Cyber attacks & Its Security Predictions in 2020

– Sachin Kumar
Research Executive, Scholastic Seed Inc., New Delhi
https://orcid.org/0000-0002-1540-5989 ksack123@outlook.com

Article History
Paper Nomenclature: Scrutiny Tip (ST)
Paper Code: CYBNMV1N5OCT2019ST2
Submission Online: 02-Oct-2019
Manuscript Acknowledged: 07-Oct-2019
Originality Check: 17-Oct-2019
Originality Test Ratio: 18%
Peer Reviewers Comment: 19-Oct-2019
Blind Reviewers Remarks 20-Oct-2019
Author Revert: 21-Oct-2019
Camera-Ready-Copy: 24-Oct-2019
Editorial Board Citation: 25-Oct-2019
Published Online First: 31-Dec-2019

Cyber-attacks are the one of the critical issue faced by all and every human being including organizations. The Security of information systems is critical task for everyone. Human being should be able to understand the ecosystem, Hacking mechanism and predict attacks. Cyber-attacks quantitatively should be part of risk management. The cost impact due to worms, viruses, or other malicious software is significant. This paper proposes a Security Prediction & some previous massive Cyber-attack to predict the impact of an attack & how we can overcome from this situation based on significant factors that influence cyber security. This mechanism also considers the cyber prediction of 2020. It is fact or though and can be customized to the needs of the individual and any organization.

Keywords : Cyber Attack | Security Audit | Prediction2020

Introduction:

To triumph a battle, you well again join forces with like-minded allies, something that unluckily may not be well thought-out at all by the entities under attack, but has proven to be a successful strategy for cyber criminals.

At the present generationeveryone is endure connected, our smartphone have many in turn about us and just in case we can also come across this information in our gadget additionally, for a moment, our electronic items offer new prospective gratitude to the fact that they have accessibility to connect on the internet. In a matter of very few years, the Internet consolidated itself as a very powerful platform that has changed forever the way we do business, and the way we communicate.Internet is innovative. Two facts, in our opinion, have marked its evolution recently: the social web and mobile technology. These two innovations have changed the way people use the Internet. In the social web people have found a new way to communicate. Since its creation in year 2004, Facebook has grown into a worldwide network of over 2,450 million active users. Mobile technology, on the other hand, has made possible a much greater reach of the Internet, increasing the number of Internet users everywhere. The Internet, as no other communication medium, has given an International or, if you prefer, a "Globalized" dimension to the world. Internet has become the Universal source of information for millions of people, at home, at school, and at work.We depend on technology each time more but we don't perceive about one significant thing: the cyber-security. We are sure about many of you are not aware about cyber security. Cyber-attacks are not only for computers. We can suffer one when you least expect it. For example, have you ever have stayed in a hotel and you have connected your mobile to its Wi-Fi? If your answer is affirmative, you have put at risk your Smartphone and you have been a focus to a possible cyber attack.

These are some worldwide Colossal Cyber-Attack

1. Yahoo!: Hacker's front-runner?

It was colossal cyber-attack divulge by YAHOO on 2014, they disclose around 500 million user's confidential information was hacked including their Name, Telephone no. Date of Birth, User name & password. While YAHOO also assured that Banking Data has not been affected.

2. Marriott hotels:-Customer's Data's compromised

Data of 500 million guest was hacked, this was first time Marriott's era in 2018. Around $100 user bank details were hacked .

3. Equifax: Catastrophe

It's an American credit company, they provide credit to the stake holder.

Theyhave revealed (first six weeks after the fact), that it had crossedby a cyber attack over the course of a number of months. Detected in mid july, it contained the personal data (names, birthdates, social insurance numbers

4. The Target pointed

Target, is the second-largest US discount retail chain, was the victim of a large-scale cyber attack in December 2013. The Data from 110 million customers was hijacked between November 27 and December 15 including banking data of 40 million customers and personal data (names, postal addresses, telephone numbers, and email addresses) of another 70 million customers.

