Cost of Cyber Crimes and Information Insecurity in India

Mukhtar Ahmad Sofi, Pondicherry University

ABSTRACT

In this era of technology, as the internet has become entrenched in the entire space of business and common life of the people, the higher trajectory of the so-called "cyber crime" has created an alarm for developed as well as developing countries. It (cyber crime) does encroach upon not only the confidential data of government but also the transactions carried out by the people using internet. This study covers some facets of cyber crime that are considered in the literature as having the most devastating consequences for the targeted individual or the entity. It addresses the region-wise and industry-wise phenomena of risk associated with cyber frauds besides giving the scenario for last several years. It also goes on to discuss the loss which India has suffered due to cyber-related frauds. Finally, it gives some solutions to prevent the data from being taken into control by the unauthorised users.

1. INTRODUCTION

Internet, with its advent in 1960s, while dramatically alleviating the world of communication and research by making available wealth of information at our finger prints, has also offered a way to a fraudulent to commit crimes effortlessly. In the contemporary world, as data transfer using internet has become a transcendent reality in private as well as in government arena, the emergence of cyber crimes at an alarming pace has placed a formidable challenge, nationally and/or internationally, to be dealt with. The term "Cyber crime" is defined as a criminal activity involving the use of computer or computer network for committing a crime, with both of them are bound to be tools as well as targets -- cyber crimes include, piracy and counterfeiting, intellectual property fraud, and identity theft. More generally, a cyber crime encompasses everything that ranges from electronic cracking to hacking of websites and denial of online services. Notwithstanding a sufficient awareness of the aforementioned various facets of cyber crimes, the respondents are not equipped to get away with the same owing to the lack of knowledge as to how such frauds are actually carried out.

With information and cyber insecurity as one of the prey of cyber crimes, the India Risk Survey 2012 places it at number one, and thereby posits it as a serious concern. Pertaining to information-related cyber crimes, one of the serious and growing concern is the so-called "Information Espionage". It involves the extraction of confidential information without the holder being kept privy of.

India, as being a developing country with growing trajectory of internet usage on the one hand and the lack of adequate expertise and knowledge of cyber crime prevention on the other, was put at 5th rank by the country's Home minister in terms of number and growth of cyber crimes, during NASSCOM Global leadership Awards. The number of cyber crimes in India are increasing at a spiralling pace, with the annual growth rate of about 50 per cent. Over last five years, more than 9,000 websites, including those of government departments carrying sensitive information have been hacked. According to sources, the government websites have become prone to cross-border hacking especially to countries like; Pakistan, China, Bangladesh and Nepal. In the Indian context, the major cyber crime instances or threats are reported as; SPAM, computer viruses and worms, denial of services, cyber stalking and phishing, defacement of websites, pornography and cyber squatting. Meanwhile, the information espionage is still posing a severe threat to companies despite the establishment of Information and Technology (Amendment) Act - 2008 -- it lays down provisions related to piracy and cyber terrorism, and data protection. While setting out to create a high performance culture, organisation must strategically come up with a comprehensive fraud risk management frameworks to mitigate the cyber frauds, which have become more sophisticated over time -- it calls for creating strong controls and pro-active supervision to deter the potential misbehaviour. All this require an apt use of technology and independent mentoring of key performance parameters.

This paper is an attempt to draw attention of the researchers and policy makers to the challenges put forth by spurt in the cyber crimes over last one decade besides bring into light the latest experiences of cyber fraud suffered by organisation in corporate India. It describes the extent to which the corporate sector in India has managed or failed to combat the menace of cyber crimes and frauds.

2. TOP EMERGING FRAUDS

"Knowledge", as it is recognised undisputedly as a key organisational asset, is now becoming increasingly susceptible to fraudulent by different ways, as follows: Cybercrime, Intellectual Property fraud, including
counterfeiting and Piracy and Identity theft have been recognised as among the top emerging frauds.

2.1. Cyber crime
"Cyber crime" as defined above refers to any criminal activity involving the use of computer or computer network for committing a crime, with both of them are bound to be tools as well as targets.

A way to defraud individuals as well as entities -- Cyber crime -- has rendered business or individual, using internet, insecure. Sensitive data and money of companies is vulnerable to perpetrators besides the instances of cyber attacks, which are plotted to disrupt, in target organization, the vital operations and critical functions, thereby hurts the confidence of customers and financial loss -- resulting into degradation of market reputation.

