	-80.0	2	0	-100.0	0.0
	TOTAL UT(S)	185	300	62.2	57	109	91.2	3.1
	TOTAL ALL INDIA	5693	9622	69.0	3201	5752	74.3	100.0

Source: www.ncrb.gov.in

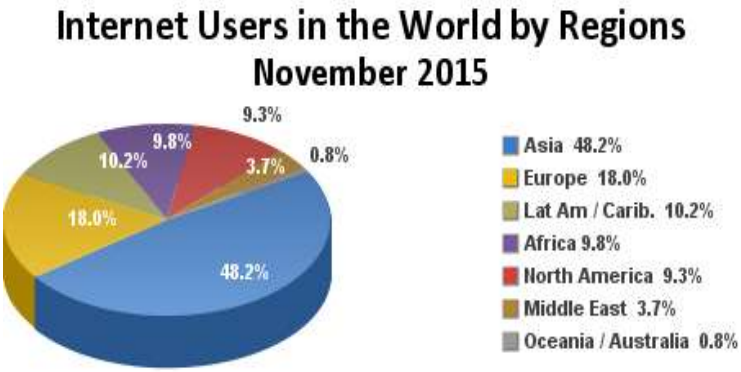
TABLE II

FIGURES AT A GLANCE - 2014

SL NO.	CRIME HEADS	CASES REPORTED	% TO TOTAL IPC CRIMES	RATE OF CRIME	CHARGE-SHEETING RATE	CONVIC-TION RATE
	CYBER CRIMES					
1	Total Offences under IT Act	7201	0.3	0.6	52.4	26.3
2	Total Offences under IPC (cyber related)	2272	0.1	0.2	66.8	35.3
3	Total SLL Offences (cyber related)	149	0.0	0.0	97.3	17.5
	Total cyber crimes (1+2+3)	9622	0.3	0.8	57.0	23.9

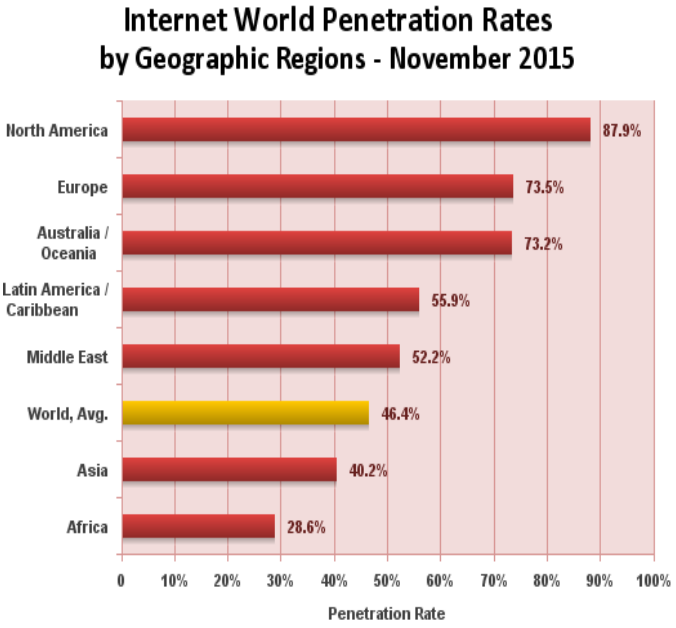
Source: www.ncrb.gov.in [12]

STATISTICS OF CYBER USERS IN WORLD



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,366,261,156 Internet users on November 30, 2015
Copyright © 2015, Miniwatts Marketing Group

FIGURE VII



Source: Internet World Stats - www.internetworldststs.com/stats.htm
Penetration Rates are based on a world population of 7,259,902,243 and 3,366,261,156 estimated Internet users on November 30, 2015.
Copyright © 2016, Miniwatts Marketing Group

FIGURE VIII

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,366,261,156 Internet users on November 30, 2015
Copyright© 2015, Miniwatts Marketing Group

INTERNET USAGE STATISTICS
The Internet Big Picture
World Internet Users and 2015
Population Stats

