IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 20-23

Cyber Security & Role of Cyber Law

Asst.Prof.Rajesh Gauns[1], Asst.Prof.Nora Naik[2]
Computer Engineering Department
Agnel Institute of Design & Technology
Assagao,Mapusa,Goa
rkg@aitdgoa.edu.in[1]
nn@aitdgoa.edu.in[2]

Abstract: *Considering modern era and Wide spread use of Internet Technology & Information Technology has given a new rise to dimension of communication today. This has cemented a new way for e-commerce, internet technology, e-solutions etc., which has led to reduction of costs. Many users of internet technology which are termed as cyber punks, crackers, hackers, have been able spread their roots to interfere with the internet accounts through various techniques of cyber-attacks and get admittance to the user's computer system and use that data to gain profits from stolen information. As Internet Technology is evolving with tremendous development in hardware sectors, internet alone can be used as a tool for betterment of a society or can be used as a tool to harm any individual/group/organization/nation. It has resulted in several threats to the consumers all around the globe who are now a day's using internet as a platform to perform daily activities such as buy/sell/e-banking and many more. In this paper we focus on rising concern about cyber security and its effect on the individual/group/organization/nation, how can we keep data more secure by improvising some facets of the cyber law in our country and also focuses on key comparisons on cyber law in other country such as United Kingdom with India.*

Keywords: *Cyber Security, Cyber Law, Attacks, Hackers.*

I. Introduction

Cyber security means protection of data over the network from attacks. These attacks have the capacity to change the data, modify the data, alter the data, can be used as a means for extortion from users, or just as eavesdropping which can help the attacker know understand the process which he is interested to figure out.

The impact of the internet as a vibrant reserve has certainly not been restricted to the developed world, in spite of considerable changes in technological development. However, the internet advanced in a different way in different jurisdictions due to their unique economic, social and political situations. Cyber security can have several, possibly challenging viewpoints – economic (as in protection of businesses), social (protecting individual privacy) or sovereign (national security). Cyber security means different things for different stakeholders, who rank certain viewpoints higher over others. The foremost cyber security policy usually reflects which of these views controls political discourse. For instance, finding the institutions as Critical Infrastructure [1]("CI") as areas of specific worry for cyber security helps know the perspectives on 'criticality' within each jurisdiction. Critical infrastructure identification is an essential element of national cyber security policy, and helps identify areas of importance when making policy. Evaluating criticality delivers some perspective on the discursive politics of cyber security. Critical Information Infrastructure[1] ("CII"), which, as the terminology suggests, is CI in information networks, and to which cyber security is possibly most relevant, can be assessed as structurally critical i.e., significant from the viewpoint of the interdependence of numerous other systems outside of cyber space to information infrastructure. Cyber security guidelines can have accomplishment on civil liberties, on the right to privacy and the freedom of speech, expression and the liberty of organization. Countries have diverse methods on how these values are protected in regulation dealing with cyber security, and what level of legislative or judicial oversight cyber security bodies have.

II. Cyber Security Plays A Vital Role

Today all are connected via the technology using smartphones, desktop computers which are linked to every possible infrastructure such as banking, hospitality, and keeping them safe from the cyber attacks will enable proper functioning of our day to day life process. Cyber defense protects all the users across the world by keeping their identity safe, data safe, keeping them away from the extortion etc.

Researchers who devote share of time on undertaking research about the cyber-attacks, helps to find new upcoming threats that can affect us. Thus helps in figuring out new vulnerabilities, also can educate public/society/government etc and can help in making the defense stronger.

III. Types Of Cyber Security Threats

Ransomware: Users file system is totally encrypted and if that particular user wants to have access to files he has to pay some ransom money and then the system files are decrypted and unlocked for the use.

Malware: Any program that can harm the computer files (alter,deletes,modifies,copies) such as viruses, worms etc.

***Phishing*:** Some misleading electronic mails are sent which appears from a trustworthy sourceto steal the information such as credit card details etc[18].

