# How safe is the information in this Digital era? –A critical review of the status quo

**Arcot Purna Prasad**

Associate Professor, Institute of Management, Christ University, Bangalore, Karnataka, India

***Corresponding Author:**
Email: arcot.1974@gmail.com

## Abstract
In the Digital World cyber-attack has become a routine activity, and prudence lies in how to manage this without losing focus on prime business activities. On one side technologies and competition is atempting business to try new things to develop effectiveness on the other side data is becoming a threat at various levels. Threat perception has really created stress on systems, and considerable investment is forced to make on IT infrastructure and policy making. In this system whole system is strong in terms of operations and fragile in terms of maintaining the sanctity of the data.

**Keywords:** Cyber Attacks, Cyber Security, IT Infrastructure and IT Policy.

## Introduction
In 1988: The Morris worm - one of the first recognized worms to affect the world's nascent cyber infrastructure - spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted of the US' computer fraud and abuse act. He now works as a Professor at MIT.

December 2006: NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest US space launch vehicles were obtained by unknown foreign intruders.

October 2013: NCIRC Upgrade - The NATO Computer Incident Response Capability (NCIRC) upgrade project, a 58-Million-euro enhancement of NATO cyber defences, is on track for completion by the end of October 2013. This major capability milestone will help NATO to better protect its networks from the increasing number of cyber-attacks against the Alliance's information systems.
(Source:https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm)

Cybercrime has grown up. It is now a multi-billion dollar industry bigger than most "traditional crime" and on par with many traditional, non-criminal industries. The rise of Cybercrime-as-a-service has made hacking easier and more business-like than ever before. Organised cyber-crime gangs have become far more professional and troublesome than any bored lone-wolf. Cyber-criminal markets even do Black Friday-like deals now.

But despite growing up and becoming more organised, it's still the internet. And trust is always at a premium. According to one Microsoft Research paper, "ever-present rippers who cheat other participants ensure that the market cannot operate effectively". These cheats – aka Rippers - fail to provide the goods or service for which they've been paid, whether that's a low quality of malicious software, providing fake data dumps, or selling the same information multiple times and therefore reducing the value (especially for bank account information, which may well have limits in place).

"Fraud between cyber criminals has always been an issue that limited the profitability of their malicious campaigns," says Michael Marriott, Research Analyst, at security firm Digital Shadows. "Cyber-criminal markets are lemon markets where buyers can't differentiate low and high-quality goods, therefore providing a breeding ground for rippers."
(Source:http://www.idgconnect.com/abstract/24968/cyber-criminals-realising-plenty-learn-legitimate-business)

Networking and the Internet were considered to be the biggest breakthrough, and it has become the biggest threat to the whole world now. This can also be the best example of system thinking and design thinking. The above information is recorded and proves that best of the orgnisations are unable to protect their systems from the Intruders. The Internet is the breeding ground for all these activities of the intruders. Cyber-attacks may happen with different flavors and colors. Worms, Virus, Hacking Phishing, spoofing, Denial of Service Attacks (DNS) and so on…These are the some of the known formats of cyber-attacks. Some of the Perpetuators focus on weaknesses of the existing software systems, and some develop access to the databases by getting the hook of the user-id and passwords.Cyber war has begun, and the attackers are unknown, and these cowards are more intelligent and think more about short term gains rather than long term implications.Cyber security is related to the set of processes to keep information safe.On one side governments and other side stake holders are strengthening and tightening the laws and the onus lies on the service providers to safeguard and protect information which is collected

from the customers and the beneficiaries. These digital initiatives are new to many economies and need to take proactive steps to handle so that failure costs can be controlled to some extent and safeguard the most important asset of any nation. The most important thing in this society is the information and needs protection both at the micro level as well as at the macro level. If the information is controlled by the people who have some nefarious designs will create the havoc, and failure cost of that will be really huge. As the law states that ignorance is never bliss, better to know the things and upholds the concept of Buyer beware. There are many instances in which the innocent people are sabotaged, and losses can be really devastating. When it comes to information and governance, one has to have a right policy, right implement, right monitoring and timely updation. It is really a big task to design and implement IT policy. Now IT companies are following zero tolerance data security and protection. Vigilant systems are monitoring in the background and can carry out aninvestigation without any complaint. Intranet and Internet technologies started to insulate from each other and carry out activities without any interference. Investment in buying firewalls has increased in the recent past and companies not allowing any employees to carry out any memory devices which can trigger many unwanted activities.

**Research Methodology**

Objective:

1. To understand the Cyber Attacks at global and local perspectives.
2. To suggest some strategies to develop immunity into the system

**Data Collection:** This is an exploratory research, and Secondary Data is collected from authentic websites and reports and used for analysis.

