# WHITE BLACK LEGAL

LEGAL

LEGAL

VOLUME 1: ISSUE 10

|| May 2020 ||

Email: editor@whiteblacklegal.co.in

Website: www.whiteblacklegal.co.in

# DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

# EDITORIAL TEAM

## *ABOUT US*

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

**WHITE BLACK LEGAL: THE LAW JOURNAL**

# SECURING THE CYBER WORLD: VERITY OF THE HALF-BAKED LAW

# SUB THEME – CYBER SECURITY

(Names of Author - Aman Choudhary)

## ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my Professors for their exemplary guidance, monitoring and constant encouragement throughout the completion of this project topic. The blessing, help and guidance given by them time to time shall carry me a long way in the journey of life on which we I am about to embark. Also, the guideline provided by them to stick to the deadline was also encouraging.

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend our sincere thanks to all of them.

My thanks and appreciations also go to my colleague in developing the project and people who have willingly helped me out with their abilities.

Lastly, I thank almighty, my parents, brother, sister and friends for their constant encouragement without which this assignment would not be possible.

# TABLE OF CONTENT

## INDEX OF AUTHORITIES

Statute

- INFORMATION TECHNOLOGY ACT OF 2000
- Additional Protocol to the Convention on Cybercrime
- UNCITRAL Model Law on E-Commerce 1996
- UNCITRAL Model Law On Electronic Signatures (MLES), 2001
- Health Insurance Portability and Accountability Act (HIPAA),1966
- Gramm-Leach-Bliley Act,1999
- Homeland Security Act, which included the Federal Information Security Management Act (FISMA),2002
- Cybersecurity Information Sharing Act (CISA)
- Cybersecurity Enhancement Act of 2014
- Federal Exchange Data Breach Notification Act of 2015
- National Cybersecurity Protection Advancement Act of 2015
- The UK NIS Regulations
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Communications Act 2003
- Data Protection Act 1998
- Privacy and Electronic Communications (EC Directive) Regulations 2003

## HYPOTHESIS

The advanced age of technology gave huge rise to cyber transactions but also sprang cyber attacks and cyber crimes from its root, thus there is great need to understand and develop cyber security laws and regulations.

# CHAPTERISATION

## ABSTRACT

Our Country being a developing nation also gives rise to imminent dangers of cybercrimes, with these types of crimes comes a great responsibility to form certain regulations and come up with a process of cyber security. In view of certain regulations it is thus very important to trace the history of cyber security in India and equally essential to understand and examine the issues relating to cybercrimes and cyber security. Although we have a legislation to curb cybercrimes known as the “The Information Technology Act, 2002” but what is upsetting is that, the Indian cyber security agencies are still unable to have access to the data from the foreign and internet companies due to the reason that the servers are being hosted outside the country, this not only acts as a roadblock but will also have far reaching consequences and implications to the Indian society in near future. Thus, the paper attempts to analyze the laws relating to cyber security in detail and the major reasons or issues for its failure in India. The author has focused mainly on the cyber security regulations prevalent in our country in comparison with the cyber security laws in other countries. The paper also seeks to trace the history of cyber security and its international perspective. The paper is based on authors' research on statutes of various countries in contrast to statutes in India, interaction with victims, international online sessions on topics, case study and analysis, reference material and other secondary sources.

## INTRODUCTION

With the growth of internet, the dependence on computers has increased exponentially. The challenge is to protect critical information infrastructure, like civil aviation sector, Railways‟ passenger reservation system and communication network, port management, companies and organisations in power, oil and natural gas sectors, banking and finance, telecom sector, etc. from cyber-attacks. India is ranked fourth among the top 50 countries in terms of the number of cybercrime complaints reported to the Internet Crime Complaint Centre (IC3)[1], preceded only by the US, Canada and the UK based on the 2014 IC3 annual report (The Telegraph, 2015).

Shortage of trained cyber security workforce is of serious concern to India. In comparison to China, US and Russia that have 125000, 91080 and 7300 trained cyber experts respectively; India has merely 556 cyber experts deployed in various government agencies (Joshi, 2013).

[1] The mission of the Internet Crime Complaint Center, also known as IC3, is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation (FBI) concerning suspected Internet-facilitated criminal activity and to develop alliances with law enforcement and industry partners.

