2011 3rd International Conference on Information and Financial Engineering
IPEDR vol.12 (2011) © (2011) IACSIT Press, Singapore

Economic Impact of Identity Theft in India: Lessons from Western Countries

Dr.P.Arunachalam

M.A (Loyola, Madras), M.Phil and Ph.D (CUSAT, Cochin), PDT (Tilburg University, the Netherlands),

Editor,

"International Journal of Marketing and Trade Policy"

Serials Publications, New Delhi,

Faculty Member, Head (2004-07), Department of Applied Economics, Cochin University of Science and Technology, Kochi-22. E.Mail: arunachalam14@yahoo.co.uk , 09746770732 (Cell), 0484 2577741.

Abstract. In this computerized, globalised and internet world our computer collects various types of information's about every human being and stores them in files secreted deep on its hard drive. Files like cache, browser history and other temporary Internet files can be used to store sensitive information like logins and passwords, names addresses, and even credit card numbers. Now, a hacker can get at this information by wrong means and share with someone else or can install some nasty software on your computer that will extract your sensitive and secret information. Identity Theft posses a very serious problem to everyone today. If you have a driver's license, a bank account, a computer, ration card number, PAN card number, ATM card or simply a social security number you are more than at risk, you are a target. Whether you are new to the idea of ID Theft, or you have some unanswered questions, we've compiled a quick refresher list below that should bring you up to speed. Identity theft is a term used to refer to fraud that involves pretending to be someone else in order to steal money or get other benefits. Identity theft is a serious crime, which is increasing at tremendous rate all over the world after the Internet evolution. There is widespread agreement that identity theft causes financial damage to consumers, lending institutions, retail establishments, and the economy as a whole. Surprisingly, there is little good public information available about the scope of the crime and the actual damages it inflicts. Accounts of identity theft in recent mass media and in film or literature have centered on the exploits of 'hackers' - variously lauded or reviled - who

are depicted as cleverly subverting corporate firewalls or other data protection defenses to gain unauthorized access to credit card details, personnel records and other information. Reality is more complicated, with electronic identity fraud taking a range of forms. The impact of those forms is not necessarily quantifiable as a financial loss; it can involve intangible damage to reputation, time spent dealing with disinformation and exclusion from particular services because a stolen name has been used improperly. Overall we can consider electronic networks as an enabler for identity theft, with the thief for example gaining information online for action offline and the basis for theft or other injury online. As Fisher pointed out "These new forms of high-tech identity and securities fraud pose serious risks to investors and brokerage firms across the globe,"

I am a victim of identity theft. Being a victim of identity theft I felt the need for creating an awareness among the computer and internet users particularly youngsters in India. Nearly 70 per cent of Indian‘s population are living in villages. Government of India already started providing computer and internet facilities even to the remote villages through various rural development and rural upliftment programmes. Highly educated people, established companies, world famous financial institutions are becoming victim of identity theft. The question here is how vulnerable the illiterate and innocent rural people are if they suddenly exposed to a new device through which some one can extract and exploit their personal data without their knowledge? In this research work an attempt has been made to bring out the real problems associated with Identity theft in developed countries from an economist point of view.

Key Words: Identity, cyber crime, internet security, cyber law, Identity fraud

We, the human beings, have always been threatened by different types of problems at different times. Certain problems are quite natural known as natural calamities like earthquake, drought, flood and tsunami etc. and certain problems are created by human beings or man made like melting of ice in Arctic and Antarctic regions, aids, terrorism, etc,. In addition to the above said problems in recent years human beings started facing one more major problem, which is threatening the human society as a whole, due to technology development, is identity theft or high tech cyber crime commonly known as. In this paper an attempt has been made to analyze various aspects of identity theft with respect to

How important identity is?

What are the problems associated with identity theft?

What are the safeguards mechanisms available with respect to identity theft?

What are the rules and regulations implemented by the government or associated with identity theft?