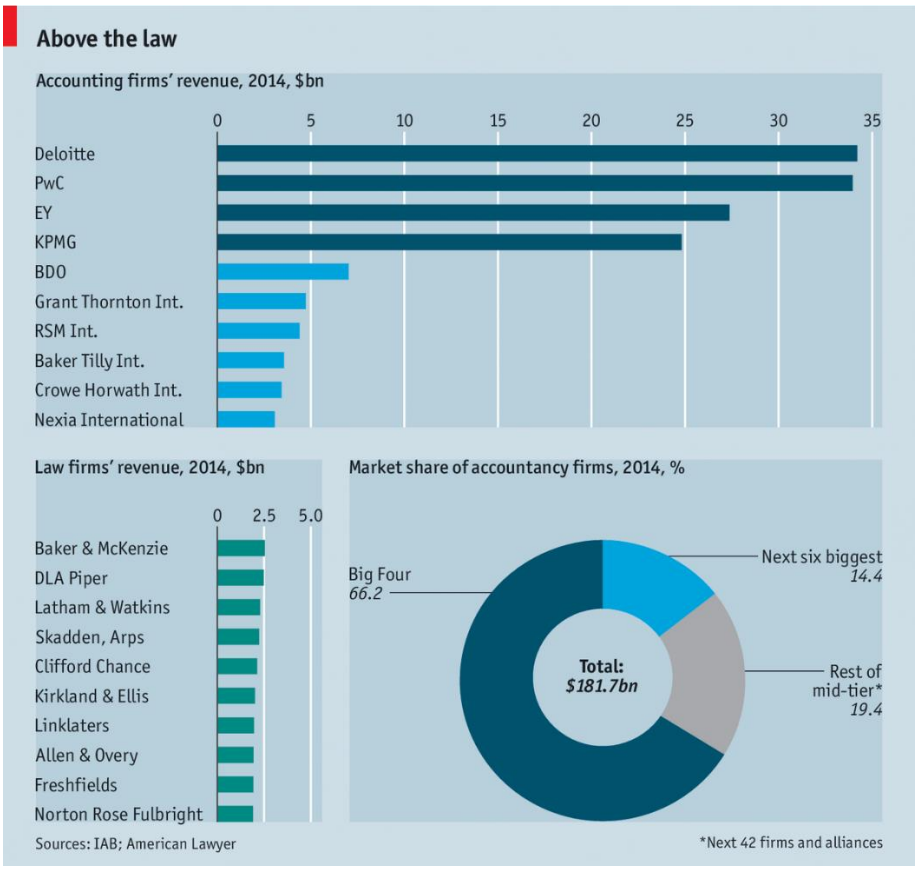
**Tools used:** SWOT is used to analyze cyber systems.

**Analysis**

According to the latest report on cybercrime, In India Cyber-crime takes place at every 10 mins and it was 12 in 2016. The process of cybercrime obviously takes a longer time to investigate and bring culprits to the books. The investigation takes longer time because of the reason that stake holders are scattered and need to observe the behavior of the users and it involves a lot of research and data analytics. This has given rise to a special branch called cyber forensics. It is a new branch, and lot youngsters are showing interest in this, and it will become the order of the day in tomorrow's digital sphere. In the recent past, Delloite was in the news because of cyber-attack, and it is one of the accountingfirms along with other three giants PwC, KPMG and EY (as shown in the graph) faces a huge threat from all dimensions. The intenal threat is from the employees and other stakeholders who are involved in their processes. In case of Outsourcing and consultancy one needs to believe each other and sign a Non-Disclosure Agreement (NDA) and carry out the activities. Here one is dependent on the other because of expertise and knowledge and that itself is posing a great threat to the business and society at large. The European Union is coming up with a set of cyber norms which will make operations of all organsiations to take care data of the customers along with theirproduct and services. The customercentric laws and judiciary always cheers the customers. This makes processes more stringent, and shifts focuson the protection of Data and Information. Insurance companies started cyber insurance to protect data and charging a huge premium from the companies and expected to treble their premiums by 2020. Hackers attacking and the frequency is really high and apart from this ransomware has really increased in the recent past. Bitcoins are becoming the new mode of money transfers.

Banks are under attack. In the recent past, Banks like American Express, JP Morgan wereattacked, and hackers siphoned money without gun and trucks. This is the new style of looting bank without physical presence. Customers are very innocent because of the fact that it is anew thing and needs a lot of intelligence to maintain the security. Some even might not have imagined the attacksand losses associated with that.

Data is collected and stored in two ways. Customers or stakeholders voluntarily give data and will be stored and used ethically to promote products and services. Data is collected by the governments for better governance. Hackers try to get access to these databases and playhavoc. Some do it for fun, and some do it for financial benefits. It might be easy to track the second ones than the first type. Some people write a virus, and it becomes a staring point for anti-virus markets. Cookies are the programs which pass on the data from the laptops or desktops to the server. This data protection is a real big question mark. Businesses of all formats collect information, and some will misuse that by selling databases to the big fishes of the market. Databases are just sold without thinking about the long-termimplications.