India is considered an IT superpower that is a major exporter of software and hosts major ITES-based outsourced businesses. Therefore, IT constitutes a major share of Indian economy. Recently, European Union has picked holes in India's data security system and suggested that a joint expert group be set up to propose ways on how the country should tighten measures for qualifying as a data secure nation (Sen, 2013). Therefore, India needs look seriously into upgrading its Information Security infrastructure and reframe cyber policies to get data secure status from EU. This is crucial for India to retain high-end outsourced business, which has a potential of increasing from the existing $20 billion to $50 billion.

Detecting and responding to such attacks is a daunting task. Analysts have been debating whether cyber deterrence, on the lines of nuclear deterrence, can dissuade such attackers.

In the light of the hacking of the website of the Indian Space Agency's commercial arm in 2015, Antrix Corporation and government's Digital India programme, a cyberlaw expert and advocate at the Supreme Court of India, Pavan Duggal[2], stated that "a dedicated cyber security legislation as a key requirement for India. It is not sufficient to merely put cyber security as a part of the IT Act. We have to see cyber security not only from the sectoral perspective, but also from the national perspective."

## CYBER SECURITY

Generally, Cyber Security[3] is to be defined as the protection of computer system from theft or damage to their hardware, software etc.

The field is growing in importance due to increasing reliance on computer systems, the Internet[4] and wireless networks such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions and the various tiny devices that constitute the Internet of things. Due to its complexity, both in terms of politics and technology, it is also one of the major challenges of the contemporary world.

In other words, Cyber Security is defined as the protection of internet-connected and related systems, including hardware and software. Security comprises cyber security and physical security -- both are used by enterprises to protect against unauthorized access to data centres

[2] Pavan Duggal is an advocate specialized in the field of Cyberlaw, E-Commerce law. He is also a member of NOMCOM Committee on Multilingual Internet Names Consortium(MINC)

[3] *Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017)."Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law.**12** (2). ISSN 1558-7215*

[4] "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian

and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

## ELEMENTS OF CYBER SECURITY

Ensuring cyber security requires the coordination of efforts throughout an information system, which includes the following elements-

- Application security
- Information security
- Network security
- Disaster recovery/business continuity planning
- Operational security
- End-user education

One of the most problematic elements is the constantly evolving nature of security risks. The traditional approach was to focus resources on crucial system components and protect against the biggest known threats, whereas in order to deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach.

The National Institute of Standards and Technology (NIST)[5], for example, recently issued updated guidelines[6] in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments.

Version 1.1[7] released in April 2018 provided for the Framework for Improving Critical Infrastructure. The voluntary cybersecurity framework, developed for use in the banking, communications, defense and energy industries, can be adopted by all sectors, including federal and state governments. President Donald Trump issued an executive order mandating that federal agencies adopt the NIST Cybersecurity Framework (NIST CSF) in May 2017.[8]

[5] The National Institute of Standards and Technology (NIST) is a physical sciences laboratory, and a non-regulatory agency of the United States Department of Commerce.

[6] NIST Special Publication 800-53

[7] NIST Special Publication 800-53 A

[8] NIST SP 800-53A Revision 4

As a result of security risks, investments in cybersecurity technologies and services are increasing. In 2017, Gartner predicted that worldwide spending on information security products and services would reach $83.4 billion -- a 7% increase from 2016 -- and that it would continue to grow to $93 billion by 2018.

## CYBERSECURITY THREATS

In the advanced world of technology use of computer and internet comes with alarming caution that are the threats. The Cyber security threats are those threats or dangers which poses harm or danger to the computer system and can erode or delete data. The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it's necessary in order to protect information and other assets from cyber threats, which take many forms.

- Ransomware is a type of malware that involves an attacker locking the victim's computer system files through encryption and demanding a payment to decrypt and unlock them.
- Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

## CYBER SECURITY TECHNIQUES

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

## AUTHENTICATION

The process of identification of an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP) [9].

[9] as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication

## ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it.

## DIGITAL SIGNATURES

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication.

## ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus.

## CYBER SECURITY HISTORY

After understanding about cyber security and cyber crimes we must understand the evolution or history of Cyber Security. In ancient times when there were no computers or internet the transactions used to happen manually but with the onset of technology, cyber crimes and attacks were born and thus the need for cyber security was required.

Cyber Security began as a research project when around 1970s, a man named Bob Thomas realised that there was possibility for a computer program to leave small trail wherever it went. He named the program CREEPER, which went onto become the first antivirus called REAPER, which was created by Ray Tomlinson.

