A Study on Cyber Security, Its Issues and Cyber Crime Rates in India

Saurabh Mishra, Saru Dhir and Madhurima Hooda

Abstract In the current technological era, use of computers becomes an essential part of our lives. But this part is also affected by a new breed of security known as cyber security. It is a global issue that arises by different organisations. This paper presents the global cyber security scenario, cyber security and its practices, and firms who are major stakeholders in the cyber security. At the end counter measures of cyber crimes, its average rate is calculated in India during the years 2009–2013.

Keywords Cyber security · Issues · Cyber cases · Cyber crime

1 Introduction

Today, cyber security has become a global issue attracting widespread concern from all across the world from various organisations such as Governments and International Bodies. A simple reason for it: browsing on a trusted website can completely compromise your computer, allowing a hacker to read your sensitive files or worse, and delete them. The term 'hacker' has become a part of our everyday scenario, and projected in nearly daily headlines.

Global cyber crime incidents are increasing at a rapid rate which is not only unprecedented but also alarming, for much of today's critical infrastructure like electricity, water, gas and secure data, like banking is completely computer based. In such a scenario, a cyber attack on the stock market would probably affect more people than a bomb in a marketplace. Governments are hiring computer security

S. Mishra (✉) · S. Dhir · M. Hooda
Amity University Uttar Pradesh, Noida, India
e-mail: mishrasaurabh95@gmail.com

S. Dhir
e-mail: sdhir@amity.edu

M. Hooda
e-mail: mhooda@amity.edu

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,
Advances in Intelligent Systems and Computing 413,
DOI 10.1007/978-981-10-0419-3_30

professionals to counter the growing menace. Every day, new advancements in cyber security are made. Ethical hackers are a very important part of the cyber security movement throughout the global scenario. Cyber security is being made available to all computer users. Cyber security is thus an integral part of the IT scenario, today and overlooking it can gravely undermine the IT sector itself. Cyber security and IT sector are closely entwined where the cyber security is for everything, from computer viruses, Trojans, worms and other malicious programmes; to malicious characters like hackers who intend to get into your computer system; and to security protocols, policies and compliance and regulatory concerns. Here, an effort has been made to give a research-oriented analysis and point of view cyber security, ethical hacking and why we need both to keep the IT sector going smoothly. An effort has been made to do an analysis of cyber security issues, firms that are providing cyber security services, and measures for effective cyber security in India.

2 Literature Review

Cyber security today has become a global issue, for it has now become a matter of economic importance, privacy in society and national security where the cyber network has become a part of the national economy. Security models suggest that to counter this in an effective manner and keep the attacks in check, it is recommended to place intrusion detection devices at the weak points of the networks [1].

Security system has its disadvantages as well; new techniques are being developed today like applications that take part in their own defence [2]. An effective counter measure for protection is the use of DNS health indicators where a proper method and procedure defines the way for measuring the DNS security levels. Such a step can help secure the critical infrastructure during a cyber attack or cyber war scenario [3].

As an analysis, it was found that undetected malware attack cut off the Royal Air Force and Royal Navy from defence network access, and most of hospitals also had lost their network connectivity due to the same malware attack [4]. Furthermore, research and development has been done to obtain self-reliance; and compliance and enforcement have been applied. A good international cooperation from international organisations like UN has also helped the country in obtaining its objective [5].

Major stakeholders in the computer industry are also the top cyber security firms today such as Hewlett Packard Company, Dell Inc., IBM and Intel Corporation, which are all providing cyber security services to a wide population, whereas Kaspersky Labs and Symantec Corporation are providing antivirus solutions to the general everyday users and providing cyber security solutions. All these firms have been providing cyber security solutions and have been the front runners in the cyber security movement [6]. Meanwhile, people ask today, “Can cyber terrorism really affect our computer systems and jeopardise a Nation’s security?” [7]. Well, the

answer to this is "Unfortunately, yes"; probably the reason why all agencies, from FBI and CIA to the Indian RAW, have their own specialised cyber security cells. The US suffered from the largest power outage in history on 14 August 2003, which left one-fifth of the population without power, i.e. about 50 million people for over 12 h [8].

3 Issues Relating to Cyber Security

Cyber security today has several issues: Phishing, pharming and e-mail spoofing. These are all issues faced by people while simply browsing the internet or using services like net banking [9].

One of the biggest and most significant cyber security issues is the one being faced by each nation in the world today: An attack on their critical infrastructure and information grid. The U.S. has setup a Defense Critical Infrastructure Programme (DCIP), where each critical infrastructure is assigned a separate lead agent to provide security [10]. Cyber criminals use address and logos resembling those of trusted organisations like banks to obtain the user's privacy information like passwords and credit card numbers. A case of a very good cyber security and protection step is that of the Malaysian Government to counter the cyber security issues faced by the country. It was aimed at protecting assets vital to the nation like it is image, defence and security and different sectors through affective governance, a good legislature and regulatory framework, a strong cyber security technology framework and developing a culture of security and capacity building in its citizens [11].

A very stunning and alarming cyber security issue, whose significance is understood by very few, is how easily hacking tools are available today on the internet and can be used to create severe cyber security problems that can cripple even an entire nation. An example for this is the "Eligible Receiver", exercise conducted by the National Security Agency (NSA) in 1997, where the NSA conducted an experiment by briefing 35 computer hackers to hack and disrupt U.S. National Security Systems and Databases using only software and hacking tools available freely for download on the Internet. The results were appalling, where the 35-man team was able to compromise several security sectors in the U.S. Pentagon and other Government organs [12]. And sadly, this issue can never be kept entirely in check, as such tools for hacking can never be entirely removed from the internet.

