International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Global Perspective: Cyberlaw, Regulations and Compliance

Syed Meharanjunisa

University of Mysore, Mysore, Karnataka, India

ABSTRACT

Cyber security provides protection to the internet connected networks and system from the cyber-attacks. To stop attacks everyone must know and aware of all cyber law, regulations and compliance to secure the cyber. Cyber security is all about to stop cyber-crime. Cyber security is must and we have to know about all safety measures required to stop cybercrime. This paper give details information about cyber security and its safety measure. Also we will discuss about the activities related to it and how actually cybercrime happens and all steps taken by the various organization and Government to have cyber ethics everywhere. Cyber security provides protection against the cybercrime and teach us what essential safety measures one need to follow from all cybercrimes. Securing online information is priority where everyone is involved with technology. Whenever anyone talked about cyber security, straight one thing comes in mind that is cybercrime and what safety measures need to take to be safe from it.

KEYWORDS: *Cyber security, cybercrime, safety measures, cyber ethics*

How to cite this paper: Syed Meharanjunisa "Global Perspective: Cyberlaw, Regulations and Compliance" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.4-7, URL: www.ijtsrd.com/papers/ijtsrd31684.pdf

IJTSRD31684

I. INTRODUCTION

A cyber security regulation comprises of ordinances that protect information technology and computer systems to protect the organization from cybercrimes and cyber-attacks of viruses, phishing, unauthorized access etc [1]. There are many measures to prevent from all these. Cyber Security refers to the all safety measure taken to protect from all deception practices done online to steal personal data and to protect networks, programs, devices, damage and any unauthorized access. Any information which transferred through network can be easily hacked these days and everyone access most of the things only whether it is professional or personal. In organisation most of the work done through email, audio video conferences, HRMS, etc. and in personal people do online banking as well. Even the online chats are also not safe these days [2-4]. Anyone while doing work ever think of that how much it is secured to access everything online. Cyber-crime is increasing day by day therefore there are various organisation and Government who come in front to deal with all kind of cyber-crimes. IT industry must focus on safety measure as 60 percent of total transactions are done online so this field must have high quality of security to give all safety to users while doing any transactions. Even the cyber space these days are not safe. Latest technologies like E-commerce, mobile computing, cloud computing need high cyber security standards. Making the internet safer is the important and integral part of the development IT Services and for Government also important to look into it to safeguards IT Services. Though we have individual cyber cells to deal every individual case and the response time is great. In 1903, first attack came into existence and after that frequent crimes came up. People associated with cyber security but it is more than that. The modern hackers are there who are breaking down cyber securities. Method have increased of hacking, new techniques and new ways came up of cybercrime. These tools know a exploit kits which is designed to exploit human and to blackmail them and get all information. Effective cyber security will protect but not necessary to protect network where hackers will not attempt to attack and target to track the system or whole server. But by cyber security, it will difficult for hackers to crack the firewall and get into it [3-6].

II. CYBER LAW

Cyber law is the law which deals with overall legal system of cyberspace and internet legal issues which covers broad area of cyber and all legal issues including right to freedom on internet, freedom of expression, access to and usage of internet and privacy of individual on internet. In common language cyber law is the law of internet. In 1986, first cyber law was enacted which covers computer fraud and abuse act [7].

III. REQUIREMENT OF CYBER LAWS

Like existence of any other law, a cyber law is also created to help people and organization to protect them from all legal cases which is done online. It protects and safe against any crime done online. For example, if anyone do any crime online, victim can take action against that person and fight till the time criminals get punished or sentenced. If you break cyber law there are different kinds of punishment depends upon what you affronted, where you broke and

where you live. There is situation when your website gets suspended or banned if your IP address is found in any criminal activity and it will get blocked also. If someone committed more serious crime such as hacking, misusing of any personal data, hacking website, company distress etc. then some serious action must take against you where one ca have to give good amount of penalty or may get into prison as well [8,9].

IV. CYBER REGULATION

A cyber regulation is the regulation which comprises of ordinances to protect individual and organization of any kind of fraud related to cybercrimes like phishing, unauthorized access, viruses, worms, personal online damage etc. Regulations are meant to prevent from all these. In India, the Information Technology Act, 2000 came into existence to provide legal acknowledgement to online communication and to facilitate filing of online records with the Governments. Regulations covers all aspects of crime related to cyberspace and provide judgement basis on ordinance [10].

V. CYBER COMPLIANCE

Compliance is defined as rules and requirements meeting. Cyber compliance is to create compliance which controls risk based crime and protect the integrity, confidentially and accessibility of information which are stored safely so that it can be processed and transferred. Every organization have their own cyber department which look after the cases and they have there on compliance to deal with the cybercrimes [11,12].