5 The South Korean's hallucination

The South Koreans face cyber-attack in January 2014,they disclose the data of 100 million credit cards had been hacked over the course of several years. In addition, around 20 million bank accounts had also been hacked

6 Adobe's misery

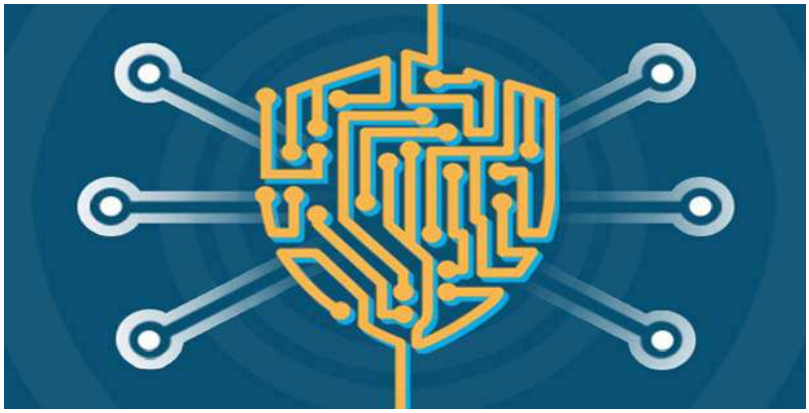
This was also the massive on attack on Adobe they announced 2013, that there was a massive on our IT infrastructure. Personal information of around 150 million was affected.

Adobe announced in October 2013 the massive hacking of its IT infrastructure. Personal information of 2.9 million accounts was stolen (logins, passwords, names, credit card numbers and expiration dates). Another file discovered on the internet later brought the number of accounts affected by the attack to 150 million (only 38 million active accounts). To access this information, the hackers took advantage of a security breach at the publisher, specifically related to security practices around passwords.

Cybercriminals are going to create 3.5 million new, unfilled cyber-security jobs by 2021. Compare that with one million openings in 2016. That's an increase of 350 percent in just five years.Let's talk some positive and some negative. Start with negative first. GDPR and CCPA may be onerous for some to deal with, these regulations will continue to force companies throughout 2020 to install and build processes that can identify, reduplicate, centralize and most importantly eliminate sensitive data generating a major win for all

Negative

- In 2020, we will witness an enlarge of targeted cyber threat attacks. Threat actors behind virus campaigns will switch tactics, leveraging access to organizations available for sale in the cybercrime underground.
- The most successful cyber attacks are executed by highly professional criminal networks that leverage AI and ML to exploit vulnerabilities such as user behaviour or security gaps to gain access to valuable business systems and data.
- Office 365 is a major target for IP theft, data leakage, credential cracking, and O365-specific attacks because that's where a big bulk of sensitive, enterprise data is
- In 2020, attacks will become more targeted and sophisticated. *Hackers will pivot from spray-and-pray tactics.*
- *Advertisers like Google, Facebook, and Amazon are going to start using more offline data to target consumers*
- Cybersecurity is a way which must be important for us, including companies. Last year in Spain, there was an increase of 200% in cybersecurity incidents (source: El País). It means that is important that we become more aware and take action.



Positive

- The adoption of AI dramatically improves the early detection of the threats and their mitigation. AI accelerates the identification of threats, especially new ones, and helps organizations to rapidly respond to them to block ongoing attacks.
- AI is going to be HUGE in 2020. And by huge, I mean that a lot of vendors will claim they are using AI—ranging from using simple linear regressions, up through using deep learning.
- As digitization continues in 2020, *data will become more valuable than ever before*.
- *In 2020, we'll see more organizations using AI and predictive proactive management to better anticipate, safeguard and prevent potential threat vectors ahead of time.*
- Artificial intelligence (AI) and machine learning algorithms used in cybersecurity have historically been trained with Information Technology (IT) network and system behavioral datasets. But in 2020 *we're going to see a rise of AI occurring in Operations Technology (OT) and automation control*
- Companies will reach a critical mass of 5G-enabled devices in 2020, forcing them to reevaluate their risk paradigm for connected devices
- *Security will become a leading decision criterion for the purchase of cloud services*. It will no longer just be about cost, flexibility, tooling and support