A large chunk of population have revealed that, they intermittently have been receiving emails from their respective banks or the authorities thereof, asking or making requests regarding validation of user names and passwords and in some cases asking for sharing such details. Besides, it sometimes happened to be containing instructions -- asking to transfer money to some accounts unknown to us and bullying the users of the bad consequences, like seizing of the account or any other action, in case they fail to follow the instruction given. Such sort of communication is called as "Phishing" -- it is occupied a central focus in debates related to cyber crimes. More than seventy percent of the respondents have expressed their anxiety over experiencing or hearing about this kind of cyber crime. One of the new ways adopted by fraudulent is what is called as Smishing -- through SMSs to target cell phones and handheld devices. These kind of devices are also targeted through voice mails, called Vishing.

Alarmed by the unprecedented growth in the trajectory of cyber crimes during last six years -- almost ten-fold increase -- the RBI has issued advisory to customers warning them against such incidents. The menace of the cybercrime-oriented mails can be understood by knowing the fact that these have enabled the hacker or fraudulent to an extent, that they do not only get hold of the access to computer and compromise it, but also to the company's network as a whole.

Cyber crimes are likely to be manifested in several ways: Respondents, conscious regarding the data theft (eighty percent), Intrusions or hacking of network (seventy six percent) and virus/malware (seventy six percent) -- these figures quite concur with the figures at international level with the figures as: hacking (eighty one percent), malware (sixty nine percent) have dominated in the manifestation cyber crimes.

2.2. Intellectual property fraud, counterfeiting and piracy
With India being a knowledge economy where, intangible assets like R&D capital, intellectual property, brand equity etc constituting a notable proportion of firm's value of assets, it is revealed by The Conference Board that, book value forms now a minuscule portion of company's market value. Significant proportion of intangible assets is formed by intellectual property like, trademarks geographic indications, inventions and copyrighted material etc. The study quotes the example of the pharmaceutical sector where for some companies as much as two-thirds of their market value comprised of intangible assets. This being the case, any theft or counterfeit of intellectual property could adversely affect companies. A recent World Customs Organization report highlighted that, globally, in 2011 over 25,500 cases were reported involving the seizure of more than 143 million counterfeit and/or pirated articles. The study further indicated an increase in counterfeits of pharmaceutical products, and mobile phones and their accessories. In India counterfeits could comprise as much as 50 percent of all products one uses. It is therefore not surprising to note that 38 percent of respondents have highlighted intellectual property fraud, counterfeiting and piracy as areas of concern in the future.

2.3. Identity theft
Identity theft refers to accessing the personal identifiable information of entities or individuals, to encroach upon the information and to attain benefits which you were not entitled to, without their permission. The principal reasons explaining the increase in identity theft includes internet proliferation. The numbers of internet users, in India, have grown massively -- to 243 million in June 2014 from 7 million in 2001 -- and it is bound to jump up further towards 300 million mark by 2014. Although a number of measures in the form of regulations and controls are taken to protect the confidentiality, but the issues seem to be growing over time. Each of the remaining gaps in the measures are being exploited by the fraudulent to breach the confidential information of individuals and organization. According to reports like, Norton Cybercrime report 2011, the cybercrimes are as high (globally) as 431 million adults have become its victims, whereas, more than one million adults fell prey per day. The report also shows that India is one of the fastest among emerging as a soft target for organized cybercrime -- 80 per cent of online adults have suffered the identity theft in 2011. As most of the employees in corporate world make use of their office laptops or for their personal transaction ranging from online shopping to online banking, therefore, they are susceptible to identity theft and thereby not only
their private information is at risk but also the information of the companies they work in.

3. PERCENTAGE RISK OF INFORMATION AND CYBER INSECURITY ACCORDING TO REGIONS IN INDIA

Cyber insecurity has been observed as one of the main risks affecting the business of India while analysing overall risks as per the geographic locations. The percentage risk of cyber frauds has been observed less in 2013 as compared to 2012 with no decline in cyber frauds, but the percentage of cyber frauds was affected by the increase in other types of risks like ‘Political and governance instability’, ‘Strikes, Closure and unrest’, etc.