VI. STEPS TO CREATE CYBERSECURITY COMPLIANCE

There are 5 steps which may create cyber security compliance program as follows-

1. **Develop Compliance Team**- An organization must have compliance team whether the company is small or big, must have team of compliance to handle all work and issues related to cyberspace and can communicate to across business and IT departments.

2. **Determine a Risk Analysis**- Organization must follow and have approach on risk based to compliance and easy flow risk analysis process.
   - Identity of all information systems, assets, networks and data access.
   - One can access the risk at all level and determine high risk information stored, collected and transmitted.
   - After access of risk, one need to analyse the risk by using formula
   - Once the risk is analysed, one need to determine how to handle it whether to keep or reject the risk.

3. **Arranged Controls**- Based on risk analysed one need to set risk controller like arrange of firewalls, strong password policies, encryption, two factor authentication protection, insurance, training of employee etc.

4. **Generate Policies**- Create policies documents which controls and aware about all compliance of activities and controls.

5. **Monitor and Respond**- All compliance must be check and monitor to respond on time to time and find out new ways to treat with threats and any kind of vulnerabilities [13].

VII. GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE (GRC)

As compliance and risk go simultaneously organization must implement governance, risk and compliance (GRC) program to improve sharing information among one another. The compliance feature of GRC is to define to take legal requirement in the organization for management process to identity the role of legislation, policies and regulations to deal with legal aspects and develop the compliance report. GRC will help in analysing the gap to know the risk potential associated with compliance versus potential costs of non-compliance actions [14].

VIII. CHALLENGES OF CYBER SECURITY

There are many challenges while doing effective cyber security in an organization or for personal reasons [15-18]. Few of them are as follows-

1. Network Security - The networks are not secure as there are many unwanted users sitting online and ready to attack and destruct the interventions.
2. Application Security- Regular updating of mobile and computer application is must to ensure any kind of attacks and need to check on time to time.
3. Data Security - Second layer of security is required to secure data on applications and network which is very challenging. The use of two factor authentication safety is must these to protect themselves from cybercrime.
4. Cloud Security- Cloud protection is must which require large amount of space and online safe environment to protect from data stolen.
5. Mobile Security- It involves every type of security from login to space, from chat to banking which again require conscious user's involvement

IX. CYBER ETHICS

Organization must aware of cyber ethics of internet and use this practice for proper use of knowledge to safe internet. There are few points which need to consider for cyber ethics-

- Do not use any offensive and violent language
- Cyber Bully is a crime so don't bully
- Plagiarism of any content come under stolen and hacking.
- Involve with someone other computer or network comes under cybercrime.
- Follow the copyright rules, never download material or software's which involve the information of other. Always us free data available on internet or software's.

Cyber ethics is significant and must be trailed by everybody and takes the responsibility to decline the cybercrimes [13-16].

X. SAFETY MEASURES FOR CYBER LAW SECURITY SYSTEM

Basic precautions must be taken by everyone who use internet and online transactions and work:

1. Security Suite- Keep real time full security through

secure suite which will protect from online malware and from any loss of personal and professional loss.

2. Strong Password- Password must be strong and powerful so that no one can guess and use it for any kind of fraud and it should be changed frequently by using special character.
3. Regular Update Software – It is important for OS and internet security to update regular software to avoid any kind of cybercrime as criminal's use known exploits and flaws to gain access of system.
4. Manage Social Media Settings- Cyber criminals keep an eye on social media information so it must be locked and frequently change like password. Share as much less information on social media so that anyone won't be able to guess security questions answers.
5. Intensify Home Network- Home network must have strong encrypted password and have virtual private network. If cybercriminals do succeed to drudge your interaction link, they won't intercept anything but encoded data. It's a great idea to use VPN in both public and personal network so that it protects everywhere.
6. Secure Personal Computer- This can be done by activating computer firewall, using anti-virus, malware software and block spyware attacks by regularly installing and updating software's.
7. Secure Mobile Devices-Mobile devices must be updated and password protected in two-factor authentication and applications must be downloaded from trusted sources.
8. Install latest Operating System- All Current and updated operating system must be used in Windows, Mac, Linux to prevent potential attacks on older software.
9. Use of Big data sciences and data mining techniques for additional security cover to preven cyber breaching [19-21].

