JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Impact of Cyber Security and Cyber Crime

Submitted by :-

Arupjyoti Das

IN

BUSINESS ANALYTICS

SCHOOL OF BUSINESS

Under the Supervision of

Ms Rashi Mittal

Professor school of Business

SCHOOL OF BUSINESS

Abstract

The usage of cyber security aids in protecting a variety of online data that is vulnerable to theft from many types of criminals, including malicious software, hackers, and viruses. External risks that can seriously harm a person or an organisation must be protected from access to this information. All people and organisations are shielded from these risks of intimidation and cybercrime thanks to cyber security. In order to protect their sensitive information, including employee information, product-related information, and confidential data, many organisations and businesses hire professional cyber security experts. These organisations and businesses are often afraid of these crimes and are extremely hesitant to take any risks given the vast amount of data they maintain. The issues that current hackers present to cyber security are the main topic of this paper. The most recent developments that are altering the nature of cybercrime are likewise covered, along with how cyber security is addressing these fresh dangers.

Introduction

Everyone now lives in a contemporary, technologically advanced world where a variety of electronic devices, software programmes, mobile networks, and other technological advancements play a significant role in our daily lives. For their daily operations, several commercial entities, including the banking system, the healthcare system, institutions, and many other businesses, use the internet extensively. Everyone spends the majority of their time online, making it the platform with the quickest growth in today's globe. Bank statements, personal information, and financial data, among other highly valuable data, might be sensitive and exposed to hackers, which could have a detrimental effect on the organisations. Today around 60 percent of total commercial are done through the use of internet and that’s why high quality of security is required in this field to protect the information available throughout the internet. This informations gives the invader to use the exposed data and bring threat to popular public figures, politicians, businessman etc. cyberattack has become a global international threat which we have to deal in daily basis where hackers breach protocols and goes to our system and take out all the data we need. Cyber security is bringing new techniques to deal with these challenges to keep our internet journey safe. The fight against this cyber criminals are our own individual fight too and that’s why we also need to know some basic elements of cyber security to keep our information safe. Many governments are making strict laws to keep our valuable informations protected and to stop the ongoing channel of cybercrimes in large scale.

Objective

Keeping data from being stolen by hackers is the goal of cyber security. Information protection is the main objective of cyber security. The security industry presents a triangle of three interconnected concepts to defend data from cyber-attacks. This idea goes by the moniker "the CIA trio." The goal of the CIA model is to assist organisations in formulating their information security architecture policies. When a security breach is found, at least one of these guidelines has been violated. The CIA model consists of three elements: confidentiality, integrity, and availability. People can follow this security paradigm as they navigate various facets of IT security. A safe national cyber network is often built as a result of cyber security. It creates a framework for design of security policies to strengthen and secure the cyberspace ecosystem.

ASSUMPTIONS

During the course of this study, I discovered the following assumptions about cyber security:

1. Employees will be able to recognise phishing assaults with ease, but in practise, they are often unable to do so.

2. The workforce needs to receive cyber security education from firms. Every week, 40% of workers fall for an email posing as coming from a member of their company, and 50% of workers still open attachments from unknown sources.

3. When it comes to connecting with users and assisting them in consistently making the proper security decisions, you and your IT staff must embrace new-school security awareness training.

4. People click on unidentified links that include viruses and malware that can hack any account or obtain all of your personal information in a matter of minutes by sending data to the hacker's source.

5. Different people and criminal hacking groups continue to commit cybercrimes on a regular basis, so we should learn some fundamental security measures to protect ourselves.

Review of Literature

Having knowledge about cyber attacks and cyber crimes is the first step of protection. Training about cyber crimes and cyber security is really essential in this generation. Cybersecurity professionals improve understanding of the latest cyber attacks and train normal persons to increase skill levels in defending and mitigating against them. The aim of this paper is to research the idea of a cyber range, and to include a full fledged analysis of literature covering unclassified cyber attacks that are developed newly by modern day hackers. In this review, we analyse existing literature that focuses on architecture and scenarios, but also capacities, functions, resources etc. In this paper the risks and future approaches are analysed and are focused on forms of cyber threats that are Included as an in depth analysis of the cyber-security environment. In particular, we concentrate on observing and analysing vulnerabilities in the network, challenging the malware's and required protection needed. The paper provides a deep knowledge about cybersecurity vulnerabilities and solutions, and provide a map to future cybersecurity researches.