WORLD INTERNET USAGE AND POPULATION STATISTICS NOVEMBER 30, 2015 - Update						
World Regions	Population (2015 Est.)	Population % of World	Internet Users 30 Nov 2015	Penetration (% Population)	Growth 2000-2015	Users % of Table
Africa	1,158,355,663	16.0 %	330,965,359	28.6 %	7,231.3%	9.8 %
Asia	4,032,466,882	55.5 %	1,622,084,293	40.2 %	1,319.1%	48.2 %
Europe	821,555,904	11.3 %	604,147,280	73.5 %	474.9%	18.0 %
Middle East	236,137,235	3.3 %	123,172,132	52.2 %	3,649.8%	3.7 %
North America	357,178,284	4.9 %	313,867,303	87.9 %	190.4%	9.3 %
Latin America / Caribbean	617,049,712	8.5 %	344,824,199	55.9 %	1,808.4%	10.2 %
Oceania / Australia	37,158,560	0.5 %	27,200,530	73.2 %	256.9%	0.8 %
WORLD TOTAL	7,259,902,243	100.0 %	3,366,261,156	46.4 %	832.5%	100.0 %

FIGURE IX [13]

TURNAROUND AND TRANSFORMATION IN CYBERSECURITY: TELECOMMUNICATIONS

Telecommunications organizations are addressing escalating cyber-risks by implementing technologies such as cloud-based cyber security, Big Data analytics and advanced authentication. Additionally, more telecoms share cyber security threat intelligence with others than ever before. They also are investing in security: Following a slight decline last year, respondents boosted their information security budgets by 37% in 2015.

Protecting Customer Data:-

Telecoms typically store a huge amount of very detailed customer data that is of high value to certain adversaries. No wonder, then, that compromise of customer records—already the most frequently cited impact—climbed 25% in 2015.

At Home In The Internet Of Things:-

Some of the most promising opportunities of the Internet of Things are the digitally connected home and vehicle, segments that telecoms are well positioned to enter. There are serious privacy and security risks associated with connected homes and vehicles, however, since providers will amass and store an unprecedented amount of information about consumer activity and create points of access into home and car networks that did not exist five years ago. And the ecosystem is far from secure: Exploits of IT components such as operational systems, embedded devices and consumer technologies like home routers more than doubled in 2015.

Going Mobile With Payments:-

Contactless payment services represent a natural fit for telecommunications businesses, and many are partnering with technology companies, credit card issuers, banks and retailers to develop mobile payment systems that can drive new revenue streams. The fact that 64% of telecoms already accept mobile payments reflects the interest in this fast-growing segment. As with most technologies, however, adoption of new payment systems may bring unanticipated security risks. Compounding that, respondents reported a 40% increase in mobile device exploits in 2015.Many telecoms are proactively partnering with providers to help secure mobile payment services. They are helping to reduce fraud related to malware, verification, provisioning processes, device vulnerabilities, and protection of customer personal information [14].