CYBER-ATTACKS: A MOUNTING FEAR

IT industry is playing a dynamic part today in all possible sectors such as e-commerce, being service providers, etc. Many small scale companies are dependent on IT industry today, thus making cyber security a main concern.

If data breach occurs in Company *A*, clients/customers which are having any relationship with the company *A* will be in fear as such this data breach could lead to financial loss to them and also could be a possible threat for them to think of having such data loss in future.

In many ways data breach can happen, one way could be through the people working in respective companies who pass the information to third parties which could eventually get them in some profit. The biggest attack that had impact in the past few years is hacking. Even after knowing that hacking is a threat and is affecting the organization through which data can be lost or stolen through employees, still many companies do not have necessary policies in place to shield against this threat.

WHY IS CYBER SECURITY A GROWING CONCERN?

Framework

Inside the Government, there are several institutions which are responsible for sometimes intersecting aspects of cyber security[2] there is not at all pure primary body responsible for developing cyber security policy.

The lack of a formal inter-governmental information sharing mechanism also damages collaboration between government bodies. The task of operationalizing cyber security initiatives falls on a mix of law enforcement agencies and newly created cyber security organizations, like the CERT-In[3] and NCIIPC[4]. Similarly, there is not one sole co-coordinating agency responsible for co-coordinating efforts towards cyber security in India.

The CERT-In, besides being the primary incident response agency for non-critical threats, is also the central agency responsible for information collection on cyber security incidents and also to monitor non-compliance with cyber security directions under the IT Act, and its mandate is broad enough for it to investigate and respond to potentially any manner of cyber security concerns, while the NCIIPC's function is limited to the identification and protection of CII. The CERT-In is obligated to convey cyber security incidents relating to critical sectors, to the NCIIPC[5].

Legal Antecedents

The closest antecedent to the IT Act, the Indian Telegraphs Act of 1885, has been used as a legal basis to take control of communications infrastructure (including the internet) by the Government, including for shutting down networks and intercepting communication. This law is regularly used to deny internet access to politically volatile areas although its application to issues of cyber security is not known. Prior to the introduction of the Indian Information Technology Act, India did not have existing criminal law addressing issues of cyber security, such as targeted attacks against computer infrastructure. However, existing criminal law has been used to prosecute instances of 'data theft', which includes unauthorized access to computers [6]. There are no incidents of courts interpreting common law duties of care which are owed under tort law (for example for maintaining confidence), for the protection of data or computer resources, although there may be some support for such a duty within the interpretation of the tort of breach of confidence in India.

THE ROLE OF THE CYBER LAW

Cyber law concerns the whole world. As the internet is continuously evolving many people are committing traditional crime such as robbing a bank on digital grounds such as internet thus the nature and purview of Internet is changing, and this new standard is being the ultimate medium ever evolved in human history, every activity in cyberspace will have a cyber legal dimension to it.

Cyber Law or Internet law is a term that covers the legal issues which are related to the use of the Internet. It is important as it includes all aspects of transactions and activities happening over the Internet, and Cyberspace.

Cyber law concerns one and all. It is a frequently growing. As the nature and scope of Internet is shifting, every activityof the over the internet will have a cyber legal point of view.

CYBER SECURITY CAN BE IMPROVED USING CYBER LAW

The law can carry out two vital roles:

1) Enhancing cyber security awareness.
2) Shielding consumers.

Companies within the same jurisdictionscan have a familiar, minimum and compulsory standard of security, which will lead to a unified defense against attacks. This will develop trust and business relationships among each other since they understand that partners and other stakeholders that they are dealing with are also protecting their data. In order to break down the jurisdiction barriers between nations an international legal standard should be brought into act.

The law can impose protection by making firms to report data breaches, enabling the appropriate government establishments to take action to make security stronger and authorize individuals to lessen harm, as well as encouraging organizations to take up effective security measures and guard their internal systems.