In order to address the issues linked to cybercrimes in daily life, a cyber security control model is constructed in this study. To describe and pinpoint information security controls that are prone to error, a quantitative technique is developed. It has been confirmed that the constructed model might supply necessary knowledge about cyberattacks and how to handle those in our daily life. The emphasis of this paper is on the value of various cyber security framework architectures and cyber defence units. Threats to security, criminal activity, and cyber security are covered. We talk about numerous government initiatives to safeguard cyber security as well as the national information security policy.

How cyber attack affect us -

There are huge No of cyber attacks daily in India .Maharashtra was the most targeted state in India — facing 45% of all ransomware attacks. India is one of the most profitable regions for hacking groups and then this hackers ask Indian firms to pay a ransom through cryptocurrencies in order to regain access to their valuable data. One in five Indian organisations suffered a ransomware attack in 2021 where they used to ask for payment through cryptocurrencies so their address can't be detected by the cyber security officials in an easy way. Alongside India, US is just one of the countries that have invested huge amounts of money in developing not only their defence but also the ability to tackle high level of cyber attacks. United States, China, Russia, Israel, and the United Kingdom are the nations with the most advanced cyberwarfare technologies. According to data provided and maintained by the Indian Computer Emergency Response Team, 6.86 lakh cyber security events were nonetheless reported in the first half of 2020, roughly equal to the preceding four years put together. In order to attack India's electricity sector, a Chinese company by the name of Red Echo has dramatically increased the usage of tools like malware.Using a backdoor to access Indian systems, the virus named Shadow Pad, which was employed by red Echo, was used. A municipal, state, or federal government stores a substantial amount of private information about the nation and its residents, which hackers target in an effort to access the data and use it for their own gain.

Hackers prey on people by accessing the photos, videos, and other private information they disclose on social networking sites, which makes them vulnerable to serious and even fatal acciintegrit

The Companies' systems are filled with a wealth of data and information. A cyber attack by any organisation could result in the loss of proprietary information (such patents or original work), customer or employee data loss, and the total erosion of public confidence in the organization's integrity.

How to prevent cyber attack-

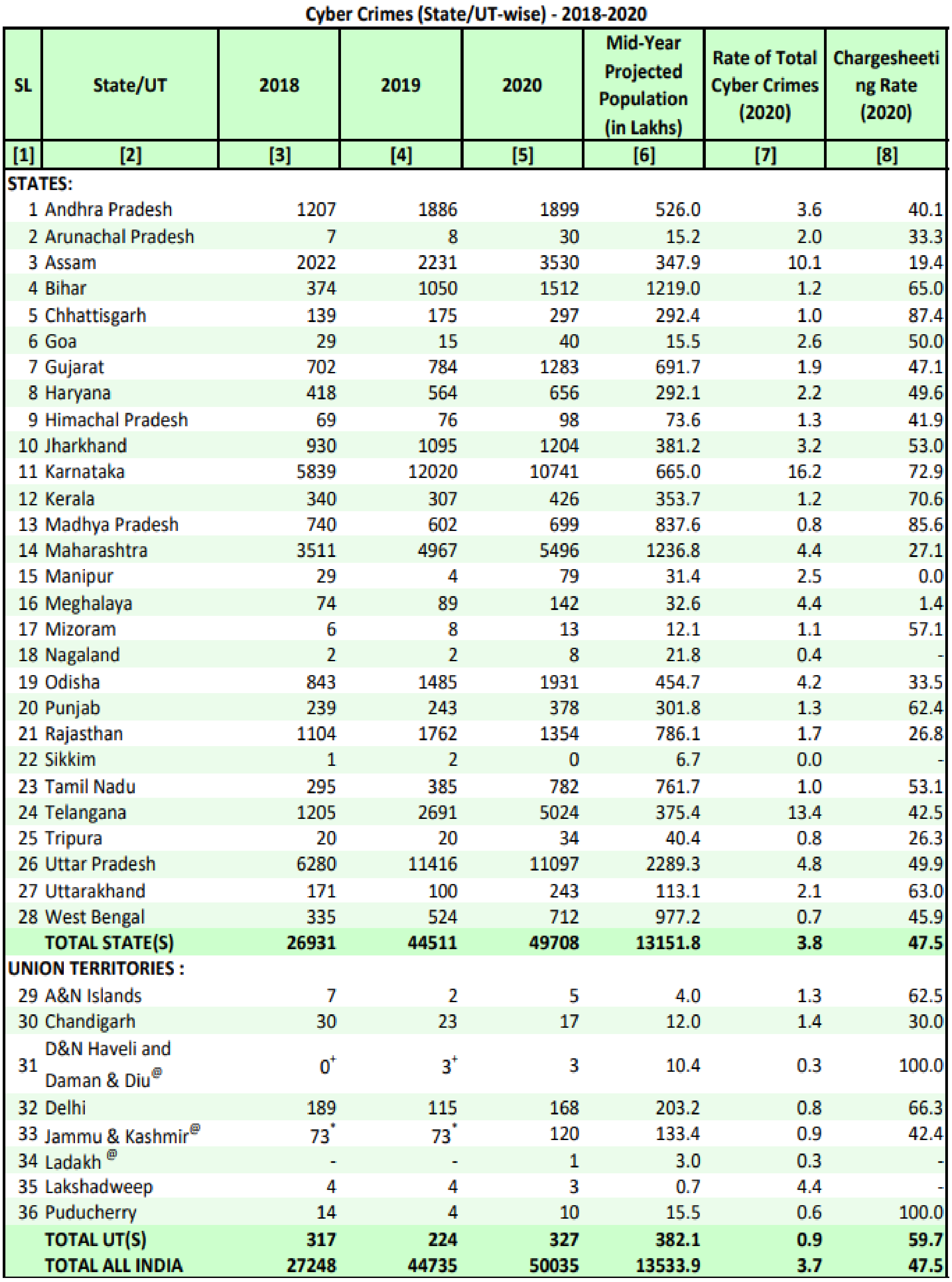
Knowing the various kinds of protocols, exploits, and resources that hackers utilise will help you defend against cyberattacks. In order to safeguard our systems from assaults, we must become aware of where and how to anticipate attacks so that we can take preventive action. To prevent the device from being exploited to exploit a vulnerability or valuable information, the proper countermeasure for each attack must be employed. In order to protect our devices from threats like social engineering, email spam filtering, network firewalls, vulnerability scanning, penetration testing, and risk management, it's crucial to establish security policies.

The security risk management method detects, evaluates, and checks vulnerabilities that influence various information assets (i.e., systems, hardware, applications, and data), and then filters the numerous hazards that could effect those vulnerabilities. The main goal of a risk assessment is to tell the user about weaknesses in business systems so they may take quick defensive measures and plan efficient risk responses. Additionally, it offers a thorough summary to assist executives in making informed choices regarding ongoing security issues. Additionally, other helpful techniques, such as setting up a powerful new generation firewall, would guard against numerous high-level cyberattacks brought on by hackers. The security of the network perimeter must be ensured while establishing any firewall, which requires keeping in mind a specific set of policies and rules. The network's many firewalls can also be subjected to these restrictions in the future, which will help the device's security. To stop the effects of hacker virus attacks, many antivirus programmes can also be installed. To combat viral attacks by hackers who can send them through email links or other covert channels, people should do routine virus scans.

Methodology

The study employs both secondary and primary data. To comprehend cybercrimes that have occurred in recent years and to undertake analysis, we have looked at previous studies, publications, and news that is available online. Additionally, information was gathered from a variety of books, journals, and websites on the internet that included secondary data and supporting documentation. Additionally, a number of case studies and surveys about online cybercrimes were studied. After using all of the techniques, raw data is treated.

Data interpretation and analysis-



Cyber Crimes (State/UT-wise) - 2018-2020

SL	State/UT	2018	2019	2020	Mid-Year Projected Population (in Lakhs)	Rate of Total Cyber Crimes (2020)	Chargesheeting Rate (2020)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
STATES:							
1	Andhra Pradesh	1207	1886	1899	526.0	3.6	40.1
2	Arunachal Pradesh	7	8	30	15.2	2.0	33.3
3	Assam	2022	2231	3530	347.9	10.1	19.4
4	Bihar	374	1050	1512	1219.0	1.2	65.0
5	Chhattisgarh	139	175	297	292.4	1.0	87.4
6	Goa	29	15	40	15.5	2.6	50.0
7	Gujarat	702	784	1283	691.7	1.9	47.1
8	Haryana	418	564	656	292.1	2.2	49.6
9	Himachal Pradesh	69	76	98	73.6	1.3	41.9
10	Jharkhand	930	1095	1204	381.2	3.2	53.0
11	Karnataka	5839	12020	10741	665.0	16.2	72.9
12	Kerala	340	307	426	353.7	1.2	70.6
13	Madhya Pradesh	740	602	699	837.6	0.8	85.6
14	Maharashtra	3511	4967	5496	1236.8	4.4	27.1
15	Manipur	29	4	79	31.4	2.5	0.0
16	Meghalaya	74	89	142	32.6	4.4	1.4
17	Mizoram	6	8	13	12.1	1.1	57.1
18	Nagaland	2	2	8	21.8	0.4	-
19	Odisha	843	1485	1931	454.7	4.2	33.5
20	Punjab	239	243	378	301.8	1.3	62.4
21	Rajasthan	1104	1762	1354	786.1	1.7	26.8
22	Sikkim	1	2	0	6.7	0.0	-
23	Tamil Nadu	295	385	782	761.7	1.0	53.1
24	Telangana	1205	2691	5024	375.4	13.4	42.5
25	Tripura	20	20	34	40.4	0.8	26.3
26	Uttar Pradesh	6280	11416	11097	2289.3	4.8	49.9
27	Uttarakhand	171	100	243	113.1	2.1	63.0
28	West Bengal	335	524	712	977.2	0.7	45.9
	TOTAL STATE(S)	**26931**	**44511**	**49708**	**13151.8**	**3.8**	**47.5**
UNION TERRITORIES :							
29	A&N Islands	7	2	5	4.0	1.3	62.5
30	Chandigarh	30	23	17	12.0	1.4	30.0
31	D&N Haveli and Daman & Diu$^{@}$	0^{+}	3^{+}	3	10.4	0.3	100.0
32	Delhi	189	115	168	203.2	0.8	66.3
33	Jammu & Kashmir$^{@}$	73^{*}	73^{*}	120	133.4	0.9	42.4
34	Ladakh $^{@}$	-	-	1	3.0	0.3	-
35	Lakshadweep	4	4	3	0.7	4.4	-
36	Puducherry	14	4	10	15.5	0.6	100.0
	TOTAL UT(S)	**317**	**224**	**327**	**382.1**	**0.9**	**59.7**
	TOTAL ALL INDIA	**27248**	**44735**	**50035**	**13533.9**	**3.7**	**47.5**

Conclusion

The cybercrime has serious repercussions for national and economic security, this report says. It is brutal, pervasive, all-pervasive, and getting more sophisticated. The need for a cyber-security function in all of its components is essential for future growth, innovation, and competitive advantage. There are substantial hazards for many industrial agencies, public and private organisations for businesses and governments alike. Each year, there are new ways that cybercrime and data security continue to remain distinct from one another. The most recent and tumultuous advances, combined with developing cyber tactics and ongoing attacks, are challenging organisations that not only need to secure their infrastructure but also require new channels and intelligence. To reduce cybercrime, however, is a task we must all take on if we are to live in cyber-houses in a safe and secure future. As significant study areas for the twenty-first century, the technologies of a reliable Internet and effective systems have been suggested.

References

1)Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518. 2)Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

3)Mellado, D,Mouratidis, H,Fernández-Medina, E. Secure Tropos Framework for Software Product Lines Requirements Engineering. Comput. Stand. Interfaces 2014, 36, 711–722

4) VeenooUpadhyay, SuryakantYadav Study of Cyber Security

5) A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems

6)Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand

6)Wikipedia

7)Internet