© 2018 IJSRST | Volume 4 | Issue6 |Print ISSN: 2395-6011 | Online ISSN: 2395-602X
National Conference on Smart Computation and Technology in Conjunction with The Smart City Convergence 2018

Cyber Security for the Economy and Protecting Cyber Space Reliant Societies Again Cyber Threats

Department of Computer Engineering, Poornima Institute of Engineering & Technology, Jaipur, India

ABSTRACT

Internet is essential for development for both social and economic sectors to form vital infrastructures. Due to the increased use of Internet Cyber Threats are evolving and increasing rapidly. Two interrelated objectives of Cyber Security aims for strengthening cyber Security for the economy and protecting cyber space reliant societies again cyber threats. But, to achieve these two objectives in parallel is complex, and probably the main challenge of Cyber Security policy. With this objective, this paper analyses the background, characteristics, current research work, counter measure techniques and future research perspectives of Cyber security. Initially, mobile cloud computing is highlighted and then features and recent survey issues has discussed. Finally future trends have been discussed [1].

Keywords:- Cyber Security, Cyber Crime, Cyber Space, Cloud Services, Ransom Ware

I.INTRODUCTION

In this interconnected world and increased in the use of Internet Cyber Security crimes up 19 times over 10 years.

Cyber Security is a claiming issues that not only affects individuals but Government organizations, big enterprises and armed forces too.

In this increasing interconnected world, every user does not possess knowledge about the technical solution to the problems related to security.

Right from the loss of customer data to the intellectual capital continues despite of the increasingly efforts of IT budgets and sophisticated security solutions.

II. WHAT IS CYBER SECURITY? STRIVING FOR DEFINITION

Cyber Security is the solution which deals with the germinating Cyber Criminals, it is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization .The general objectives which Cyber Security comprises of:

- Confidentiality
- Availability
- Integrity

Creating an open, substantial, vital cyberspace which can be used by users safely and that supports open societies [3].

Table 1

	Today	2020
Estimated	7 billion	~8 billion

world population	people	people
Estimated Internet Population	2.5 billion people (35% of population is online)	~5 billion people (60% of population is online)
Total No. of devices	12.5 billion internet connected physical objects and devices (~6 devices per person)	50 billion internet connected physical objects and devices (~10 devices per person)
ICT Contribution to the Economy	~4% of GDP on average for G20 nations	10% of worldwide GDP

III. WHERE ARE WE ON CYBER SECURITY IN INDIA?

More than 50,300 cyber security incidents were faced by many Indian Organizations. There are many cyber security incidents including phishing, probing, website intrusions and defacements, virus/malicious code and denial of service attacks. "Around 10 million customer records were stolen from e-ticketing portal server of Indian Railway Catering and Tourism Corporation (IRCTC) website by Cyber Criminals". "Fraudsters spoofed the email account of Binny Bansal ,chief executive officer (CEO) of Flip kart, and sent two emails to the chief financial officer (CFO) demanding a transfer of $80,000". "A cyber Criminal known as Faisal breached the website of Canara Bank. The attacker defaced the site by inserting a malicious page and blocked some of its payment services". [10]

"RBI has registered a total of 9,500, 13,083, 16,468 and 8,689 cases of frauds involving credit cards, ATM/debit cards and internet banking during the year 2013-14, 2014-15, 2015-16 and 2016-17 (up to December 2016), respectively".[7]

There were 19 DoS attacks that exceeded 100Gbps during the first three month of year.

When referring to Cyber Security in India, we have to believe this that the security incident can happen to anyone at anytime; including us therefore we have to be prepared for our future. To detect malicious mechanism across an entire area, there are few organizations that have crossed maturity sufficient.

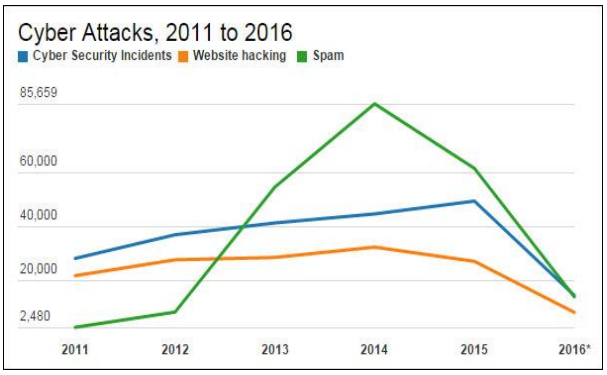

Figure 1. Year wise Cyber Attacks from 2011 to 2016[11]

IV. RECENT SURVEY ISSUES ON CYBER SECURITY TRENDS

“The development and adoption of new national cyber security strategies is an emerging trend characterised by its dynamism”.
Security will continue to escalate around not only securing networks but physical security too.

As per the recent Survey issues, there will be rapid increase in:

- Internal Threats.
- Spending on Business Security will increase.
- Industrial hacks will be increased.
- Increase in Cyber-Defence capacities.
- Ransom ware and extortion will increase [5].

V. PRACTICES AND CONCERN BY GOVERNMENT FOR CYBER SECURITY

"As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 44,679, 49,455 and 50,362 cyber security incidents were observed during the year 2014, 2015 and 2016, respectively," Minister of State for Electronics and IT replied to Lok Sabha.

The efforts of Indian Government are also started for the recruitment of Cyber Security experts and partnership with top international Cyber Security Firms[2].

Standardization of Cloud Security:

Full capabilities and potential of cloud services are held by State government, their Cyber Security models will be rigorously transformed. Establishment of Focused Governance Structure: Full capabilities and potential of cloud services are held by State government, their Cyber Security models will be rigorously transformed. each agency should follow three steps namely develop, document, and implementation of its own information security plan should be carried out, which must be approved by the state CISO. Public comment should be made available for the information security plan.[8]

VI. CYBER SECURITY TECHNOLOGIES

Cybercriminal total annual revenue is higher than the drug trafficking.