XI. CONCLUSION

For the emerging trend of online crime cases, it is very important for every organization to have compliance department which handle all cybercrime cases and must aware of cyber law and regulations to deal with it. Cybercrime are coming with new faces these days and we listen many kinds of crimes related to it. We must follow regulations and aware of cyber law to handle all compliances and must take legal action to stop it in future. There is no absolute solution of cybercrimes but one can take precautions while using online and networks. Organization must emphasis on regular trainings to IT department and basis training to every department to enhance the knowledge of online uses of networks, data and information so that they can save the work. Individual also must be aware of cyber law, regulation and compliance to deal with any kind of issues related to cybercrimes. Cyber security takes all measures to protect online crime and use as a safeguards with regulations and compliances for all networks, programs, software, data and information. The protection and prevention of network is must and provide all intentional and unintentional intrusion for both inside and outside system to protect and ensure assurance, integrity of information and data online.

XII. REFERENCES

[1] Rahul Reddy Nadikattu, New Ways of Implementing Cyber Security to Help in Protecting America x Journal of Xidian University, VOLUME 14, ISSUE 5, 2020, Page No: 6004 - 6015. Available at SSRN: https://ssrn.com/abstract=3622822 (May 14, 2020).

[2] M. Bada, A. M. Sasse and J. R. Nurse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv, abs/1901.02672*. (2019).

[3] A. Ertan, G. Crossland, C. P. Heath, D. Denny and R. B. Jensen, Cyber Security Behaviour In Organisations. *ArXiv, abs/2004.11768*. (2020).

[4] M Lakshmi Prasanthi. Cyber Crime: Prevention & Detection International Journal of Advanced Research in Computer

[5] M. H. Kumar and A. S. Rani, Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *International Journal of Advance Research, Ideas and Innovations in Technology, 5*, 1343-1346. (2019).

[6] K. Halouzka and L. Burita, Cyber Security Strategic Documents Analysis. *2019 International Conference on Military Technologies (ICMT)*, 1-6. (2019).

[7] J. Rosenoer, Cyber Law: The Law of the Internet. (1996).

[8] G. M Someswar and K. Roopanjali, Constitutional Implications of Cyber Security Laws in India. *International Journal of Research, 5*, 601-620. (2018).

[9] B. Sahu, N. Sahu, S. K. Sahu and P. Sahu, identify Uncertainty of Cyber Crime and Cyber Laws. *2013 International Conference on Communication Systems and Network Technologies*, 450-452. (2013).

[10] Podbregar and P. Sprajc, Adaptability of state to a new CI challenges – with focus on cyber warfare domain. *National security and the future, 19*, 187-199. (2018).

[11] S. E. Blythe, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control. *Journal of Management Policy and Practice, 11*, 19-33(2010)..

[12] S. Chatterjee, A. K. Kar, Y. K. Dwivedi and H. Kizgin, Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Inf. Technol. People, 32*, 1153-1183. (2019).

[13] https://www.computerhope.com/jargon/c/cyber-law.htm

[14] https://digitalguardian.com/blog/what-cyber-security

[15] https://www.rcmp-grc.gc.ca/to-ot/tis-set/cyber-tips-conseils-eng.htm

[16] https://www.computerhope.com/jargon/c/cyber-law.htm

[17] Mohammad, Sikender Mohsienuddin, Security and Privacy Concerns of the 'Internet of Things' (IoT) in IT and its Help in the Various Sectors across the World x International Journal of Computer Trends and

Technology (IJCTT) – Volume 68 Issue 4 – April 2020. Available at SSRN: https://ssrn.com/abstract=3630513 (April 4, 2020).

[18] Soni, Vishal Dineshkumar, Challenges and Solution for Artificial Intelligence in Cyber security of the USA. Available at SSRN: https://ssrn.com/abstract=3624487 or http://dx.doi.org/10.2139/ssrn.3624487(June 10, 2020)

[19] Rahul Reddy Nadikattu, Data Warehouse Architecture – Leading the Next Generation Data Science Rahul Reddy Nadikattu "Data Warehouse Architecture – Leading the next generation Data Science" International Journal of Computer Trends and Technology 67.9 (2019):78-80.. Available at SSRN: https://ssrn.com/abstract=3622840 or http://dx.doi.org/10.2139/ssrn.3622840(September 11, 2019).

[20] R. Hewett, S. Rudrapattana, P. Kijsanayoth. Cyber-security analysis of smart SCADA systems with game models. Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109–112.

[21] RachnaBuch, Dhatri Ganda, Pooja Kalola, NiraliBorad, World of Cyber Security and Cybercrime. Recent Trends in Programming Languages. ISSN: 2455-1821 (Online) Volume 4, Issue 2