In the late 1980s, the first worm was introduced by Robert Morris with an idea to gauge the size of the internet and thus wrote a program called MORRIS WORM in order to propagate across networks and then copy itself. However, it replicated so aggressively that is slowed the internet and caused damages. After the Morris worm, viruses started getting deadlier. We also began to see the rise of antivirus as a commodity—1987 saw the release of the first dedicated antivirus company. From the year 1976-2006, GREG CHUNG of Boeing unleashed the biggest insider attack stealing 2 billion dollars of aerospace documents.

With the new millennium came more targeted cyberattacks, the most memorable of which was the first serial data breach of credit cards. Between 2005 and 2007, Albert Gonzalez formed a criminal ring that stole information from around 45.7 million payment Also, in 2013 EDWARD SNOWDEN unleashed a insider attack famously known as the SNOWDEN EFFECT, wherein he stole classified information from CIA and leaked them.

The years 2013-2014 saw the biggest data breach in Yahoo where many hackers jepradised the accounts of more than 3 billion users. In 2015, the world saw the biggest data breach in the US office of Personal Management, known as the OPM DATA BREACH, Stealing 4.2 million of personal files.

In the year 2017, the first ransomware called WANNACRY was introduced which targeted computers and ransomed payment in form of crypto currency. The largest credit card attack was reported in 2017 by the company Equifax, the failure on their part made them vulnerable to get their data compromised. Hackers git access to 209,000 consumer credit cards. It also resulted in resignation of CEO Richard Smith.

On 25 March 2018 , Under Armour learned that someone had gained unauthorized access to MyFitnessPal. The incident did not expose users' payment information, as Under Armour processes this data separately. Nor did it compromise Social Security Numbers or driver's license numbers, as the apparel manufacturer said it doesn't collect government identifiers.

Around 150 million MyFitnessPal users are believed to have had their information compromised in the data breach.

## ISSUES RELATING TO CYBER SECURITY

Cyber security poses bigger threat than any other spectrum of technology. Cyber criminals have already started abusing technology controlled devices for propelling cyber-crimes such as frauds and thefts. With technology protocols, still being developed and evolving at a gradual pace, it is very difficult to avoid such cyber-attacks.

The issues in cybersecurity make it a growing IT field dealing with protecting computer systems against attacks by hackers and cybercriminals. Cyber attacks may involve malware or hacking in order to get information, disrupt business, or even steal money.There are a numerous issues in cybersecurity that are challenging and formative for the industry.

There are new technologies that are constantly being developed, from cloud servers and other software,. Unfortunately, each new technology brings with it the potential for vulnerabilities that hackers and cybercriminals can exploit.

Also, the nature of human and cyber criminals play a huge role in issues that are prevalent. If all workers followed directions exactly, a lot of cybercrime could be avoided. Human nature contributes to cybercrime in various ways, including opening documents that contain malware, sharing passwords, and using easy-to-guess passwords to protect sensitive information.

Cybercriminals began by targeting larger corporations, but as they developed cybersecurity measures to counter the attacks, smaller companies and startups, particularly those in developing countries, became targets.

Cybercriminals continue to find better ways to commit their cybercrimes. A new technique called PowerShell[10] uses malicious scripts that are difficult to track and usually evade antivirus software. PowerShell has already been used in a major Saudi Arabian cyberattack.

## CYBER SECURITY IN INDIA

India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%.

India had no Cyber security policy before 2013. In 2013, *The Hindu* newspaper, citing documents leaked by NSAwhistleblower Edward Snowden, has alleged that much of the NSA surveillance was focused on India's domestic politics and its strategic and commercial interests. This sparked a furor among people. Under pressure, the government unveiled a National Cyber Security Policy 2013 on 2 July 2013.

## FAILURE IN INDIA

In India, it is imperative that cyber networks, software and cyber-physical systems, and platforms should be cyber-secure. This requires a judicious mix of people, policies and technology, as well as robust public-private partnership.

Institutions such as the National Cybersecurity Coordinator (NCC), National Technical Research Organisation, Computer Emergency Response Team and the National Cyber Security Coordinator Centre are all doing a reasonable job. But they suffer from the lack of skilled manpower and proper coordination.

[10] PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language.

The existing National Information Board (NIB), headed by the National Security Adviser (NSA), duly empowered, can play the role of an apex body in India. NCC, set up in 2015 as a part of the National Security Council Secretariat, should be strengthened to bring about amuch-needed synergy among various institutions and to work out a coordinated approach to cyber security, including cyber deterrence.

India faces the highest number of cybersecurity threats in the Asia-Pacific region with over 500,000 alerts daily, which is nearly thrice the number of alerts at global companies. And around 39% of these alerts remain unattended due to lack of required skill.

## COUNTER CYBER SECURITY INTIATIVES IN INDIA

To counter cyber security attacks, Government of India have taken some initiatives which are listed below:

1. National Counter Terrorism Center(NCTC): After 26/11 attack in 2008, Indian government realized the importance of Counter terrorism initiatives and proposed National Counter Terrorism Center(NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities.

2. National Information Security Assurance Programme (NISAP): To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP), to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure.

3. Computer Emergency Response Team-India(CERT-In): The Indian Computer Emergency Response Team was created in 2004 by Department of Information Technology. The purpose of creating CERT-In was to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country and is also responsible for overseeing administration of the IT act (CERT-In, 2014).

## INTERNET AND THE INFORMATION TECHNOLOGY ACT OF 2000[11]

In 1991, Manmohan Singh, India’s Finance Minister under the PV Narasimha Rao, further liberalized the economic policies. A new industrial policy (NIP) vastly easing onerous industrial license policies and import restrictions on high technology was announced. Export-

[11] (No 21 of 2000)

oriented ventures were given tax incentives. Foreign direct investments (FDIs) were welcomed in all sectors. In 1986 the government's Department of Electronics (DOE) obtained a funding of $6 million from the UNDP to create the Education and Research in Computer Networks (ERNET). ERNET was formally connected to the Internet on February 12, 1989 (Ramakrishnan 2009). Initially, ERNET was limited to researchers and employees at seven elite academic and research institutions and the government's Department of Telecommunications (DOT), and ERNET staff.

## INTERNATIONAL PERSPECTIVE

The international community has been unable to agree on suitable norms of behaviour in cyberspace. In 2013, the UN Group of Government and Experts (UNGGE) had suggested 11norms.

However, implementing them in cyberspace is a difficult task. In a major setback to the process of norms development, the 2015 UNGGE failed to arrive at a consensus. Presently,

The following figures would reveal the worldwide penetration percentage of cyber crimes. [12]

Penetration Rates are based on a world population of 7,519,028,970 and 3,731,973,423 estimated Internet Users on March 31,2017

In general terms, political commitment, reference to common international standards and continuous participation in international peer reviews enhance the chances of success of capacity building programmes. Each project or organisation may have its own formula to make this work.For the Council of Europe, the Budapest Convention, the Cybercrime Convention Committee and capacity building by C-PROC form a "dynamic triangle": Capacity building programmes support the implementation of the Budapest Convention as well as recommendations of the Cybercrime Convention Committee; and at the same time, the experience of capacity building programmes is fed back into the Committee and the further evolution of the Convention. The long-term involvement of "project countries" in the Cybercrime Convention Committee helps sustain the process beyond the life cycle of individual projects.

[12] Source: Internet World Stats-www.internetworldstats.com/stats.htm

The Additional Protocol to the Convention on Cybercrime came into force on March1 2006 and it mainly deals with the criminalisation of acts of racist and xenophobic nature which are done via computer systems.. the emergence of international communication networks like the Internet provide certain persons with modern and powerful means to support racism and xenophobia and enables them to disseminate easily and widely expressions containing such ideas.

The International Legal Instruments relating to E-Commerce are mainly-

1. UNCITRAL Model Law on E-Commerce 1996

The world nations came together in order to harmonise and unify international trade laws all over the world. Its main purpose is to serve a model for evaluating and modernising laws and practices relating to the commercial relationships that involve computer and internet and for providing a legislation for the same where it does not exist. The major drawback of this model is that it is not binding on the state sand acts only as a guiding force in them.

2. UNCITRAL Model Law On Electronic Signatures (MLES), 2001

The main object of this Law was granting legal recognition to e-signature and bring uniformity in national laws regarding e-signature. This model applies where e-signature are used in and for commercial purposes. It consists of two parts- Part 1 has 12 articles and Part-2 having the guide of enactment of MILES.

## CYBER SECURITY IN OTHER COUNTRIES

## UNITED STATES

For more than a decade, cyber security has been a concern for the government and private sector alike. The growth in Information Technology and E-commerce sector in the United States have given rise to cyber crimes, causing a huge loss to the US government and its people. The number of breaches in the U.S increased from 157 million in 2005 to 781 million in 2015. In 2016, the number of data breaches in the United States were around 1093 with around 36.6 million records exposed.