What would be the impact of identity theft on Indian economy?

This study is mainly based on secondary data published by government agencies like The Federal Trade Commission (FTC), USA and various Non –Governmental Organizations (NGO’s) functioning in India and abroad. Data have been collected through internet only.

Virtually anyone may become the victim of identity theft. Contrary to popular misconception, personal information is not stolen just from the affluent. Persons of even modest means may become victims of identity theft. In most cases all that are required is good credit, which is what identity thieves use to steal thousands upon thousands of dollars in the name of the victim. No particular age group is immune. Due to the common interest in the Internet, younger Americans may be victimized at a higher rate, which is the primary tool in many identity theft crimes. However, elderly Americans are highly vulnerable to other types of identity theft schemes, particularly the various telephone scams used by perpetrators to acquire personal information.

Some people have first encountered identity theft through appropriation of their email address or instant messaging service name, with a spammer for example using a name that appears on the web (on a personal

or corporate site or in a web newsgroup archive) as a false identity in messages to people across the globe. That theft is of concern because most of the online population has yet to recognize that email addresses are readily forged and thus assume that the owner of a stolen address has either authorized the message or has failed to maintain effective anti-virus protection and thereby allowed a spammer to propagate messages from a 'zombie' machine. Appropriation of an address or online name is also of concern because it may result in blockage of legitimate communications from the owner of that name, in some instances forcing the unfortunate owner to acquire a new name. Some observers have criticized vigilante online spam filters for simply blocking names without proper investigation. Name appropriation is not restricted to email addresses. Contacts in China have lamented that their online names in messaging services such as QQ and their avatars in gaming or other social networking spaces have been stolen, typically through surveillance while using a cybercafe. That theft poisons their online identity - the owner typically abandons the name/avatar - and can imperil online relationships.

Identity theft is the fastest-growing sector of crime not only in US and other developed countries but also in developing countries. Identity theft occurs when someone obtains your personal information, such as your credit card data or Social Security number, to commit fraud or other crimes. The Federal Trade Commission estimates that 9 million Americans suffer identity theft annually. It sounds like a big number, but it isn't. For one, the hysteria has been stoked by much-publicized data breaches. In reality, identity theft only touches a sliver of the U.S. population each year (about 3%). One-quarter of those cases are credit-card fraud and not full-blown identity theft, according to FTC figures. The credit-card fraud occurs when a thief uses your credit card to make purchases. More serious is when someone uses your information to open accounts or take loans in your name. That's when you'll have to fight to get your credit restored and your name cleared an arduous process that can take months or years to complete. In response to concerns over identity theft, numerous companies and financial institutions have stepped in with products that monitor your credit, reimburse you for lost wages or funds and guard your identity. Some employers also now offer ID theft insurance to help you reduce the amount of time and money spent resolving the crime, so check with your company's benefits specialist about your eligibility (guides.wsj.com). Of course, stealing your identity isn't much of a crime itself; it's what the criminal does with the information that's damaging like Credit card fraud, Phone and utilities scams and Draining bank accounts. Identity theft is a two-step process. First, someone steals your personal information. Next, they use that information to impersonate you and commit fraud. It's important to understand this two-step approach, because your defenses also must work on both levels. Protect your personal information diligently to avoid becoming a victim. If identity thieves can't access vital data like your social security or bank account numbers, they can't defraud you. Most identity theft occurs the old-fashioned way. Thieves' rifle through trash, steals mail, and use con games to trick you into revealing sensitive details. It's up to you to protect your personal information.

a. Don't give out your social security number over the phone.
b. Shred paperwork containing account information or personal identifiers.
c. Keep important documents in a locked safe.
d. Pick up and send sensitive mail at the post office.
e. Online identity theft is also a problem.
f. Notorious risks are posed by phisihing and pharming.