The top innovative Cyber Security technologies of 2016 and till date are introduced as day by day hackers are getting smarter they are using many other techniques for the violation of data like Man-In-Middle Attack, Memory Scrapling Malware, Bespoke Attack, Spying Software and Google Glass.

Traditional and tool based approaches no longer cut all this threats. Some of the hot technologies are:

1) Context Aware-Behavioural Analytics: Organizations should be aware about the context and examine in which the data has been used i.e. unusual behaviour = nefarious doings.

2) Next Generation Breach Detection: It tells that what will happen if, once the attacker is inside the system instead of focusing on first line of defense. Machine learning and behavioural analytics are combine to detect breaches and trace them [4].

3) Virtual Dispersive Networking (VDN):

Traditional encrypting technologies are cracked by (MiM) attacks and ultimately target the intermediate code. In this message is split into multiple parts, each part is encrypted separately and routes them over servers.

4) Smart Grid Technology:

There are many smart devices which have left vulnerable infrastructure issues in the architecture. In order to avoid this new practical measure and ranges are been implemented.

5) SAML and Cloud:

Many applications are beyond the area of firewall and many other traditional techniques. In order to avoid

this SAML and Intrusion Detection Techniques are combined to control the traffic.

VII. POSSIBLE COUNTER MEASURE TECHNIQUES

Basic Cyber security measures to reduce the exploitable weaknesses and attacks:

Control System Devices should be accurately maintained and eliminate any exposure to external network: No machine or any other control network can communicate directly to other machine or on the Internet.

Implementation of Firewalls and Network Segmentation: With the rise of Internet Of Things many non-Internet connected device such as video camera have been linked to systems and web, so the importance of segmenting have been increased ever.

Security protocols are implemented and number of pathways is reduced then it is very difficult for a threat to enter in the system.

Implementation of System Logging and establishing Role Based Access Controls: By implementation of logging capability it allows for the monitoring of system activity. Establishment of Role-based access control grants limits the ability of users, attackers to the access prone areas.

Maintain Vulnerabilities and implementation of patches and updates:

System of monitoring for and applying system patches and updates should be implemented for the protection of one's organization from attacks and threats.

Developing and enforcing policies on Mobile Devices:

The spread of smart phones and smart devices in the workplace presents notable security challenges. In order to avoid threats and prevent devices from unauthorized access devices should be protected by the passwords .User should be cautious while using one's own device.

VIII. KEY CHALLENGES TO SOCIETY

Every Minute we are seeing about half a million attack attempts that are happening in Cyber Space.

Public and private institutions are the critical infrastructures of our Nation's in the sectors of Government, Defense, Energy, Transportation and finance. Full scale computerization has been opted by many banks for security purpose and due to this it has evolved the concept of e-commerce and e-banking [9].

IX. CONCLUSION AND FUTURE SCOPE

Inherent nature of information technology (IT), results in cyber security issues. Implementation of Cyber Security can be improved by calling two kinds of activities: What is known about improving Cyber Security, develop new knowledge about Cyber security. Focused attention and should be invested adequately for achieving the good degree of cyber security and to prevent one's data and information from the threats. Continuous evolving technology should be tracked globally, as it is a must requirement for Cyber Security. By growing interdependencies among infrastructures, global problems require global solutions, greater efficiency and faster results improves cost-effectiveness too.

It is crucial not only to our national sense of well-being, but also to our national security and economy. Considering the importance of Cyber Security challenges and counter measure techniques have been discussed in future, this will become the fifth utility because it plays major rule in smart city so the future work would focus to explore more control system devices to eliminate the exposure to external network. It will also focus to develop more policies for mobile devices to provide secure communication.

X.REFERENCES

[1] OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k8zq92vdgtl-en

[2] cybersecurity-related-incidents-in-india-during-2016.http://www.bgr.in/news/cert-in-reports-50362-/cybersecurity-related-incidents-in-india-during-2016(Feburary,2016).

[3] Thomas H. Karas and Lori K. Parrott , Judy H. Moore , Metaphors for Cyber Security ,Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839.

[4] Luca Urciuoli, Toni Mannisto, Juha Hinsta and Tamanna Kahn. "Supply Chain Cyber Security— Potential Threats," Information & Security: An International Journal 29, no. 1 (2013): 51–68. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf.

[5] Steven R. Chabinsky "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines," Journal of National Security Law & Policy 4, no. 1 (2010): 27. 30 Trusted Computing Group.FactSheet.2009.http://www.trustedcomputinggroup.org/files/resource_files/7f38fa361d093519add14cb3d28efea6/fact%20sheet%20May202009.pdf

[6] Symantec, 2015 Internet Security Threat Report,7(Apr.2015),FL.Retrieved from http://know.symantec.com/LP=1123.

[7] David E. Sanger and Nicole Perlroth, Bank Hackers Steal Millions via Malware, International New York Times (Feb. 14, 2015) (noting that, since late 2013, an unknown group of hackers has reportedly stolen $300 million -and possibly as much as triple that amount - from banks across the world), FL. Retrieved from http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

[8] Promoting Private Sector Cybersecurity Information Sharing,Exec.Order No.13691(Feb. 20, 2015),80 Fed.Reg.9349,FL. Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[9] Integrated Defense Staff,"National Informatics Center",Ministry of Defense,India.

[10] whereareweoncybersecurityinindia.https://securityintelligence.com/whereareweoncybersecurity-in-india (November, 2016).

[11] http://im.rediff.com/money/2016/jun/02graph4.jpg