The year 2016 witnessed the largest data breach till date in US history as online platform Yahoo revealed that hackers stole user data and information related to at least 500 million accounts back in 2014.

The United States cyber security laws and privacy system is arguably the oldest, most robust and effective in the world.

There are three main federal cybersecurity regulations –

– Health Insurance Portability and Accountability Act (HIPAA),1966[13]

– Gramm-Leach-Bliley Act,1999[14]

– Homeland Security Act, which included the Federal Information Security Management Act (FISMA),2002[15]

These three regulations mandate that healthcare organizations, financial institutions, and federal agencies should protect their systems and information. However, these rules are not foolproof in securing the data and require only a "reasonable" level of security.

In a recent effort to strengthen its cyber security laws, the federal government is introducing several new cyber security laws as well as amending the older ones for a better security ecosystem. Below are a few of them:

Cybersecurity Information Sharing Act (CISA) [16]– Its objective is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The bill was introduced in the U.S. Senate on July 10, 2014, and passed in the Senate October 27, 2015

Cybersecurity Enhancement Act of 2014[17]: It was signed into law December 18, 2014. It provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

Federal Exchange Data Breach Notification Act of 2015[18]: This bill requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach.

National Cybersecurity Protection Advancement Act of 2015[19]: This law amends the Homeland Security Act of 2002 to allow the Department of Homeland Security's (DHS's) national cyber security and communications integration center (NCCIC) to include tribal governments, information sharing, and analysis centers, and private entities among its non-federal representatives.

[13] Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996)

[14] (Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999)

[15] (Pub.L. 107–296, 116 Stat. 2135, enacted November 25, 2002)

[16] (CISA S. 2588[113th Congress], S. 754 [114th Congress])

[17] 113th Congress (2013-2014)

[18] H.R.555 — 114th Congress (2015-2016)

[19] H. R. 1731[Report No. 114–83]

Going by the looks of the United States cyber security laws and regulations above, it is pretty evident that the government has been working to introduce stricter laws to equip organizations to secure the data from the latest cyber threats. However, *Bruce Schneier* rightly said that successful cyber-attacks on government systems still occur despite government efforts. This holds true for private companies as well.

It is advisable that organizations become proactive about the security of their apps and data. Cyber criminals are always on the prowl & are becoming sophisticated in their approach to attack. For the same reason, companies should keep a regular check on their systems to identify any vulnerabilities and address the loopholes immediately.

## UNITED KINGDOM

The UK NIS Regulations[20] (implementing the NIS Directive) come into force in the UK on 10 May 2018. The NIS Regulations represent a significant change in the legal environment relating to cybersecurity in the UK.

The NIS Regulations serve a number of purposes, including the development of the UK's national framework and strategy relating to network security. The NIS Regulations also impose new obligations on operators of "essential services" and digital service providers in relation to the security of their network and information systems. Companies that fall within the scope of the NIS Regulations should be aware of these obligations and how they can be satisfied, particularly given that the NIS Regulations introduce a stringent penalties regime for non-compliance.

Under the NIS Regulations, entities meeting certain threshold conditions in the energy, transport, healthcare, utilities and digital infrastructure sectors will be considered to be operators of essential services. Competent Authorities also have discretion to deem a particular organisation to be an operator of essential services even if these threshold conditions are not met.

Providers of essential services are required to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential services rely. Providers of essential services must also notify

[20] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union". EUR Lex. Retrieved2018-04-26

their designated “Competent Authority” within 72 hours about any incident which has a significant impact on the continuity of the essential services that they provide. The relevant “Competent Authority” depends on the sector in which the provider of essential services is operating. Such “incidents” may include cyber-attacks, power outages, system malfunctions and hardware failures.

The NIS Regulations impose similar obligations on digital service providers that provide online marketplaces, search engines or cloud computing services in the UK.

Penalties for non-compliance with the NIS Regulations are potentially severe, with fines of up to £17 million permitted in some circumstances.

UK Cybersecurity law is mainly governed by the following acts.