In these scams, thieves use fake emails and Web sites to impersonate legitimate organizations. Likewise, hackers and viruses can infiltrate your computer to steal data or capture account names and passwords as you type them (Symantech.com). I have given here some of the ways how hackers steal your identify. In fact I am a victim of identity theft. I would like to state my own experience here. I have received an account alert mail from yahoo service. I have listed some of the important cheating methods the hackers generally used to steal the personal id's of individuals.

Identity Theft and Assumption Deterrence Act of 1998 defines it as the illegal use of someone's "means of identification" - including a credit card. So if you lose your card and someone uses it to buy a candy bar,

technically you have been a victim of identity theft. The misuse of lost, stolen or surreptitiously copied credit cards is a serious matter, but it need not force anyone to hide in a cave. U.S. law caps personal liability at $50, and even that amount is often waived. Surveys have found that about two-thirds of Americans classified as identity theft victims end up paying nothing out of their own pockets. The more pernicious versions of identity theft, in which someone's name is used to open lines of credit or obtain government documents, are much rarer (iht.com).

High tech cyber crimes, also known as Identity Thefts, Cyber crime incidents are spreading like wild fire. In 2004, the UK lost about three billion pounds to unauthorized access, penetration into computer systems, data theft, virus attacks and financial frauds.
The FBI chief Chris Swecker reported to the US Senate Judiciary Committee that he "opened 1,081 investigations of Identity Thefts" and was carrying out over 1,600 "active investigations". In India, the security agencies lodged over 800 cases under the Information Technology Act 2000 and Indian Penal Code provisions, in 2002. In 2003, the number fell to about 500 cases. Speakers from India strongly believed most cases were not reported. Cyber crimes in India has an additional face, pornographic messaging. The 2004 figures are yet to be made available. The IT industry contributes $28 billion to India's GDP. The industry growth being at 18%, software services export has grown to 30 per cent in 2004 at $12.5 million. The country is mulling to invest about $500 every year in e-governance initiatives. Growth of cyber crimes is also fast (indiatimes.com).

According to a website that monitors cyber crimes, in 2006, identity theft complaints made up 37 per cent of all fraud complaints. Sharing personal information on social networking sites like Orkut, Tagged, hi5, etc can be hazardous.' Identity theft is a crime of opportunity. Vigilance and awareness is essential in combating the fast growing non-discriminatory crime', says Johnny May, a specialist in protecting individuals and organizations from identity theft. Vigilance and awareness is essential in combating the fast growing non-discriminatory crime', says Johnny May, a specialist in protecting individuals and organizations from identity theft. Employers have to learn to protect their employees from the invasive crime. Moreover, as most data theft is from within the company's rank-and-file, changing the negligent approach is more than warranted. Afterall, it's a whole lot easier to keep the identity theft from happening than to repair the imminent damage. For starters, determine where and how employee information is currently stored – in the form of paper files and spreadsheets, on executives' computers or in online format (Payal Chanania).

Information Security is emerging as the greatest challenge facing countries, companies and individuals in the global networked economy. Recent incidents of call centre data theft in India have been much publicized. Few other countries are subject to the same level of scrutiny, but what are the facts? Problems related to data security are not limited to any one country. Research conducted in 2005 found that there were more security breaches in UK and the US than in India. In the past 18 months, according to reports by privacy watch-groups, the incidents of identity theft in the US alone have been 148 and affected nearly 94 million identities. In the UK, the Home Office estimates that identity thefts result in losses of over a billion pounds, and a quarter of all UK citizens has either been affected by ID theft or knows someone who has been (sunmediaonline, 2006).

The Sunday Times reports, Identity fraud has increased six fold over the past five years and is estimated to cost the economy more than £1.7 billion a year. In fact Stolen identities of Britons-including their credit card details, home addresses and security passwords-are being sold on Russian websites for as little as £1 each. The criminals have used a so-called "trojan" software to track every keystroke made by the victim when he or she is accessing secure sites. The victim unwittingly downloads it from a website or through e-mail and this enables the criminal to find out all of the vital information. Now this may be stories from the west but closer home in India Identity theft is being used in even more damaging ways.

Identity theft is the crime of the century – the latest and most horrendous of a string of appalling white-collar crimes. Almost everybody is unsafe, as more and more data fraud cases are making international headlines by the day. What's more, the incidence is rapidly spreading to developing economies like India too. And shockingly, employee identity theft forms a whopping 90% of overall business record theft!

Hackers unscrupulously break into classified company information to steal employees' identities. The personal details are sold off to bad elements who abuse the data to no end. They assume false identities to secure loans, gain employment, buy cars, rent houses, rack up debts and even perpetrate serious crimes.

Hapless victims are forced to legally change their names and details to prevent the nightmarish misuse. However, the worst damage is already done within the first few hours, while untangling from the mess takes years. Therefore, with the mounting scare of mortal embarrassment, financial mutilation, reputation blemishes and life devastation, is it any wonder that the general public is becoming increasingly paranoid about personal identity security? Afterall, what is more important than your name?

While the Indian cyber crime unit have been hesitant to reveal the number of cases reported, that wouldn't really give a true picture of the scenario. Since, most of these cases are never even registered. Firewalls, anti-spyware softwares, secure and password protected pages and documents may all offer you protection. However, once your 12 digit card number, 15 digit account number and basic information has been typed out in cyberspace, there is no turning back. We are all sitting ducks in the hands of sophisticated criminals who want to make "quick-money".

Suggestions:

a. Tightly control general contact with data files by reviewing who should and needs to have access. Restrict the access to limited staff with strict guidelines for those who have the authority to handle the personal-identifying information.
b. Secure physical employment records. Basic security precautions such as alarm systems and locking storage areas where sensitive information is stored are often overlooked.
c. Safeguard the digital information with sophisticated security measures like password-protection, data encryption and firewalls that keep intruders out by preventing unauthorized entrance.
d. Train employees who handle the sensitive data about safe record keeping and preventing accidental disclosure.
e. Conduct regular audit trails to track database access and isolate illicit/unnecessary retrievals.
f. Do not request superfluous information from employees. Acquire reasonable details in a safe manner without any scope for incautious lapses.
g. Dispose of sensitive personal data once it is no longer needed. Destroy sensitive matter in a shredder (papers tossed in the trash are a sitting duck).
h. Scrutinize employee backgrounds especially for vulnerable jobs like HR and payroll that involve access to employee records.
i. Limit ex-employee access to internal computer networks instantly to prevent unhealthy infiltration.
j. Some companies employ third-party investigators to gauge organizational vulnerability and check identity thefts while some others institute in-house privacy officers too.
k. Also, employ additional safeguards like educating employees about how to keep their own identities safe - proper personal information disclosure and procedures for data protection with emails, newsletters, staff orientations, departmental meetings, workshops or conferences.

Finally, inspite of all the tech-savvy practices, no protection is completely foolproof. All that we can do is minimize the risks of identity theft, as eventually crooks will outwit the best security. James Van Dyke, president of Javelin Strategy & Research, USA concludes, 'Fighting identity theft is a cat and mouse game – there's always room for improvement!'

References:

[1] Payal Chanania, The spectre of workplace identity theft Online edition of India's National Newspaper

[2] Indiatimes.com,http://timesofindia.indiatimes.com/articleshow/1084598.cms International Herald Tribune, Global edition of the New York Times. November 15 2005.http://www.iht.com/articles/2005/11/15/business/theft.php

[3] International Herald Tribune, Global edition of the New York Times. November 15 2005. http://www.iht.com/articles/2005/11/15/business/theft.php

[4] http://www.gartner.com/it/page.jsp?id=501912 This guide was created in partnership with FiLife's identity theft guide.How-To Guide Home Credit How To Protect Yourself From Identity Thefthttp://guides.wsj.com/personal-finance/credit/how-to-protect-yourself-from-identity-theft/)