**Graph 1**

**Table 1: NCRB Report (National Crime Report Bureau)**

| SL. No. | Crime heads | Cases Registered | | | % Variation in 2014 over 2013 | Persons Arrested | | | % Variation in 2014 over 2013 |
|---|---|---|---|---|---|---|---|---|---|
| | | 2012 | 2013 | 2014 | | 2012 | 2013 | 2014 | |
| 1 | IT - Tampering computer source documents | 161 | 137 | 89 | -35.0 | 104 | 59 | 64 | 8.5 |
| 2 | IT - Computer related offences | 1875 | 2516 | 5548 | 120.5 | 749 | 1011 | 3131 | 209.7 |
| 3 | IT - Cyber Terrorism@ | - | - | 5 | - | - | - | 0 | - |
| 4 | IT - Publication/transmission of obscene/sexually explicit content | 589 | 1203 | 758 | -37.0 | 497 | 737 | 491 | -33.4 |
| 5 | IT - Intentionally not complying with the order of controller | 6 | 13 | 3 | -76.9 | 4 | 3 | 4 | 33.3 |
| 6 | IT - Failure to provide or monitor or intercept or decrypt information | 3 | 6 | 2 | -66.7 | 3 | 7 | 0 | -100.0 |
| 7 | IT - Failure to block access any information hosted etc.@ | - | - | 1 | - | - | - | 0 | - |
| 8 | IT - Not providing technical assistance to Govt. to enable online access@ | - | - | 0 | - | - | - | 0 | - |
| 9 | IT - Un-authorized access/attempt to access to protected computer system | 3 | 27 | 0 | -100.0 | 1 | 17 | 0 | -100.0 |
| 10 | IT - Misrepresentation/suppression of fact for obtaining license etc. | 6 | 12 | 5 | -58.3 | 5 | 14 | 13 | -7.1 |
| 11 | IT - Breach of confidentiality/privacy | 46 | 93 | 16 | -82.8 | 22 | 30 | 13 | -56.7 |
| 12 | IT - Disclosure of information in breach of lawful contract@ | - | - | 2 | - | - | - | 5 | - |
| 13 | IT - Publishing/making available false elect. Signature Certificate | 1 | 4 | 0 | -100.0 | 0 | 8 | 0 | -100.0 |
| 14 | IT - Create/publish/make available Elec. Signature Certificate for unlawful purpose | 10 | 71 | 3 | -95.8 | 3 | 51 | 5 | -90.2 |
| 15 | IT - Others | 176 | 274 | 769 | 180.7 | 134 | 161 | 520 | 223.0 |
| **Total Offences under IT Act** | | **2876** | **4356** | **7201** | **65.3** | **1522** | **2098** | **4246** | **102.4** |

Note: '_' implies sezo value in previous year
"@ implies data collected in 2014 for the first time

**Table 2: Cyber cromes/cases registered and persons arrested under IPC during 2011-2014**

| Sl. No. | Crime heads | Cases Registered | | | % Variation in 2014 over 2013 2011 | Persons Arrested | | | % Variation in 2014 over 2013 |
|---|---|---|---|---|---|---|---|---|---|
| | | 2012 | 2013 | 2014 | | 2012 | 2013 | 2014 | |
| 1 | Offences by public servant | 2 | 1 | 0 | -100.0 | 4 | 2 | 0 | -100.0 |
| 2 | Fabrication/Destruction of electronic records for evidence | 13 | 12 | 1 | -91.7 | 18 | 11 | 1 | -90.9 |
| 3 | Cheating@ | - | - | 1,115 | - | - | - | 335 | - |
| 4 | Forgery | 259 | 747 | 63 | -91.6 | 263 | 626 | 58 | -90.7 |
| 5 | Data Theft@ | - | - | 55 | - | - | - | 11 | - |
| 6 | Criminal Breach of Trust | 282 | 518 | 54 | -89.6 | 215 | 471 | 39 | -91.7 |
| 7 | Counterfeiting * | 45 | 59 | 10 | -83.1 | 49 | 93 | 8 | -91.4 |
| 8 | Others | - | - | 974 | - | - | - | 772 | - |
| **Total Offences under IPC** | | **601** | **1,337** | **2,272** | **69.9** | **549** | **1,203** | **1,224** | **1.7** |

Note *includes property marks, tampering and currency/stamps till 2013 and currency & stamps during 2014
Note: "_" in the column of percentage variation implies zero value in previous year

**NCRB Report**

Two tables are extracted from the chapter 18 of the crime report. This table depicts the number of Cybercrimes.In India, according to the Crime Report 2015, Uttar Pradesh and Karnataka are in the leading positions and booked more than 1000 crimes in a year. Another important thing note here is four to five percent of the people come report about these crimes. It means the only tip of the iceberg what we are addressing.

**SWOT Analysis of Cyber Systems:**

| **SWOT Analysis of Cyber systems** | |
|---|---|
| **Strengths** | **Weakness** |
| Easy to do Business | Data is stored in Unsafe environment |
| Transparency | Train stake holder to handle data |
| Globalization | Poor Digital Literacy |
| Global reach | |
| **Opportunities** | **Threats** |
| Expansion | Cyber Attacks |
| Reduce Cost | Huge failure cost |
| Improve customer Satisfaction | Cost of rebuilding of the system is huge |
| Snub Competitors | Investment in security is never ending one |

In India, Aadhar card collects all the information about the citizens to maintain better governances, and it resulted into misutilization of the same for sending communication during elections to influence voters. Permanent Account Numbers which are supposed to be unique but big racket is behind in producing duplicate ones. Indian railways used to display PAN details to the gereral public which has become the starting point for many illegal activities. In cyber-attacks, there is no beginning and the end. The behaviour of attackers is very random in nature and very difficult to predict. Even the latest IT laws are also not equipped enough to handle these challenging issues and need to amend the same at every eventuality. Cyber police stations started to encounter and control cybercrimes. On the top of it, people need more training to handle the same. The best to control these aspects is to make customer and organizations be award and equip to handle challenges. It is anideological war and fought in the space and not knowing who is the Villain and who is the Hero. This is fought between any two individuals, tworeligions, twocountries and list will continue. One of the deterrents can be to catch the intruders and punish at the earliest so that others don't get into these wrong practices and make people more empowered to report and take some preventive actions to control this social menace.

**Data leaks created Havoc**

The International Consortium of Investigative Journalists (ICIJ) over the past year established the technical foundations for the worldwide mass media investigation. The ICIJ also laid the technical grass roots of the "offshore leaks" involving international tax-shelter accounts in 2013, the "Lux Leaks" of Luxembourg's tax rulings in 2014 and the "Swiss Leaks" of cash shelters in Switzerland in 2015, and so has a lot of experience in data analytics for journalistic purposes. Mar Cabra works at the data and research unit at the ICIJ and knows the Panama Papers' technical

challenges better than anyone else. These data leaks have created a new way of looking at tax evaders. Panama leaks and involvement of political and business leaders in this type of society is really dangerous and risky too.

Cloud level Security is the need of the hour.SMAC is becoming very popular and maintains security all these levelsbecome imperative and crucial. Firewalls to clouds become very important, and viruses like a trojan horse will hit our system at every point. One needs to have internal vigilance as well as external vigilance to ensure smooth operations.

Cyber security calls for mobile security. Off late internet and mobiles are converged, and mobile domains also become vulnerable to attacks. This will lead to infrastructure which manages both the worlds and protects data of mobile users as well as system users. Data of the customer are captured throughMobile Applications, ATMs, and online shopping websites. There are some fake websites which are meant for just data collection and can make use of confidential data for wrong purposes. Google and Amazon servers are sitting on huge amount of data and need to protect this confidential information at any cost. Information is the power, Facebook analytics, google analytics is becoming very popular and may be useful if data is used ethically or it may pull down the whole system. Data about the whole supply chain is maintained and led supply chain analytics. Services also come under the ambit of analytics and the whole system is under the control of data and analytics. Data science is becoming the order of the day and to the protection of the data is more crucial for existence.

Internet of things (IoT) is the latest development getting into business domain. As technologies are far ahead of Businesses and organizations are skeptical about technology absorption. That fear came true because of cyber attakcs and businesses are in the middle of the path and neither they can go back traditional practices nor progress further to reach their ultimate goal. Ultimately those organsiations which will survive in these turbulent waters will only survive, and there is no guarantee about any business for its long term survival. IoT is emerging, and it can be handy to handle crimes to some extent by controlling operations remotely and monitor. It makes use of theInternet and mobile systems optimally and reduces wastage to some extent. In Israel agriculture is driven by IoT and they were much successful in managing agri. business inspite of the scarcity of water.

## Conclusion

This will continue and has no end. Many Cyber Attacks get unnoticed, and the stake holders need to be motivated to come out and report. Security starts with the letter "I" which is embedded in the spelling of the Secur "I" ty. Collective responsibility is the need of the hour and cooperation is very much required at all levels. Multiple Dimension of data visualization can solve problems to some extent. Prevention is better than cure.

## References

1. https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm
2. http://www.idgconnect.com/abstract/24968/cyber-criminals-realising-plenty-learn-legitimate-business
3. Report on Cyber Crime chapter 18"-NCRB report-www.ncrb.gov