Data Breaches: Some Facts And Figure

- According to Capgemini, 63% of organizations are planning to deploy AI-based solutions in 2020, most of them to improve network security.
- According to the Data Breach Report published by the Identity Theft Resource Center, more than 1,200 data breaches were disclosed in 2019. As a result, hundreds of millions of records flooded the cybercrime underground. The availability of such data will be the root cause for most of the data breaches reported in 2020. In the next 12 months, we will see the rise of credential-stuffing attacks.
- Software and hardware supply chain attacks will characterize the threat landscape in the next 12 months. Attackers will attempt to compromise the supply chain of legitimate software packages by implanting malware.
- With advancements in the deepfake voice technology, I expect a rise of voice phishing schemes in 2020 in which employees are tricked into sending money to scammers or revealing sensitive information after getting voice messages and calls that sound like they are from the CFO or other executives.
- Deepfakes and synthetic identities will open the door for the next wave of identity fraud.
- Hackers will attack AI while it's still learning. As we increasingly depend on smart technology, the door for sabotage keeps opening wider and wider.
- By 2022, governments, organizations and individuals will realize their failure to protect 100% of their owned/handled information. They will begin limiting protection

down to the most valuable 25%, while placing the rest into fully/partially open access"—Joseph Feiman, Chief Strategy Officer, WhiteHat Security

Remedy & solution

- The crime-as-a-service (CaaS) model will continue to fuel the growth of the cybercrime ecosystem. The model facilitates the emergence of new criminal organizations and speeds up the operations of existing ones
- In the world of financial services, because of the ever-growing number of financial cyber-attacks, *regulators will become more open to banks using advanced AI systems to identify unknown and unexpected threats*.
- As we move into 2020, *companies need to shift to a more preventative approach to cybersecurity over a detection-focused approach*. The number of connected IoT devices will continue to increase making the likelihood of a cyberattack even more prevalent.

Finally there are certain solutions which need to be answered and if not answered we will answer in forthcoming issue.

- **Q-1:** What role emerging technologies (AI, machine learning, 5G, quantum computing) and evolving technologies (IoT, mobile—including autonomous vehicles, cloud) will play in improving the efficiency and effectiveness, breadth and depth, of cyber attacks in 2020?
- Q-2: What is Blockchain? What is the difference between Bitcoin blockchain (**Cryptocurrency**) and Ethereum blockchain?
- Q-3 : What happed if technology constant?
- Q-4 : Does our mechanical Devices can also be a part of hacking?
- Etc

References

Venkatesh Jaganathan, Priyesh Cherurveettil, and Premapriya Muthu Sivashanmugam, *Using a Prediction Model to Manage Cyber Security Threats*-The Scientific World Journal

https://www.checkpoint.com/definitions/what-is-cyber-attack

https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks

https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#2648bd1d4352

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4433707/

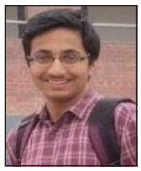
https://www.researchgate.net/publication/276488035_Using_a_Prediction_Model_to_Manage_Cyber_Security_Threats

https://www.ncbi.nlm.nih.gov/pubmed/26065024

https://www.sciencedirect.com/topics/computer-science/microsoft-word

https://resources.infosecinstitute.com/top-cybersecurity-predictions-for-2020/

https://www.carouselindustries.com/news-room/news/141-cybersecurity-predictionsfor- 2020/



Sachin Kumar is a Research Executive in Scholastic Seed Inc, He did his B.COM, M.COM* (University Of Delhi) BPP, ADCA-IT(MeitY). He have aggregate 2 year Experience in Cyber Research Field. He is owe allegiance in the area of Cyber-World i.e Emerging Data Threats, Virtual Dispersive Networking (VDN), Smart Grid Technologies, IoT (Internet of things), Cloud Sytem, also he had study on world's famous Cyber Hacker "Kevin Mitnick". He is always saying That Everything is possible in this current senerio because we're at the verge of changing the world by means of technology that can transform You & well as well as your mind, according to his Twiiter {@Shachindra26} he is substantially exploring National and international concerns. He Believes or take one's place with innovated idea's through industriousas a result of our world is Dynamic & we have work endeavour on that. He has been part of various Cyber conference & seminars.