Source FICCI-Pinkerton survey-2013/India Risk Survey-2013

‘Political and Governance Instability’ and ‘Strikes, Closures and Unrest’ emerged as risk number one and two respectively in 2012-2013 because of political violence in different regions of India. In Northern region ‘Information and Cyber Insecurity’ occupied 4th position among all major risks with 9.58 percent while occupied 2nd position in Southern Region with 11.10 percent. West region reported 9.31 percent risk of Cybercrimes. For the eastern region, however, ‘Natural Hazards’ and ‘Terrorism and Insurgency’ become high priority risks. This may be because East Indian states viz., Orissa, Bihar, West Bengal have been struck hardest by natural calamities like cyclones, flash floods and fires. In addition, some of the districts in these states have a huge presence of Naxal insurgents, which of late has emerged as the single biggest internal security threat in India.

4. PERCENTAGE RISK OF INFORMATION AND CYBER INSECURITY ACCORDING TO INDUSTRY

In today’s environment every big business is weighed down with cyber insecurity risks which need to be avoided for stability and growth. An analysis of cyber insecurity risk perception and mitigation can be a useful tool in decision making.

Source FICCI-Pinkerton survey-2013
Financial services and information and entertainment sectors have been identified as most vulnerable to frauds like cybercrime, phishing and data theft. Interestingly, both sectors identified are heavy users of technology implying that while technology can be a great spur for the business nevertheless it can also offer an equally strong platform for committing frauds. Despite having a strong watchdog against the cyber breaches, the financial services sector has emerged as the most susceptible sector to cyber fraud. Possible misuse of technology in the banking sector includes use of banking access for overpayments to vendors/self bank account, sharing of potential confidential information and misuse of company’s technology resources for unauthorised activities including conflicting business relationship. Additionally, providing services on mobile and social media platforms with limited knowledge of the security requirements, poses threats to customers as well as financial institutions. In case of the information and entertainment sector, despite functioning as global entities and complying with stringent foreign legislations, they have been identified as the second most fraudulent sector in India. Thus, organisations need to be more proactive and adopt a zero tolerance approach towards Information and cyber insecurity risk management.

5. EVALUATION OF STATISTICS OF CRIMES COMMITTED IN LAST FEW YEARS AND 2013

NCRB (National crime records bureau) divides the statistics in two groups:
2) Cyber crimes registered under Indian Penal Code (IPC).

5.1. Cyber crimes registered under IT Act-2000:

Information on various crimes registered under IT Act-2000 is presented in Table 1

<table>
<thead>
<tr>
<th>Crime Types</th>
<th>Cases Registered</th>
<th>Persons Arrested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tampering computer source documents</td>
<td>94</td>
<td>161</td>
</tr>
<tr>
<td>Hacking</td>
<td>826</td>
<td>1,440</td>
</tr>
<tr>
<td>1) Damage to computer source</td>
<td>157</td>
<td>435</td>
</tr>
<tr>
<td>2) Hacking</td>
<td>496</td>
<td>589</td>
</tr>
<tr>
<td>Obscene publication in electronic form</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Unauthorized attempt to access to protected computer system</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Obtaining license or digital signature certificate by misrepresentation of facts</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Publishing false digital signature</td>
<td>26</td>
<td>46</td>
</tr>
<tr>
<td>Breach of confidentiality</td>
<td>157</td>
<td>176</td>
</tr>
<tr>
<td>Fraud digital signature certificate/privacy</td>
<td>157</td>
<td>176</td>
</tr>
</tbody>
</table>

Source-NCRB Report 2013

The NCRB report shows that the highest number of cybercrimes cases in 2013 were for “hacking with computer systems”. Transmission of obscene messages, or "obscene publication/transmission in electronic form" came a distant second in the category. A total 2,516 cases were registered in 2013 for hacking with computer systems with 1,011 arrests. The numbers for "obscene publications/transmission in electronic form", stood at 1,203 cases registered, with 737 arrests. Offences under "hacking of computer systems" are calculated under the two subheads of "loss/damage to computer resources/ utility" and "hacking".