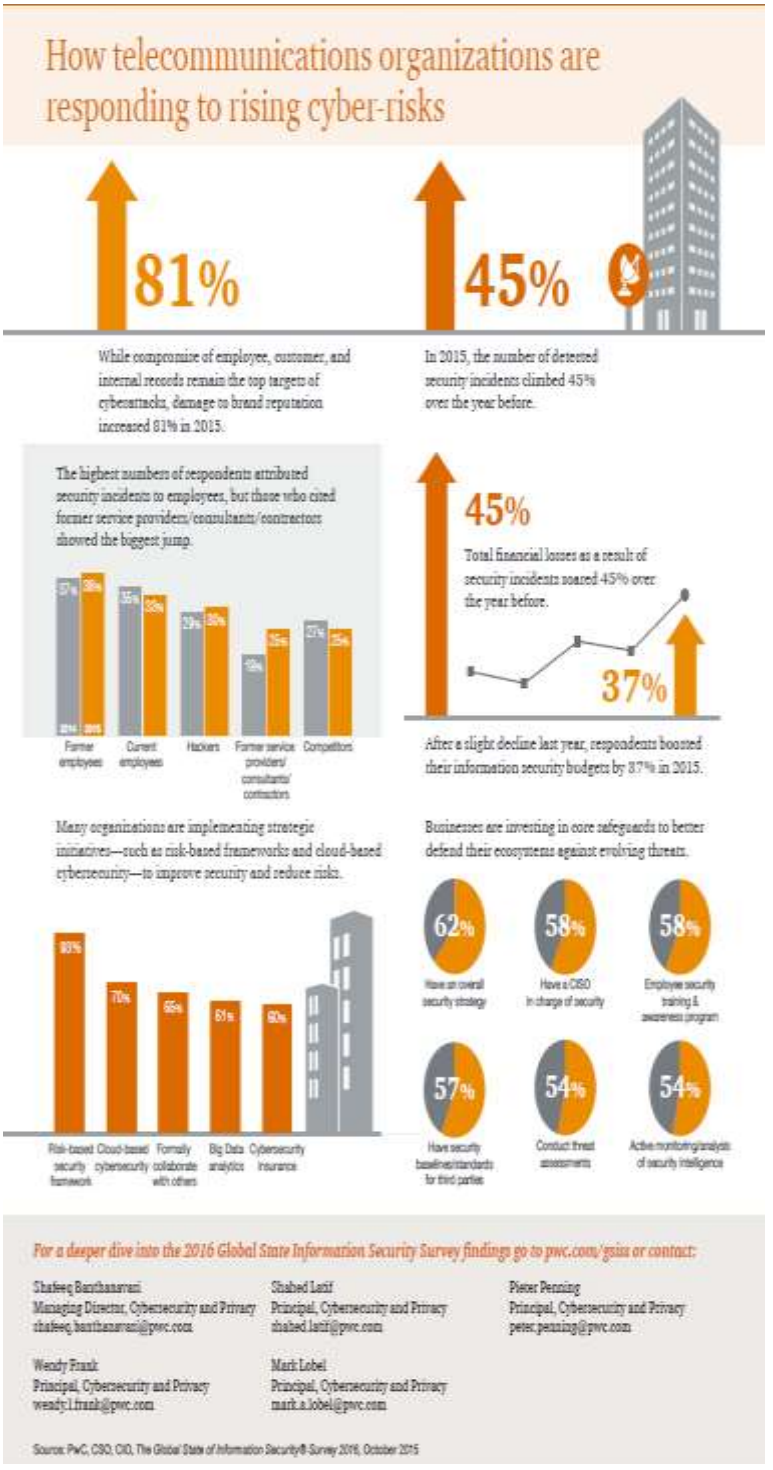


FIGURE X

CONCLUSION

Due to the increase in technology cybercrimes increases. Qualified people commit crime more so, there is need to know about principles and computer ethics for their use in proper manner. Cybercrime and hacking is not going away, if anything it is getting stronger. Cyber law will need to change and evolve as quickly as hackers do if it has any hopes of controlling cybercrime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The great thing about the internet is how vast and free it is.. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy. Yet India and world has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing time.

REFERENCES

- "CYBER CRIME AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION", ©Copyright 2000, McConnell International LLC. All Rights Reserved [1].
- RAVIKUMAR S. PATEL, DR.DHAVAL KATHIRIYA" Evolution of Cybercrimes in India", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 4, July – August 2013[2].
- Anand Kumar Shrivastav,Dr. Ekata,*"* ICT Penetration and Cybercrime in India: A Review ", International Journal of Advance Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013 ISSN: 2277 128X[3].
- Shubham Kumar, Dr.Santanu Koley,Uday Kumar," Present scenario of cybercrime in INDIA and its preventions", International Journal of Scientific & Engineering Research, Volume 6, Issue 4, April-2015 ISSN 2229-5518[4].
- Vineet Kandpal, R. K. Singh," Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013. Pp. 150-156 ©Copyright by CRDEEP. All Rights Reserved [5].
- Hemraj Saini, Yerra Shankar Rao, T.C.Panda, "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209[6]
- Mohit Goyal," ETHICS AND CYBER CRIME IN INDIA," International Journal of Engineering and Management Research, Vol. 2, Issue-1, Jan 2012 ISSN No.: 2250-0758[7].
- V.Karamchand Gandhi," An Overview Study on Cyber crimes in Internet", Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.1, 2012[8].
- Er. Harpreet Singh Dalla, Ms. Geeta," Cyber Crime – A Threat to Persons, Property,Government and Societies,"International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 ISSN: 2277 128X[9].
- Rupinder Pal Kaur," STATISTICS OF CYBER CRIME IN INDIA: AN OVERVIEW," International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume2 Issue 8 August, 2013[10].
- kpmg.com/in, Cybercrime survey report November 2015, KPMG in India[11].
- www.ncrb.gov.in[12].
- www.internetworldstats.com [13].
- The Global State of Information Security® Survey 2016[14].