ksak123@outlook.com
https://www.linkedin.com/in/sachin-kumar-aa815a191

Annexure I

Submission Date	Submission Id	Word Count	Character Count
17-Oct-2019	D61689324 (urkund)	2288	13045

Urkund Analysis Result

Analysed Document: 10/17/2019 ›curity Predictions in 2020.pdf (D61689324)
Submitted: 12/27/2019 3:17:00 AM
Submitted By: skesharwani@ignou.ac.in
Significance: 18 %

Sources included in the report:

https://www.researchgate.net/publication/276488035_Using_a_Prediction_Model_to_Manage_Cyber_Security_Threats
https://www.sciencedirect.com/topics/computer-science/microsoft-word
https://highschoolessaywritingprompts89.blogspot.com/2019/12/challenges-faced-by-business-from-cyber.html
https://www.ncbi.nlm.nih.gov/pubmed/26065024
https://varindia.com/news/channel-leadership-survey-2018--digital-transformationto-change-business-dynamics
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4433707/
https://go.gale.com/ps/i.do?id=GALE%7CA462685079&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=1537744X&p=AONE&sw=w
https://bdaily.co.uk/articles/2019/12/17/cyber-security-expert-predictions-for-2020
https://www.informationsecuritybuzz.com/expert-comments/2020-cybersecurity-predictions-experts-comments/
https://www.facebook.com/thetaray/posts
https://resources.infosecinstitute.com/top-cybersecurity-predictions-for-2020/
https://eu-es.facebook.com/thetaray/posts/?ref=page_internal
https://www.carouselindustries.com/news-room/news/141-cybersecurity-predictions-for-2020/

Instances where selected sources appear: 28

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Disclaimer: All Views expressed in this paper are my own, which some of the content are taken from open source website for the knowledge purpose. Those some of i had mentioned above in references section.

Reviewers Comment

Reviewer Comment 1: This article is based on the Current Cyber Situation, the author is really wanted to focus that how we can understand & overcome from cyber-attack. He has also discussed some passed cyber-attacks which causes a very serious issue for an Internet World.

Reviewer Comment 2: The author said that Cybercrime has increasing every year as human try to benefit from vulnerable business systems. Usually, attackers are looking for ransom. Cyber-threats can also be launched with ulterior motives such maybe- Financial, political or Social reasons.

Reviewer Comment 3: A Cyber-Attacks has variety of methods, including, malware, phishing, ransom ware, denial of service, etc,Cyber threats are constantly evolving, so the processes need to be regularly reviewed.

Editorial Excerpt

At the initial time of submission (TOS) the paper had 20% plagiarism, which on the later stages had been reduced to the 18%, which is an acceptable percentage for the publication, with the preliminary stage remarks and minor revision as suggested by the editorial board and blind reviewers at the successive stages as and when required to do so. The comments related to this manuscript are noteworthy and related to the "**Cyber attacks & Its Security Predictions in 2020**" both subject-wise and research wise. The author has crafted the paper in a well-structured manner. Due to the digital transformation there has been huge change in the medium of services being delivered this has also given rise to the prospects of cyber threats that necessitates the implementation of proper cybersecurity measures by various organisations. The article provides an overview of threats and security issues in delivering of services over internet. All the comments had been shared at variety of dates by the authors in calculation. By and large all the editorial board and reviewers' suggestions had been incorporated in the article and the manuscript had been earmarked and finalised to be published under "**Scrutiny Tip**" Category

Scholastic Seed Inc.
www.scholasticseed.in

Citation
Sachin Kumar
"Cyber attacks & Its Security Predictions in 2020"
Volume-1, Issue-5, Oct 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.