COMPARISON OF CYBER SECURITY POLICY IN INDIA AND THE UK

A major focus of cyber security in India and UK[7] has been on national security in light of the growing threat of terrorist organizations. Both nations have therefore attempted to expand the influence of cyber security through security legislation.

The pastbackground to cyber security in India and the UK has affected policy development in this area considerably. In particular Cyber security has been a priority in UK [8]considering India, and as a result, the UK has a much better defined policy and framework for cyber security. India and UK struggled to get used to existing law to speedy technological expansions, choosing instead to develop new legislation [9][10] or new institutions to focus specifically on cyber security.

Scope of Cyber Security

India and the UK both identify cyber security as a national priority. Both countries are looking forward to address cyber security through their national cyber security policies[11][1]. However, there are significant cracks in actualizing cyber security measures. In India, for instance, cyber security initiatives are hobbled by the lack of a fixed and recurring budgetary allocation.

Both jurisdictions primarily assess cyber security from a national security point of view, although the UK has a larger emphasis on multi-stakeholderism and is more collaborative in its approach.

Threats to cyber security are more clearly identified in UK policy, which identifies various objects which could pose a threat. The development of a threat typology is not as apparent in India.

The UK prioritises government data protection in its policies, while this is missing in India.

In terms of military policy, the UK places a strong emphasis on cyber offensive capabilities, while India concentrates on defensive capabilities.

Cyber Security Structures

There are important industry and civil society stakeholders in both India and the UK. UK has a much more robust cyber security society than in India, with industry bodies and civil society being important stakeholders in developing policy as well. This consultative framework could possibly be the reason for the UK adopting a light-touch regulation towards industry standards and reporting requirements. Further, both jurisdictions have programmes and structures aimed at skill.

There is an absence of a central coordinating organization in India, which is a function fulfilled by the UK National Cyber Security Centre [12]. However, the proposed National Cyber Coordination Centre is expected to fulfil this role in India.

International

Both jurisdictions support a multi-stakeholder model for internet governance in international forums. However, India's advocacy for such a model is a more recent development, and is not made out from its general emphasis on sovereign concerns. The UK, on the other hand, has been quite pro-active in engaging with the multi-stakeholder model, even where cyber security is concerned.[13]

IV. Conclusion

There are two major areas that are in need of governmental attention at the moment through which cyber-security can be improved: (i) clear policies on cyber security, and (ii) relevant legislation supporting the policy that would enhance cyber security. The considerations of the policy is of very important and should include first and foremost long-term educational efforts on all levels of society including general education on cyber security matters, as well as professional education of law enforcement, judiciary and legislative authorities. Also, an important component of a viable policy is promoting international discussion on the issues cyber security and its management on an international level. While international cooperation is necessary, each nation will have to develop, as a foundation, its own national cyber security strategy, authorities, and capabilities. Within any given nation state, adequate cyber security will require effective coordination and cooperation among governmental entities on the national and sub-national levels as well as the private sector and also civil society.

References

[1]. http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.
[2]. https://internetdemocracy.in/watchtower/
[3]. https://www.cert-in.org.in/
[4]. http://nciipc.gov.in/.
[5]. http://www.orfonline.org/expert-speaks/policing-cyber-crimes-need-for-national-cyber-crime-coordination-centre/
[6]. http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Compendium-15.11.16.pdf
[7]. Gregory T. Nojeim, Cybersecurity and Freedom on the Internet, 4 Journal Of National Security Law & Policy, 119, (2010).
[8]. SaikatDatta, Internet Democracy Project, Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, (January 2016) available at https://internetdemocracy.in/reports/cybersecurity-ig-ifp saikat-datta/
[9]. https://www.cert.org/historical/annual_rpts/
[10]. http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Compendium-15.11.16.pdf
[11]. http://nciipc.gov.in/
[12]. https://www.iso.org/isoiec-27001-information-security.html
[13]. https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement