Major Hurdles of Cyber Security in 21st Century

Deepak D M, Bhavin Kumar S, Dayanand Lal

***Abstract:** A digital assault is an attack propelled by cybercriminals utilizing at least one PCs against a solitary or numerous PCs or systems. A digital assault can perniciously handicap PCs, take information, or utilize a ruptured PC as a dispatch point for different assaults. Cybercriminals utilize an assortment of strategies, including malware, phishing, ransomware, refusal of administration, among different techniques. Albeit most government offices and significant enterprises have completely sent individual devices as data safety efforts, focuses of assaults have extended to incorporate, other than government foundations, basic frameworks and explicit ventures and partnerships, calling for increasingly powerful counter measures. In this paper we have discussed about Cyber Attack and its types, its initiated and a major cyber-attacks in 21st century.*

***Keywords :** Confidentiality, Cyber-Attack, , DoS, ,Phishing.*

I. INTRODUCTION

One of the greatest data security dangers numerous associations are confronting is the uncontrolled use of convenient stockpiling gadgets by their workers . Besides, the weakest connection in the corporate data security is the pernicious insider and guileless representative who may effectively succumb to social designing assaults. Besides, cybercrimes are expanding worldwide and they bargain the three most significant parts of data security i.e., Confidentiality, Integrity and Availability (CIA) . Digital security has consistently been a specialty field, with just digital network knowing the significance of shielding itself from digital dangers; be that as it may, the present increments in cybercrime influencing end clients have changed this discernment. The expanding number of cybercrimes and the danger of digital fighting and potentially digital psychological oppression have prompted expanding interest and worries from governments identified with their improving digital security act and their digital protection capacities. This move in the digital condition has rejuvenated the digital security industry; expanding number of individuals, (both beginner and expert), taking an interest in the digital security network, has additionally prompted more investigation into safeguard and fighting techniques and innovations. People, organizations and governments are spending noteworthy measures of cash so as to secure their computerized resources and assets against cybercrimes, for example, coercion, protection infringement, burglary of secret data and harm to their notorieties . Complete security is absurd and now and again not by any means down to earth. Associations recognize vulnerabilities and dangers related with their assets and create strategies on the most proficient method to deal with these viably. The measurements distributed in show that aggressors are presently misusing the speed, comfort and obscurity of the Web to carry out more wrongdoings, quicker and all the more adequately. There are a few sorts of cybercrimes, for example, money related wrongdoings and different kinds of coercion/misuse , which are done utilizing botnets, bespoke malware, organize interruptions, phishing, disavowal of Service (DoS), and data robbery.

Revised Manuscript Received on February 05, 2020.
***** Correspondence Author

Deepak D M, CSE Department, GITAM School of Technology, Bangalore, India. Email: deepak.manjunath@gitam.edu

Bhavin Kumar S, CSE Department, GITAM School of Technology, Bangalore, India.. Email: bhavin.kumar@gitam.edu

Dr.Dayanand Lal, CSE Department, GITAM School of Technology, Bangalore, India. Email: dayanandlal.narayan@gitam.edu

II. WHAT ARE CYBER-ATTACKS?

A Cyber Attack is characterized as an assault began by an advanced framework against another computerized gadget, site, or some other computerized framework and bargains its security, unwavering quality or the information put away in it.

Why are Cyber Attacks Initiated?

- Procuring unapproved access to an advanced system, framework or its information.
- Forswearing of administration
- Infection or malware establishment
- Hacking a site for spontaneous purposes
- To gain admittance to individual and secure data of individuals and organizations
- Unapproved utilization of a computer.

III. LITERATURE REVIEW

Now a days there will be more and more cyber-attack is happening ,it affects to banking sector, IT sector even for common people also suffering a lot. In newspapers news related to cyber-attack news is common in every day.

Mohamad Syahir Abdullah et al[1], proposed a system to identify cyber-attack news by using Natural Language Processing(NLP). NLP includes tokenization, stemming, removal of stop words ,word clod, Document Term Matrix

- **Tokenization**- breaking down sentence into unigram and bigram.
- **Stemming-** Keeping only root words. Ex: looking-> Look, Standing->Stand etc.
- **Stop words**: Removing of stop words like is, as, it, at, was etc.

- **Word cloud:** Display the positive and negative word cloud.
- **Document Term matrix**- It count the frequency of each and every word.

This scheme also uses a Conditional Random Field(CRF) and Latent Semantic Analysis(LSA) for further analysis.

Yanpeng Guan et al[2], proposed a . Distributed Attack Detection system it identifies the joint distributed attack detection and distributed secure estimation for a networked cyber-physical system under physical and cyber-attacks. This system contains models like notations, system dynamics under false data injection attack ,communication topology. In order to identifies the false data injection attack proposed system uses a two-step attack detection mechanism has been established through which the occurrence of the FDI attack can be detected and alarmed. To tackle the random jamming attacks, a refined measurement output model based on compensated measurements has been proposed and resilient estimators have been delicately constructed.

Harjinder Singh Lallie et al[3], proposed a system that uses Attack modelling Techniques(AMTs) to understanding and perceiving cyber-attacks. This system got the results of an empirical evaluation between an the fault tree standard and adapted attack graph method and to determine which one is more effective in aiding cyber-attack perception. The results show that the adapted attack graph method is more effective at aiding cyber-attack perception when compared with the fault tree method ($p < 0.01$). This proposed system has some limitations 1. The results of aag method is statistically not satisfied and still requires larger study to get proper results. 2. The proposed system also requires more time to plot graphs and comparing with results. 3. This method is not applicable for complex cyber-attacks like Stuxnet virus, Jeep Cherokee Hack, Sony Hack.

Gaoqi Liang et al[4], proposed a cyber-Topology attacks models which focuses on three types cyber-topology attacks like 1.line-addition attack 2. Line-removal attack 3. Line-switching attack which usually disturbing the power systems operations. The proposed system uses optimal attack models , metaheuristic optimization algorithm and natural aggregation algorithm to solve cyber-topology problems. This proposed system consists models like 1. **SCED**(security-constrained economic dispatch) model which optimally dispatches generators and determines LMPs of the wholesale energy market. 2**.Deviation of variables** that were using for before and after attack. 3. **Different Attack Scenarios** model which uses different scenario for finding different attack. 4. **Cyber-Topology Attack Modelling** uses different cyber-attack topologies for protecting against line-addition attack, line removal attack and line-switching attack.

Limitations: Suppose if attacker hides for a periods while launching cyber-attack this method can't applicable.

Noora Alallaq et al[5], proposed a Latent Dirichlet Allocation (LDA) Group Topic Author model and Astroturfing Group Topic Detection (AGTD) algorithm for discovering astroturfing groups with in tourism domain. Astroturfing group which creates fake messages ,fake news in favour or against some services or organization or products which misleads the customers. Latent Tourism Astroturfing Group Detection(LTAGD) model uses unsupervised method for discovering Astroturfing news and reviews accurately and this model also built a prototype application for showing efficiency.

ShengyeWan et al[6], proposed an anti-crawler mechanism called PathMarker model for protecting web information from inside crawlers. Web crawlers usually inject malicious data to server and they will download the contents from server without any permission from the website administrator. Malicious crawlers have different downloading speed and have long term and short term behaviour. By adding pathmarker to an end of each URL(Uniform resource location) we can trace the behaviour of each webpage and also we can identify users who can access webpages. This proposed system also uses support vector machine to differentiate between web-clawers and normal users . Pathmarker detects more than 6 popular web crawlers with high accuracy including google and yahoo.

AhmetOkutan et al[7], proposed a model called ASSERT(attack synthesis and separation with entropy redistribution towards predictive cyber defence) which continuously analyse and separates models which shows cyber-attack behaviour. This model helps to overcome the problem of predictive defence beyond intrusion detection, where attackers will do malicious actions by analysing different attack strategies and finding their weakness'. ASSERT contains models like Dynamic Bayesian classifier(DBC), dynamic model Generation(DMG), Kallback-leibler Divergence(KLD), Cluster validity Index(WGI). The cyber-attack details get from the ASSERT model further used for training the machine learning models which intern helps for predict the cyber-attack behaviour in future.

IV. TYPES OF CYBER ATTACKS

1. **MALWARE**:-Malware is considered as programming that is purposefully created to upset PC, server, customer, or PC organize. Malware can be as contents, executable codes, dynamic
substance, and different vindictive programming.
these codes can be PC worms, infections, ransomware, Trojan ponies, adware, spyware, or scareware. Malware, as the name recommends, is planned with a malignant purpose to make harm the site/PC client.

2. **PHISHING:-** The principle point of Phishing is to take limited and private data, for example, Mastercard subtleties, login ids, and passwords, and so on. By mimicking oneself as a solid foundation in electronic correspondence. It is typically done through email ridiculing or texting. They convey a connection that guides clients to a phony site which appears to be like the genuine site and requests that they enter individual and secure data. It is a

fake movement proposed to swindle clients. They snare the clients by professing to be from a dependable third gathering, for example, sell off destinations, online installment processors, social sites, banks, or IT managers. You should be very much aware and recognized with such deceitful exercises to sidestep any such misrepresentation exercises.

3. **Man-In-The-Middle Attack:-** In Man-in-the-center (MitM) the trespasser clandestinely changes the talks and exchanges between two individuals who are speaking with one another. In a Man-in-the-center assault, the communicators are made to accept that they are legitimately speaking with one another with no impedance from any outsider. In any case, in all actuality the entire correspondence is constrained by the trespasser while causing the communicators to accept that they are conversing with one another. It is otherwise called listening stealthily.

4. **Denial-of-service Attack:-** Willfully ignorant of-administration assault (DoS assault) the wrongdoer attempts to make computerized resources out of reach to its foreseen clients. The guilty party temporarily intrudes on administrations of a host who is connected to the Internet. It includes flooding the blockaded machine with surplus applications to trouble it from satisfying the authentic solicitations.

5. **SQL Injection Attack:-** A Structured Query Language (SQL) injection attack allows the intruders to run malicious SQL statements. These SQL statements have the power to take over the database server. Using SQL injection intruders can overcome application security measures. It allows them to pass through the validation and approval process of any web application. It also allows them to recover the entire data from their database. It also gives access to intruders to add, modify, and delete data in the database. An SQL Injection allows intruders to fiddle with various databases including MySQL, Oracle, SQL Server, or others.

6. **Zero-Day Attack:-** The zero-day defense lessness is a deformity in the product, equipment or even the firmware. It is escaped the groups liable for fixing this bug. It is alluded to as zero-day as it has a multi day time hole between the time it is distinguished and the principal assault.

7. **Cross-Site Scripting:-** In Cross-Site Scripting (XSS) assaults the malignant contents are installed to dependable sites. The gatecrashers send malignant code to various clients by installing them into a confided in site generally as a program side content. The internet browser can't perceive this malignant content and has no clue that it is inconsistent, and thus it executes the content as it originates from a confided in source. Yet, oh these malevolent contents have forces to get to any session tokens, treats, or whatever other mystery data that is utilized by that site.

8. **Credential Reuse Attack:-** With pretty much every close to home record requesting Ids and passwords, we will in general reuse them for different records. In spite of the fact that it is a major NO, we will in general reuse one id and secret word for some records. Reusing a similar secret word can be a major risk to your security. The gatecrashers can take your usernames and passwords from a hacked site and they get an opportunity to sign in to your other record utilizing a similar id n passwords. What's more, on the off chance that you have reused them they get a brilliant chance to look into your private records including your financial balance, email, your internet based life accounts, and numerous others. What's more, we truly don't have to reveal to you how unsafe it could be! So pursue secret word security best practices and abstain from utilizing a similar id and secret phrase for various records. You can utilize Password administrators to deal with the different IDs you use.

9. **Password Attack:-** Passwords are the principle passages to safely go into your own records. Gaining admittance to these passwords is a well established and most advantageous approach to barge in into somebody's private account. Our passwords are normally associated with our life's occurrences, individuals and spots and programmers take advantage of such subtleties. They can even sniff into the system to access decoded passwords. The assailants duplicate scrambled record having the rundown of passwords, and use it to a word reference of often utilized passwords. They at that point contrast the outcomes with grab hold of the client's secret phrase. The record lockout arrangement is the best strategy to avoid such
dangers as it bolts your record after a couple of wrong endeavors and consequently verifying your records.

10. **Drive-By Download Attack:-** Drive-by – download assault is a typical technique utilized by programmers to spread malignant contents or codes on client's frameworks. Assailants install a pernicious content into an uncertain site's pages. At whatever point you visit such sites, the contents will consequently introduce on your framework or might divert you to a site that is constrained by the aggressor. These assaults can happen by visiting a site, a spring up window or an email message. Drive-by downloads don't require clients contribution to get initiated. It doesn't expect you to download/open any malevolent connection. It utilizes a working framework/internet browser with deficient security highlights.

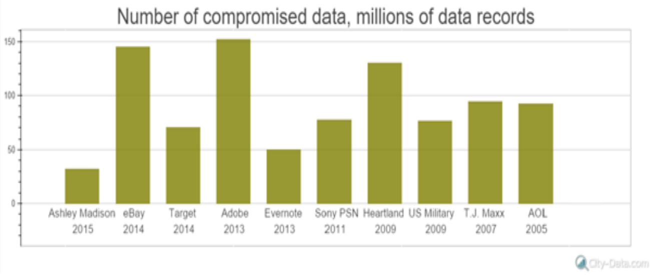
V. MAJOR CYBER-ATTACKS OF 21ST CENTURY

Presently when we have found out about different kinds of digital assaults and we make certain about their appalling presence. Digital assault can happen to any computerized client whenever and at wherever. Some may be innocuous or might cause only a little harm.
In any case, there are a couple of sorts of digital assaults that

had caused noteworthy harm and had taken passage in the rundown of most critical digital assaults.

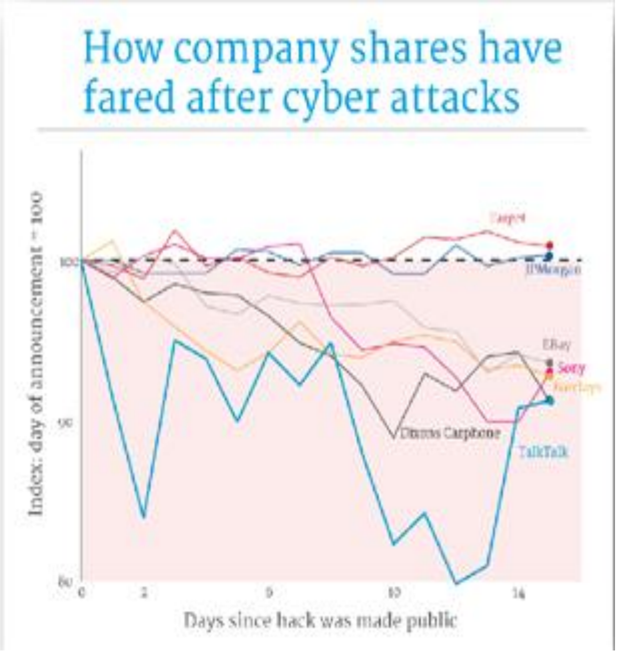
i. Cyber Attack on Yahoo

One of the most noticeable web monster, Yahoo endured a major blow when the security of their 3 billion client accounts was put on stake. The names, dates of birth, email addresses, passwords just as security questions and replies of 3 billion clients were put on stake. The assault occurred in 2013-2014. The assault had seriously influenced the organization; the Yahoo bunch that was once esteemed at $100 billion was at last auctions off to Verizon for just $4.48 billion for its center Internet business. The name of the organization was later changed to Altaba, Inc. after the deal.