- Computer Misuse Act 1990[21] – this specifies various hacking offences
- Official Secrets Act 1989[22]– this deals with national security
- Communications Act 2003[23] – this is the main source of UK telecommunications law
- Data Protection Act 1998 [24]– this implements the Data Protection Directive 1995
- Privacy and Electronic Communications (EC Directive) Regulations 2003 [25]

## COMMENTS

In the words of Tata Communication's Chief Technology Officer, Srinivasan CR

“As companies, and government departments move more and more sensitive data of employees and citizens online, India is facing an acute shortage of trained cybersecurity professionals, "People with the right cyber security skills are in short supply," Srinivasan said. "That is why we are working with universities, and have been collaborating with the Sastra university to set up a cyber security lab."

[21] 1990 (c. 18)
[22] 1989 c. 6
[23] 2003 c 21
[24] 1998 c.29
[25] (SI 2003/2426)

Srinivasan's comments echoed Andhra Pradesh's chief cyber security officer's observations in an interview with HuffPost India earlier this year.
"There is a significant skill gap in the market, where people who are studying aren't in sync with the needs of the industry," Srinivasan added. "We are trying to do guest lectures, and set up internship programs, so that people come into the industry with the required skills."

One thing that Indian Government must understand and combat is its approaches to provide beter cyber commerce and transaction that is free from cyber attacks and crimes. It was very evident from the authors interview from victims of hacking and phishing which made him believe that we as Indians are lagging extremely behind in order to maintain good and reputed cyber environment for our customer and citizens.

It must be understood that there are around 13 internet root servers in the world which are responsible to provide internet access all around the world. Bur what is shocking to note is that from those 13 around 10 are located in USA itself. Thus, it is very pertaining to know that whatever data or Information we send, it can be accessed by those root servers. Moreover, there is not a single root server which is located in India making the Indian Data and Information more vulnerable to cyber-attacks. Therefore, the most essential change that India must bring in is to try and get its on root server.

## CONCLUSION

Cybersecurity of nations is a critical issue at present. It affects the economy as well as the basic functioning of a society. There are numerous threats to cybersecurity, both internal and external. The way in which a nation attempts to address cybersecurity is often rooted in its history – historical ways in which the state has used its communications infrastructure to control and maintain power vis-à-vis use it as a developmental tool. India, with is history of colonization falls primarily in the former category, in which the information and communications infrastructure was used by the British rulers as a tool to control.

Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, Dublin, Ireland, December 10, 2016 13interception of messages of the citizens. The initial motive seems to have been an aversion to foreign ideas, and ergo, the compulsion to control such ideas and not let new ideas take root among Indian citizens. Later, such control mechanisms became useful tools for the ruling parties to maintain power and restrict the voices of the opposition parties.

Over time, the voices of democracy and civil society has begun to prevail, and formerly restrictive laws have been amended to incorporate more transparent procedures. But in most cases, such transparency has had to be fought for in the Courts. The role of the press and civil society have been indispensable in this.

At present, the main threat to the nation's security comes in the form cyber threats. Thus cybersecurity has emerged as the most important policy issue that affects the security of India.

The government seems to have taken some baby steps towards achieving cyber security. However, as noted above, this is a work very much in progress. It is important for both policy makers as well as citizens to seek and achieve the right balance, i.e. implement cybersecurity with a focus on balancing nationalsecurity with privacy concerns.

## BIBLIOGRAPHY

Acharya, B. 2015, May 30). Mastering the Art of Keeping Indians Under Surveillance.

Retrieved from http://thewire.in/2015/05/30/mastering-the-art-of-keeping-indians-undersurveillance-2756/

Agarwala, B. D. 1996). Right to Privacy: A Case-By-Case Development. Supreme Court Cases,

3(9). Retrieved from http://www.ebc-india.com/lawyer/articles/96v3a2.htm

Bharadwaj, K. 2010. How Safe Is This Shore? - Data Protection And BPOs In India. John

Marshall Journal of Computer and Information Law, 27.

BSNL Calcutta Telecom District. 2012. History and Growth of Calcutta Telephones. Retrieved

June 3, 2016, from http://www.calcutta.bsnl.co.in/mainfooter/MainFooter_Company.html

Dharmakumar, R., & Prasad, S. 2011, September 19. Hackers' Haven. Retrieved May 14, 2015,

from http://forbesindia.com/printcontent/28462

Dhavan, R. 2000, April 21. The Hindu : Tapping Mr. Cronje. Retrieved June 4, 2016, from

http://www.thehindu.com/2000/04/21/stories/05212523.htm

Dugal, P. 2008. Legal Issues Relating to Outsourcing in India. International Journal of Legal Information, 36.