The trends reveal a "maturing of the country's cybercrime economy. Hacking is no longer done to assert technological superiority, but for monetary gains. The case of a hacker Amit Tiwari from Pune, who was arrested earlier this year for compromising over a 1,000 email accounts both in India and abroad. He was a part of a global network of hackers".
As with technology progress, criminal minds are also getting activated more and more. According to NCRB report increase percentage in crimes of All type committed in 2012 and committed in 2013 is 64%. A total crime reported under IT act was 2876 in 2012 and crimes reported in 2013 are 4356. In 2012 the cases registered under categories of un-authorized attempt to access protected computer system decreased by 40% whereas in 2013 Variation of un-authorized attempt to access protected computer system increased by 800% and Publishing false digital signature by 300% which is an alarming issue to concentrate. Crime cell is also working its level best as persons arrested in 2013 for unauthorised access to computer system crime was only 1 and in 2013 are 17 with a variation of 1600 % for total 27 cases recorded. But there is also little bit relief because the cases registered under categories of tempering data decreases by 14.9% and decrease in cases registered under fraud digital signature certificate by 59.65% respectively. Although there is decrease in cases registered in above mentioned two categories but offenders are sharper as persons arrested under category of tempering data in 2012 were 104 for 161 cases registered but in 2013 persons arrested for same category were 59 for 137 cases registered. No person was arrested for publishing false digital signature certificate for one case registered under IT act 2000 in 2012 however eight persons were arrested for 4 cases in 2013.Total cases registered under IT act 2000 was 4356 in 2013 . Cybercrimes registered under the IT Act shot up by over 50% across the country between 2012 and 2013, shows the latest data released by the National Crime Records Bureau (NCRB). The maximum offenders came from the 18-30 age group. Among states, the highest incidents of cybercrime took place in Maharashtra (907) followed by Uttar Pradesh (682) and Andhra Pradesh (651). The maximum arrests for cybercrimes under the IT Act took place in Maharashtra: 426. Andhra Pradesh was a distant second with 296 arrests. Uttar Pradesh was third at 283 arrests. In percentage terms, the state that saw the most dramatic increase in cases registered under the IT Act was Uttarakhand at 475% (from 4 cases to 23); Assam a close second with 450% (from 28 cases to 154). Interestingly, the picture postcard union territory, Andaman and Nicobar islands, registered an eye-popping increase of 800% (2 cases in 2012 to 18 in 2013) in the same category.

5.2. Cases registered under IPC (Indian Penal Code):
Indian panel code is main criminal code. In IPC all the crimes are listed out which a criminal suppose to commit. Any person is punishable under IPC expect military and armed forces crimes. Cyber crimes which are not covered under IT act 2000 are registered under IPC. Information of cases registered under IPC is provided in Table 2.
## Crime Types

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Cases Registered</th>
<th>Persons Arrested</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Offence by /against public servant</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>False electronic servant</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Destruction of electronic evidence</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>10</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>Forgery</td>
<td>259</td>
<td>259</td>
<td>747</td>
<td>277</td>
<td>263</td>
<td>626</td>
</tr>
<tr>
<td>Criminal breach of trust/fraud</td>
<td>118</td>
<td>282</td>
<td>518</td>
<td>129</td>
<td>215</td>
<td>471</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.property mark</td>
<td>6</td>
<td>21</td>
<td>10</td>
<td>8</td>
<td>13</td>
<td>34</td>
</tr>
<tr>
<td>2.tampering</td>
<td>5</td>
<td>19</td>
<td>8</td>
<td>7</td>
<td>26</td>
<td>10</td>
</tr>
<tr>
<td>3.currency/stamps</td>
<td>17</td>
<td>5</td>
<td>41</td>
<td>11</td>
<td>10</td>
<td>49</td>
</tr>
<tr>
<td>Total</td>
<td>422</td>
<td>601</td>
<td>1337</td>
<td>446</td>
<td>549</td>
<td>1203</td>
</tr>
</tbody>
</table>

Source: NCRB Report 2013

The NCRB data shows that cybercrimes registered under the IT Act rose sharply by 51.5% from 2012 to 2013 and those registered under the Indian Penal Code, by 122.5% for the same time period. Both IT Act-2000 and IPC collectively constitute an increase of 63.73% overall. Only 23.5% of the cybercrime cases were registered under the IPC last year, while the majority -- 76.5% were registered under the IT Act.

In 2013 total cases registered under IPC section were 1337 under by reporting variation of 122.46% over 2012, as the cases reported in 2012 were 601. Among total 1337 cases registered, maximum cases were of Forgery as in 2012 cases reported were 259 but in 2013 were 747. Among the states Uttar Pradesh reported maximum number of cases registered (310) out of 1337 followed by Maharashtra (226), Haryana (211) and West Bengal (132).