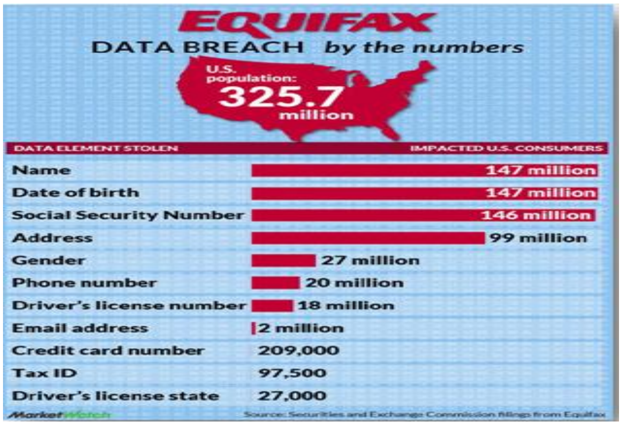
ii. eBay Cyber Attack

Another digital assault that shook the whole world was the client's database hacking by the gatecrashers. The online business monster was exposed to a significant digital assault in May 2014 when programmers meddled into the client's database utilizing their corporate worker's records. The programmers had total access into their system for around 229 days. The rupture traded off the touchy data like names, dates of birth, addresses, and scrambled passwords of around 145 million clients. However, according to the organization, the money related information of the clients was sheltered at it was put away in a different database and was not bargained. The sea shore brought about across the board analysis of the organization and acquired incredible loses.



iii. Equifax Cyber Attack

Equifax one of the US biggest credit agencies, confronted a significant blow when the information of its 143 million costumers was hacked. The client's touchy data including birth dates, Standardized savings Numbers, locations, and drivers' permit numbers was hacked by the interlopers. The assault didn't end with hacking just the individual data, even the charge card data of around 209,000 buyers was taken as well. As indicated by the organization, the application defenselessness on their site brought about the information assault. The assault was uncovered on July 29, 2017, however was suspected to have begun in mid-May that year.



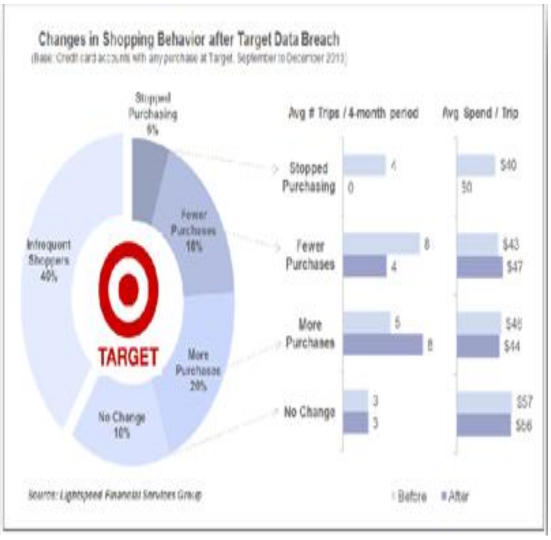
DATA ELEMENT STOLEN	IMPACTED U.S. CONSUMERS
Name	147 million
Date of birth	147 million
Social Security Number	146 million
Address	99 million
Gender	27 million
Phone number	20 million
Driver's license number	18 million
Email address	2 million
Credit card number	209,000
Tax ID	97,500
Driver's license state	27,000

MarketWatch

Source: Securities and Exchange Commission filings from Equifax

iv. Target Stores Data Breach

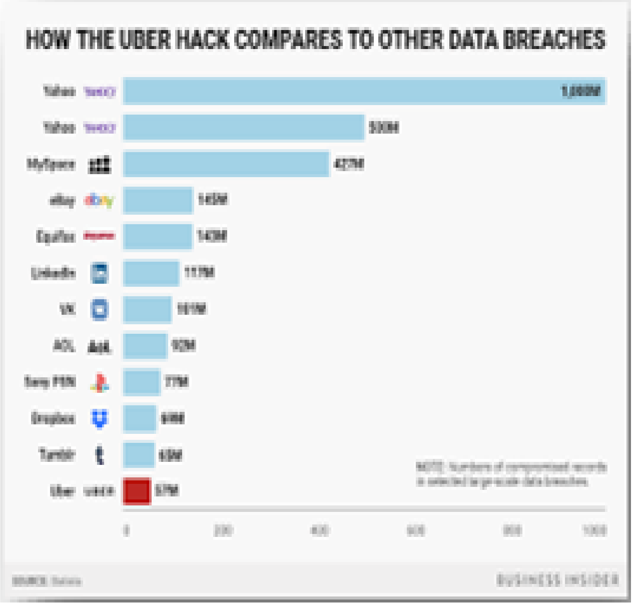
End of December 2013 gave a major hit to Target stores when they found that an information rupture into their framework had undermined the Credit/platinum card subtleties and additionally contact data of around 110 million individuals. The programmers infiltrated into their private system by abusing their powerlessness through an outsider merchant for air conditioning framework to POS installment card perusers. The digital assault cost them around $162 million. The Chief and CIO of the organization needed to leave after this major digital security issue.



Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

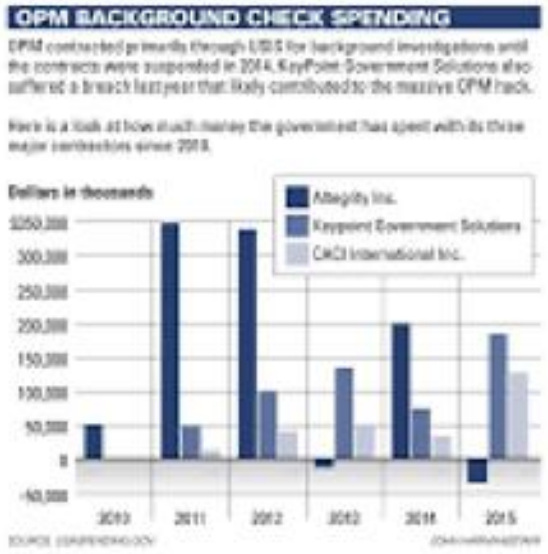
v. Uber Cyber-Security Breach

Information ruptures are basic occasions in the current advanced world. How the organizations manage it, likewise assume a similarly significant job. Uber was exposed to an information break in late 2016. The organization was very little reprimanded as its interpretation of this assault might have been. The break brought about trading off names, cell phone numbers and email locations of 57 million Uber clients and 600,000 Uber's driver permit numbers. The organization found of the break in late 2016 yet made it open practically following a year. Not just that the organization offered the programmers a measure of gigantic $100,000 to obliterate the information without confirming they really did. The break had brought about the loss of both the notoriety and accounts of the organization. The organization was in arrangement to offer its stakes to Softbank, at the time the rupture was reported. The break brought down the estimation of the arrangement from $68 billion to $48 billion.



vi. US Office of Personal Management-The OPM data breach

USA was taken off when the Chinese programmer interfered into their OPM through an outsider temporary worker. The assault began in 2012 however was found distinctly on Walk 20, 2014. A subsequent programmer again hacked into their OPM framework in May 2014 however was found simply after just about a year. The assailants hacked the delicate data including exceptional status information and unique finger impression data of more than 22 million present and past government laborers.



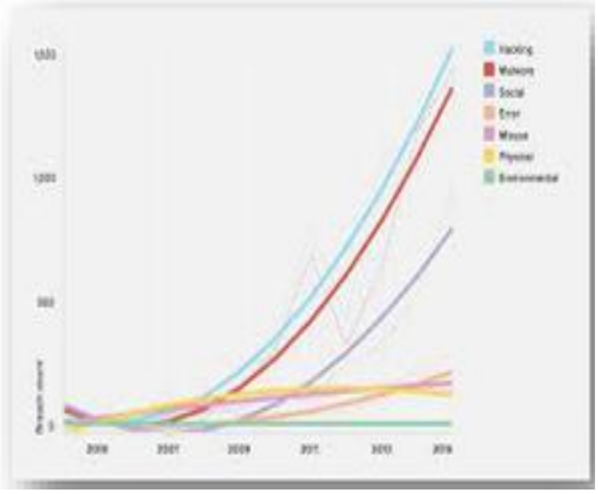
vii. Cyber Attack on Sony PlayStation Network

Perhaps the greatest datum breaks in the gaming business of all occasions occurred on the Sony PlayStation System. April 20, 2011, is a date that will consistently be recalled in the gaming business for the greatest information rupture in the gaming business. The programmers hacked 77 million System accounts. These records had 12 million records that had decoded charge card numbers. The programmers hacked complete names, messages, Visa numbers, passwords, buy history, PSN/Qriocity logins and passwords, and street numbers. Sony acquired misfortunes of a gauge of $171 million. It brought about an underlying $15 million repayment in a claim over the break.

viii RSA Security Attack

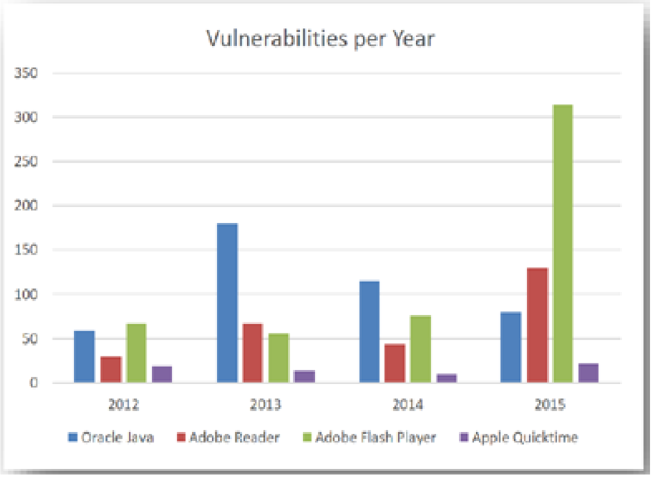
Walk 2011, is a date that is still in banters for the digital security break of the powerful security mammoth's SecurID confirmation tokens of the organization RSA. The programmers effectively figured out how to perform phishing assault on RSA workers and imitated as people and meddled into the system of the organization. The assault is evaluated to have taken 40 million worker records.

DOI: 10.35940/ijeat.C5135.029320



ix Adobe Cyber Attack

Another enormous digital assault that shook the IT mammoth Adobe occurred in October 2013. The assault bargained the individual data including client names, IDs, passwords and charge and Mastercard data of more than 38 million clients. The organization paid $1 million as legitimate charges to determine privileges of disregarding the Client Records Act and one-sided strategic approaches. At the point when advertise biggies like Yippee, eBay, Equifax, and so forth can get caught in the snare of digital assaults, you also can! So know and pursue all digital security wellbeing measures strictly and BE Protected!



VI. RESPONSE ON CYBER ATTACK

Considerably in the wake of playing it safe digital assaults can thump your computerized entryways. In such cases your underlying reactions ought to be:

i. It the assault genuine or only a trick.
ii. In the event that you can get to your information; take a reinforcement.
iii. Whenever required methodology legitimate specialists
iv. In the event that representatives abuse their privileges take fitting activities.

VII. PREVENTION ON CYBER ATTACK

In spite of the fact that there is no assurance to suspend digital assaults totally, you can play it safe as you can to maintain a strategic distance from them. A portion of the means you can pursue to shield you are:

i. Utilize a decent enemy of infection that can identify different malware and can prevent them from getting inside your framework.
ii. Utilize a decent firewall. Utilize a decent quality outsider firewall separated from your default firewall.
iii. In a corporate PC arrange, guarantee that no Connect and Play is bolstered any framework.
iv. Corporates should utilize great system traffic analyzer to follow any odd use conduct from any framework.
v. To shield yourself from DDoS assaults, relieve your site to various servers and far and away superior to utilize cloud administration.

VIII. RESULTS

Year	Company Name	Loss of Data	Loss of Money
2011	RSA	40 MILLION	36 MILLION
2013	TARGET STORES	110 BILLION	18.5 MILLION
2013	ADOBE	38 MILLION	2.9 MILLION
2014	E Bay	145 MILLION	233 MILLION
2014	SONY	77 MILLION	15 MILLION
2014	JP MORGAN	76 MILLION	250 MILION
2014	SONY	77 MILLION	15 MILLION
2016	UBER	50 MILLION	148 MILLION
2017	EQUIFAX	143 MILLION	63 MILLION

IX. CONCLUSION

Digital assaults are a miserable truth of the computerized world. Appropriate authoritative rules are currently set down to shield the clients from these dangerous assaults. Digital assaults are considerably more than simply increasing unapproved access to other's frameworks. They can be dangerous. Furthermore, can prompt loss of cash, brand name and can even be a major hit to your honesty. So being a computerized client, it is only for you to think pretty much every one of these kinds of digital assaults and take appropriate measures to stay away from them and make legitimate strides in the event that you are fallen an unfortunate casualty to them

REFERENCES

1. Mohamad Syahir Abdullah et al ," Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News978-1-5386-7541-0/18/2018 IEEE.
2. Yanpeng Guan and Xiaohua Ge , "Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False

Data Injection Attacks and Jamming Attacks ” IEEE transactions on signal and information processing over networks, vol. 4, no. 1, march 2018.

3. Harjinder Singh Lallie Kurt Debattista, and Jay Bal “ An Empirical Evaluation of the Effectiveness of Attack Graphs and Fault Trees in Cyber-Attack Perception “IEEE transactions on information forensics and security vol. 13, no. 5, may 2018.
4. Gaoqi Liang et al“A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios” IEEE transactions on smart grid, vol. 10, no. 2, march 2019.
5. Noora Alallaq et al“ Group topic-author model for efficient discovery of latent social astroturfing groups in tourism domain“ 978-1-5386-7541-0/18/2018 IEEE.
6. Shengyewan yueli and kunsun“Path Marker: protecting web contents against inside crawlers” Wan etal. Cybersecurity (2019) 2:9 https://doi.org/10.1186/s42400-0190023-1
7. Ahmetokutan and Shanchieh jayyang“ASSERT:attack synthesis and separation with entropy redistribution towards predictive cyber defence” okutanandyang Cybersecurity(2019) 2:15 https://doi.org/10.1186/s42400-019-0032-0
8. T. Bonaci, L. Bushnell, and R. Poovendram, “Node capture attacks in wireless sensor networks: A system theoretic approach,” in Proc. 49th IEEE Conf. Decision Control, Atlanta, GA, USA, Dec. 2010, pp. 6765–6772.
9. A. J. Wood and B. F. Wollenberg, Power Generation, Operation, and Control. New York, NY, USA: Wiley, 2012.
10. H. J. Carey and M. Manic, “HTML Web Content Extraction Using Paragraph Tags,” pp. 1099–1105, 2016

AUTHORS PROFILE

Mr. Deepak. D. M, Assistant Professor in CSE Department, GITAM School of Technology, Bengaluru Campus. He has published a two research papers Titled on “By-Passing Contaminated Hubs What’s More Anomalies in Remote Sensor Networks” and “A Cloud Computing Security Solution” in IJSRD and IJERT with ISSN 2321—0613,ISSN 2278-0181 on 2015 and 2016.The Research interest are Cyber Security and Big Data.

Mr. Bhavin Kumar S, Assistant Professor in CSE Department, GITAM School of Technology, Bengaluru Campus. He has published two research papers Titled on “Identifying and Ranking Prevalent News Topics Using Social Media Factors” and “An Exploratory Analysis of Customer Reviews using Natural Language Processing” in UGC approved International Journal of Research and Analytical Reviews(IJRAR) with E - ISSN 2348 –1269, ISSN 2349 -5138 on May 17th 2019. The Research interest are Artificial Intelligence and Cyber Security.

Dr.Dayanand Lal.N Assistant Professor in CSE Department, GITAM School of Technology, Bengaluru campus. He has published three research papers “Porting presentation Layer to ensure network security in mobile devices”, “configuring a secure wireless network using GNS3” and “Protective and Efficacious cloud evaluating Schema” in Scopus journals. The Research interest area is Cyber Security.