4 Survey Results on Cyber Security in India

To give a brief idea of the cyber crime scenario, we will take the case of India, where a survey of cyber crimes committed during the period 2009–2013 was done by the National Crime Records Bureau (NCRB) [13]. The graph as shown in Fig. 1

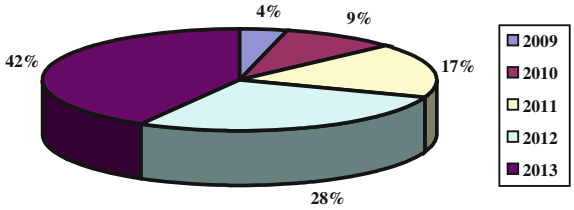


Fig. 1 Cyber crime cases registered under year 2009–2013

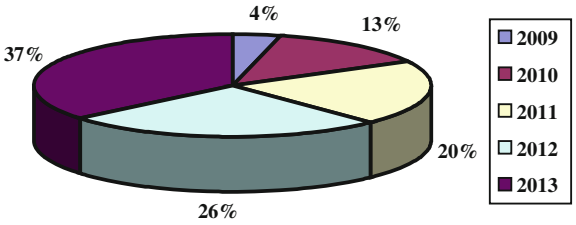
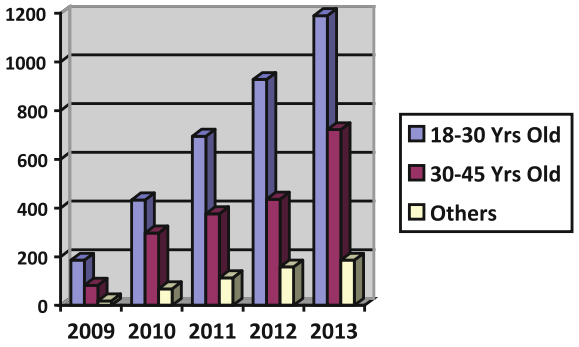


Fig. 2 Persons arrested for cyber crimes under year 2009–2013

Fig. 3 Age-wise breakdown of people arrested for cyber crimes (2009–2013)



represents that how there has been a steady rise in the number of cyber crimes cases registered in India in the past 5 years. From a mere 420 cases in the year 2009, it has risen to 4356 cases in the year 2013, which is more than 10 times the number of cases registered in 2009.

Figure 2 represents how there has been a sharp rise in the number of cyber criminals in the recent years, where, of the total people arrested in the last 5 years, 2098 people were arrested in the year 2013 alone. This is 37 % of the total criminals arrested in the period 2009–2013 for committing cyber crimes.

The graph in Fig. 3 shows how there has been a steady rise in the number of people arrested from all age groups. But one can clearly notice that the maximum number of people arrested for committing cyber crimes is in the age group of 18–30 years, followed by people of the age group 30–45 years.

5 Conclusion

With this paper, we have discussed the global cyber security scenario, where today the critical Infrastructure, people's privacy and internet protection are all under threat from the increasing number of cyber crimes. We have discussed cyber security and its practices, and firms who are major stakeholders in the cyber security scenario. We have also taken up cyber security issues and discussed their countermeasures. A general idea about the number of cyber crimes and criminals arrested in India has also been given through survey results for the years 2009–2013.

References

1. Jessie J Walker, Travis Jones and Roy Blount. Visualization, Modeling and Predictive Analysis of cyber security attacks against cyber infrastructure oriented systems. 978-1-4577-1376-7/11. page no. 82. IEEE (2011).
2. Rick A. Jones, Barry Horowitz. System-Aware Cyber Security. 978-0-7695-4367-3/11. page no. 914. IEEE (2011).
3. Andrea Rigoni, Igor Nai Fovino, Salvatore Di Blasi, Emiliano Casalicchio. Worldwide Security and Resiliency of Cyber Infrastructures: The Role of the Domain Name System. 978-0-615-51608-0/11. page no. 2 (2011).
4. Desire Athow, Trojan Malware Penetrates British Navy Defences–http://www.itproportal.com/2009/01/16/trojan-malware-penetrates-british-navy-defences/ (2009).
5. UN-backed anti-cyber-threat coalition launches headquarters in Malaysia- http://portal.unesco.org/ci/en/ev.php-URL_ID=28464&URL_DO=DO_TOPIC&URL_SECTION=201.html/ (2009).
6. Top 20 Cyber Security Companies 2014- http://www.reportlinker.com/p02148719-summary/Top-20-Cyber-Security-Companies.html (2014).
7. A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace - http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace. (2013).
8. Major power outage hits New York, other large cities-http://edition.cnn.com/2003/US/08/14/power.outage/ (2003).
9. Alex Roney Mathew, Aayad Al Hajj and Khalil Al Ruqeishi. Cyber Crimes: Threats and Protection. 978-1-4244-7578-0. page no. 16-17. IEEE (2010).
10. Critical Infrastructure Threats and Terrorism. DCSINT Handbook No. 1.02. page no. 4 (2006).
11. Mohd Shamir B Hashim. Malaysia's National Cyber Security Policy: The Country's Cyber Defence Initiatives. 978-0-615-51608-0/11. page no. 2–7 (2011).
12. Gabriel Weimann. Cyberterrorism: The Sum of All Fears?. Studies in Conflict & Terrorism, 28:129–149. Taylor & Francis Inc., page no. 138. (2005).
13. National Crime Records Bureau. Crimes in India (Compendium). http://ncrb.nic.in/ciiprevious/main.htm.