For total 1337 cases registered 1203 criminal were arrested in 2013 under IPC among which 626(46.8%) offenders were arrested for crime under “cyber forgery”.
criminals arrested for breach of trust were 471 (39.15%). The states which report highest arrest rate were Uttar Pradesh (319), Bihar (207), Maharashtra (177), West Bengal (151).

6. CHARACTERISTICS OF OFFENDERS

According to NCRB Report, Nearly 50 per cent of those arrested for the cyber crimes - hacking, obscene publications and forgery etc belong to the age group of 18-30 years. Between 2008 and 2011, 1,184 persons were arrested for various cyber crimes, which are on the rise. In 2013, a total of 3301 persons were arrested for various cyber crimes under IT act and IPC. Most offenders belong to the younger generation. They are more aware of the ways and means through which they can exploit cyber space and come from a variety of backgrounds.

![Persons Arrested Under Cyber Crimes (IT Act + IPC Sections) - All India](image)

Source-NCRB Report 2013

Cases under obscene publications climbed to 1203 cases in 2013, with 62.08 per cent of offenders from the same age group. This offence also carries a three-year imprisonment term. Forgery cases rose by over 188.4 per cent between 2011 and 2013, the NCRB data has revealed. The number of reported cases has surged over the years because people are becoming more aware of these things. More number of people are reporting these crimes, especially in instances where there was a financial loss.

7. ESTIMATING THE COSTS OF CYBER CRIME

Considering the advantages of the cyber age and increasingly competitive corporate environment, cases of business information thefts are becoming more prominent. India loses approximately INR 34,110 crores annually due to cyber related crimes. Another major concern with cyber crimes is its low detection level and next to negligible prosecution. The monetary loss due to information theft is impossible to assess as it depends upon the nature of information stolen. However, such losses can neither be recovered through insurance coverage nor is the law able to protect from such incidents. In order to deal with such crimes, India should establish more Computer Emergency Response Teams (CERT) with an objective to coordinate and respond during major security threats. According to a study conducted by Ponemon Institute in partnership with Symantec revealed that Indian organisations spent an average of INR 53.5 million to remediate a data breach.

8. CONCLUSION

The Cyber crimes have been reported from almost every industrial and corporate hub of India. However, banking industry is found to be the most vulnerable to phishing attacks in India. There is a regular complaint from all the ensuing sectors about low understanding of technical skills by the law enforcement and judicial officials. From the above study the cases which are high in number are hacking and obscene publication under IT act-2000 and under IPC cases are of forgery. Hacking is the thing which needs more attention because most of data need security. Further, preventing, tackling and mitigating cyber crime incidents are seen as the responsibility of the information security team. This is challenging as the information made available to such teams (for investigation or establishing preventive mechanisms) is often internal company data and not the vulnerabilities or information access patterns of customers or business partners (classified as third party data). Therefore utilising limited data for investigating breaches does not help get an accurate picture of the gaps.
in the control systems. Also specific skills are required to investigate cyber incidents.

At an organisational level, Workshops as well as e-learning modules can be made available to employees to help them identify potential cyber crime related risks/scenarios. Trainings can also be conducted by experts to drive home the importance of preventing cyber crime. It is in the interest of companies to have an incident response plan, which defines a clear set of steps to be taken by the organisation in the event of a security breach. Organisations must set up a separate specialist team with prior experience of handling cyber breaches, to handle their cyber security and conduct investigations into any breaches. Alternatively, they can also hire specialist agencies to do this for them. As of now, there are only 18 cyber cells in major cities of India, but with increasing dependence on the internet, even smaller cities are registering a significant rise in the number of such cases. Incidences of cyber insecurity have affected every four out of five people using the internet. However, most cases go unreported in India. Lack of legal awareness related to cyber laws, lack of cyber law experts, insufficient number of cyber cells across country, interdependence of cyber world and most importantly, rise of a net savvy generation are chiefly responsible for making this risk very critical.

REFERENCES

[1] KPMG India Fraud Survey-2012
[2] ‘Cybercrimes shoot up by over 50% across India’, The Times of India, 2 July 2014
[3] ‘Cybercrime is the big dady of all crimes’, Indian Fraud Survey Report-2012
[16] India Risk survey 2013 Report by FICCI and Pinkerton - www.ficci.com