CYBER CRIME AND CYBER SECURITY- PREVENTION AND CONTROL WITH RESPECT TO INDIAN CYBER LAWS

Mr.Santosh Sambhajirao Pawar[1]

[1] BE (MECH), BA (ECO), MOM, LLB, LLM, MSW, MCA. Security Officer, Pune Muncipal Corporation, and Research Scholar, Faculty of Law, Departmet of Law & Governance, Vishwakarma University,Pune.

Abstract: Electronic security and privacy are currently ruled by a completely ineffective regulatory body in India. The authority to prosecute and levy fines under the IT Act 2000 and the IT Amendment Act 2008 on non-compliance has slept for several years and relatively few major reforms have been made in recent years in the laws on cyber security, data security and identity safety. In 2013, the government drew up a national cyber security strategy, generating significant interest both in India and abroad, particularly as India was a growing outsourcing destination. Regrettably, reforms were not easily available for purposes that had such a detrimental effect on the government's objective of timely, robust and strict regulations in these matters.

The increasing spike in cybercrime produces over-dependent governments and technology firms. Today, cyber crime is rising.Wars between nations will move from military struggle to cyberspace in the immediate future. Cyber-battles can now be valuable weapons in the hands of global force rivals; cybercrime will also become a business for $1 million. We need straightforward and easy approaches to reduce cybercrime. To tackle cybercrime. While the suspects are still unfaced, they could be your neighbour next door, or in another urban area or world. This crime can be hard to control or dissuade. This form of crime may be directed toward governmental institutions, ministries and enterprises irrespective of scale and size. As free and open resources are available online and scripting will also allow children to download and run against any unknown targets without knowing what the attacker needs to do on a daily basis. Attack techniques are now sophisticated and there are more and more methods to detect the targets if not impossible.

Keywords: Cyber Law, Risk, Protection, Control, Elimination, Cyber Space, Act, Cyber Crime.

Introduction:

Cybercrime is a crime involving computers or computer systems where a system may be either an object of crime, a crime tool or evidence of crime. This is important for the advancement of businesses, public institutions and individuals, when a lot of information technology now relies on the use of IT. It is necessary to trace, defend and prevent cyber attacks. The procurement and training by government and companies of highly trained cyber-crime experts should not be over-emphasized. This ensures compliance with the applicable international workplace specification in computers and other technological devices. While avoiding

is better than curing, infringements will continue, irrespective of deterrence measures for cybercrime prevention and monitoring, forensic experts have been invited to perform sound, automated forensic investigation, examine, preserve and reconstruct the crime scene and supply information to appropriate authorities.

This does not mean that in this regard the urgent need for change is not understood. The Joint Secretary of the Cyber Laws, New Delhi, R K Sudhanshu, in National Cyber Security Conference, under the aegis of the PHD Chamber of Commerce and Industry in July 2016 said that the Government is preparing to review the cyber security legislation in India in terms of new cryptography and cyber security policies.

Recently Ravi Shankar Prasad, Minister of law and IT, at an assembly Affiliated to Chambers of Trade and Industry in India, said the Government is finalising cyber protection rules for mobile celluler transmitters and has already told some mobile firms that they need improve information on cyber security.

Following the launch in 2015 of the widely funded public initiative Digital India, a major effort focusing on the "Digital Web," which promotes digital connectivity and enhances digital literacy, was an ambitious move by the Prime Minister to compensate for the waste of time. The campaign addressed concerns of data and the security of privacy in media and academia that potentially will allow the government to legislate in greater depth on these issues. In the technology industry, Digital India has generated huge investment flows.

In the year, 2016 was see as a mixed bag of optimistic and slightly troubling improvements, but none of these developments culminated in significant legislative reconstruction or reparations as the authorities continued to guarantee targeted financial benefits for several years, except for the adhar regulation.

In a series of appeals challenging its procedural legitimacy, the Aadhar Act was contested. The question was asked whether privacy is a fundamental right under the Indian constitution. On 09 Jan 2020, the Supreme Court's nine-judge judicial bench delivered its verdict on certain pleas and determined that each person's personal privacy was a constitutional fundamental right.

In order to make it obligatory for taxpayers to connect their permanent account numbers (PANs), file tax returns, open bank accounts and transfers beyond or above the threshold, and reduce tax avoidance and money laundry, in addition to the contentious emerging patterns that were previously listed. The telecommunications department has already made a statutory effort to use the Aadhar Act for current telephone customers as a subscribers' inspection system.

Cyber Security Laws in India

There are following primary legislation on cyber security:

1. **The Information Technology Act of 2000 & IT Amendment Act. 2008** - The Indian cyber legislation is controlled under the Information Technology Act of 2000 & IT Amendment Act 2008. The main thrust of this Act is to provide trustworthy legal inclusion in eCommerce and facilitate the registration of records with the government in real time. But a succession of modifications followed,

with cyber attackers growing sneakier, overcome by the human desire to abuse technology. The ITA, which the Parliament of India has adopted, emphasises the severity of the fines and penalties that guarantee e-government, e-banking and e-commerce. The scope of ITA has now been improved to include all the newest communication devices. The IT Act is the most important one, directing the whole Indian legislation to strictly regulate cyber crimes:

a. Section 43 - Applicable to anybody damaging computer systems without the owner's consent. In such circumstances, the owner may demand full reimbursement for all damages.

b. Section 66 - applicable if a person is determined to have committed any conduct referred to in section 43 in a dishonest or fraudulent manner. In such cases, jail might be up to three years or a fine of up to Rs. 5 lakh.

c. Section 66B—Incorporates the penalties for receiving stolen communication instruments or computers fraudulently, confirming the likely sentence of three years. Depending on the severity of this term, Rs. 1 may also be overtaken.

d. Section 66C – The identity theft of digital signatures, hacking passwords or other distinguishing identification characteristics is examined in this section. If found to be guilty, Rs.1 lakh fine may potentially support a three-year jail.

e. Section 66 D - - This clause was included on request to penalise cheaters using computer resources.

2. **Indian Penal Code (IPC) 1980-** Identity theft and cyber fraud are incorporated in the Indian Penal Code (IPC), 1860 — invoked in conjunction with the IT Act of 2000. The main portion of the IPC deals with cyber fraud:

a. Forgery (Section 464)

b. Forgery pre planned for fraud (Section 468)

c. False Documents (Section 465)

d. Presentation of a falsified document (Section 471)

e. Damage to reputation (Section 469)

3. **Companies Act of 2013** - Under the Companies Act 2013 the corporate stakeholders relate to the legal duty required for the refinement of everyday activities. The directions of this Act solidify all necessary techno-legal compliance and legalise the firms that are not so compliant. The SFIO (Serious Fraud Investigation Office) has been given authority under the Businesses Act 2013 to prosecute Indian companies and their directors. SFIOs also become even more proactive and severe in this respect after the Companies Inspection, Investment and Inquiry Rules 2014 announcement. The legislators guaranteed that all regulatory compliance, including cyber forensics, e-discovery and cybersecurity, were adequately covered. The Companies Rules for 2014 lay out rigorous standards clarifying cybersecurity duties for managers and executives of companies.

4. **Compliance with NIST-** The cybersecurity framework (NCFS), recognised by the National Institute of Standards and Technology (NIST), is the most credible worldwide certification body and offers a unified approach to cyber security. NIST Cybersecurity Framework includes all the rules, standards and best practises necessary for responsible management of cyber-related risks. This paradigm focuses on adaptability and economic efficiency. It supports the strength and preservation of vital infrastructure through:

   a. To better analyse, manage and reduce cyber security risks – to prevent data loss, data misuse and restore expenses in the future.
   b. Determination of the most important actions and key activities – to ensure them
   c. Proves the confidence of businesses that guarantee key assets
   d. Contributes to prioritising expenditure to optimise cyber security ROI
   e. Respond to regulatory and contractual responsibilities
   f. Supports the broader information safety programme

Recommendations

Risk, Control and Prevention of Cyber Security:

In order to maintain anonymity, dignity and availability, digital properties must be secured. Awareness is important for the safety of the human brain, electronic devices, physical media and those in motion.

We will need to rely on three main categories:

1. Risk of cybercrime

2. Monitoring cyber-crime

3. Control & Elimination in cybercrime

1**. Risk & Potential of Cyber Crime** :

India is the second most populous country in the world, and IT today is a crucial part of everyday life, with no security or an unbreakable system. We have to recognise that these systems, irrespective of safeguards and deterrence, can be broken down at any moment, and that is why cybercrimen is so much risk potential. The dilemma of dangerous countermeasures needs to destroys the secrets of the cyber attack and, as this occurs, it leads to the interfere through cyberspace. This is a very interesting module because it encompasses a forensic analysis of network attacks as well as running apps such as mobile devices. Information on cybercrime risk shall be identified, gathered, retention assessed and tracked and presented. You have to dig at victimology here. As some people still use thumbs as a signature in Digital Signature Days in India, India is highly vulnerable to cybercrime danger in this scenario, it is important to focus on topics like risk of cybercrime.

2**. Prevention of Cyber-Crime** :

This will address how effective cybercrime tactics elimiation techicnics can be implemented. Therefore, if tried by a court of the competent jurisdiction it will provide the required penalty for the cyber-offenders. This would be a preventive tool for those who wish to join. The Indian IT Act 2000, IT amendment Bill 2006 and the IT amendment Bill 2008 will also be reviewed. The Indian cyber laws of Viz Complete must be checked.

3**. Control & Elimiation of Cyber Crime** :

In order to end cyber crime, we need to work on educating cyber space users and operators, best practises, knowledge of protection, etc., but it takes time to understand underground hacking technologies from defence administrators and managers. The mindset of hackers must also be centred, the techniques and tactics of hackers must be exposed and the various ways of cybercrime Elimination. Same way detection is very essential and should be evangelised accordingly. Bear in mind that users have the lowest protection links. Tools that support include, but are not limited to, commercial and open source tools: BackTrack 5r3 and Kali-Linux, Pro, Saint, Cain, Abel e-mail tracker, Nmap, Nessus, Net Cat, GFI Languard, Retina, etc. Key Effect Pro, Immune canvas, Pro and System Metasploit. The list is infinite and it is nice that most of them are available and accessible.

Given the growing likelihood of cybercrime and its effect on government institutions, citizens, and corporations, the key purpose of this article is to expose the hidden reality about cybercrime that has not yet been uncovered, as it relates to the growth rate, the complexity of threats, cybercriminal motive and finally discovering means of mitigating it. This article will help to reflect on dissuasive measures, the idea of maximum and efficient statutory sentences where deterrence and enforcement are not completely possible. In this respect we have reviewed established laws and, where applicable, propose/find amendments, define a complete and appropriate measure for monitoring cyber criminals (tracing the hacker in the cyber space). We must establish Techniques capable of handling electronic forensics.

Suggestions

On the basis of the overall results and the examination of the input from cybercrime specialists, few ideas are found that may assist all possible prospects Victims of cybercrimes protection. Each internet user is entitled to know the effects of such threats and misuse. Hence Education is significant focus on topics such as:

a) Internet use and misuse

b) Importance of security on the Internet

c) Cyber law and regulatory awareness

d) Crime Technology Impact

e) Hardware and software protection requirements

f) Exploitation and pilfering data.

f) Internet policy knowledge at the organisations.

g) the right to safeguard against disclosure of personal data with other people.

h) According to the kind, scope and sensitivity of the cyber security event, cyber incident response techniques may change from company to company. Some of the common measures advised include:

1. The implementation of a thorough information security policy for the Board to be authorised;
2. Regular monitoring of transactions;
3. Conducting safety risk evaluations of information;
4. Development of risk mitigation and transition strategy;
5. Update in advance the role of important stakeholders within the organisation;
6. Assign adequate staff to contact regulatory agencies, to deal with customers, service providers, etc.

Many organisations also choose to do frequent vulnerability assessments in their systems, including by allowing targeted hacking. Depending on the industry, organisations can also approach CERT-In and request help on recovery, damage control and the functioning of their systems. CERT-In also publishes warnings from time to time on suggested measures for parties affected by cyber-security events.

Conclusion

This would make constant advances in the battle against cybercrime or even bringing us victory. It will also instil creative and inductive thought and foster the creation of knowledge of organisational protection.

Consequently, we will have a special role to play in addressing different information security problems for states, the corporate world and individuals alike. Once these are all done, we will make our cyber-space a better environment for market activities by indirectly impacting the economy. For purchases, the internet would be a safer environment for consumers and safety tips for their transactions will be better educated.

References

1. Anshuman Jana and Kunal Kumar Mondal, “A survey of India Cyber Crime and Law and its prevention approach” ‘International journal of Advance Computer Technology’.
2. IDSA Task Report. (2012), India’s Cyber Security Challenged.
3. N.S. Nappinai (2017) Technology Law Decoded, LexisNexis.
4. Prabhat Dalei and Tannya Brahme.(2014) “Cyber Crime and Cyber law in India: An Analysis” ‘International journal of humanities and Applied science’ Vol.2 (4).
5. Talwant Singh, “Cyber Law and IT” pp. 1-4.
6. Aggarwal, Gifty. (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering, August Vol 5, Issue8.