International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 09, September 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

THE IMPACT OF COVID-19 ON CYBER SECURITY: ITS THREATS AND INITIATIVES

Author 1:

Mrs. S.Santhoshi Rupa

Assistant professor
Department of Commerce
St.Ann's College for Women
(Autonomous)
Mehdipatnam, Hyderabad
Email id: santhoshi.rupa@gmail.com
Contact No.: 9182667152

Author 2:

Mrs. R.Meena Shanthi

Assistant professor
Department of Commerce
St.Ann's College for Women
(Autonomous)
Mehdipatnam, Hyderabad
Email id: ramdasmeena.1584@gmail.com
Contact No.:9966794666

ABSTRACT

Due to Covid -19, companies adjust to an operating paradigm where working from home has become the "new normal". The coronavirus pandemic has presented new obstacles. Businesses are quickening the process of going digital, and cybersecurity is increasingly a top worry. If cybersecurity concerns are disregarded, the reputational, operational, legal, and compliance consequences may be significant. This article looks at the effects of cyber security post COVID and the protective steps that companies might take. The cybersecurity of users and enterprises should all be improved. We are more susceptible to hostile attacks as more and more of our lives take place online. This was proved in 2020, when cyberattacks progressively hampered the operations of businesses, government agencies, and healthcare facilities all throughout the world. There is a sense of urgency to increase our cybersecurity resilience due to the frequency and size of the attacks.

Keywords: Cyber security, Cyber-attacks, Data Breaches , Threats , Measures

INTRODUCTION

In March 2020, the new coronavirus (COVID-19) epidemic struck the planet, altering how humans interact, work, and communicate. Working from home and avoiding social interaction became customary. Although digitalization was already a trend, it suddenly took off with the launch of COVID-19. As a result, in just a few months, the security of our government, corporations, and citizens which had been created over centuries became a concern of cybersecurity.

Cybersecurity is a procedure created to safeguard devices and networks from outside attacks. Businesses generally hire cyber security specialists to safeguard their private data, preserve worker productivity, and boost consumer confidence in goods and services.

Confidentiality, integrity, and availability are the industry standards that govern the field of cyber security. Only authorized individuals can access data in order to maintain privacy, integrity, and availability. Systems, functions, and data must all be readily available at all times in accordance with predetermined guidelines. Utilizing authentication procedures is the key component of cyber security.

Objective of the study:

1. To emphasize on importance of cyber security
2. To explore the issues of cyber security after covid
3. To understand the various data breaches
4. To know about various cyber threats
5. To know the measures to protect the data from cyber attacks

RESEARCH METHODOLOGY:

The data sources used in this research paper are secondary data due to the complex nature of the subject topic. The sources of secondary data used in this report are:

- **Published printed sources** – books, journals, magazine/newspaper articles
- **Published electronic sources** – general websites, e-journals, weblogs, mobile applications

LITERATURE REVIEW:

1. **Research Title:** Cybersecurity post-COVID-19: Lessons learned and policy recommendations
   Author: Iva Tasheva
   The paper focuses on the impact of coronavirus on cyber activities and what are the security measures to be adopted by the organizations. This paper defines the importance of developing standards for cybersecurity tools and services. It recommended continuing the cybersecurity awareness raising and hygiene campaigns in the citizens.
2. **Article** : Impact of COVID-19 on Cybersecurity
   Author: Cedric Nabe
   This Article focuses on the effect on cyber security due to covid. The paper defines various cyber threats and security measures to be adopted by the organizations.
   It recommended that there is a need for cyberattack detection, response and recovery capabilities for all kinds of data over the internet.
3. **Research Title**: Cyber resilience during the COVID-19 pandemic crisis: A case study
   Author: Jelle Groenendaal and Ira Helsloot
   The paper focus on the how organizations, Government sectors concerned on cyber-attacks. This paper defines effect of covid on organizations and the measures to be implemented by them. It recommended to understand how cyber resilience of organizations evolve over time.
4. **Research Title**: Cyberattacks and threats during COVID-19: A systematic literature review
   Author: Joel Chigada, Rujeko Madzinga
   The paper focuses on analysing the impact of cybercrimes on the global economy at a time when the whole world is focused on fighting and minimising the spread of COVID-19.

The study recommends that firms and individuals should devise cybersecurity interventions to protect their data and information systems infrastructure by adopting diversified security protocols.

Cyber security and its threats

Meaning of Cyber security: Protecting systems, networks, and applications from cyberattacks is the practice of cybersecurity. These cyberattacks typically try to gain access to, alter, or delete sensitive data; demand money from users; or obstruct regular corporate operations.

Some of the types of Cyber Crimes:-

- Denial of Service, or DOS
- Malware
- Man in the Middle
- Phishing
- Weak and Stolen Credentials
- Missing or Poor Encryption
- Social Media Attacks

Data Breach: A data breach is a situation in which information is taken from a system without the owner's knowledge or consent. A data breach is a cyber attack wherein an illegal access to or disclosure of sensitive, confidential, or other protected data has occurred. Any size organisation, from tiny companies to large multinationals, is susceptible to data breaches.

Impact of Cybercrime:

The price of cybercrime is influenced by a variety of factors. A lack of attention to the proper cybersecurity procedures is to blame for each of these issues.

Lack of attention to cybersecurity can harm your company in a number of ways, including:

- Economic costs include the cost of rebuilding damaged systems, the loss of company information, the theft of intellectual property, and the disruption of trade.
- Cost of Reputation: Decreased Consumer Trust, Customer Loss to Competitors, and Negative Media Coverage
- Regulatory Costs: Because of the GDPR and other data breach rules, your company may be subject to penalties or other regulatory actions as a result of cybercrimes.

HOW TO RESPOND TO A CYBERSECURITY BREACH

You could become a victim of a cybersecurity breach even after taking all necessary precautions. This is the time to act intelligently and make sure you have a disaster recovery plan. It enables you to react to such an attack as soon and successfully as possible. Be prepared to shut down the compromised system as well as any other connected devices. Run a virus scan and seek technical assistance as soon as you can. Get rid of all potential network dangers, then be extra watchful moving forward. The more you can save from such strikes, the faster you can react. The damage caused by hacking can be reduced by acting quickly.

We can state that there may be solutions to lessen the effect of the cyberattack on your company. It is necessary to manage such hazards appropriately. An excellent cyber security incident response plan can save the day in the event of an attack.

- It helps to reduce the impact of the breaching done
- Cleans up the systems that have been affected

Emerging issues :-

The COVID-19 pandemic changed how many people perform basic life activities such as working, shopping, and attending school. The shift from working in an office to working remotely from home introduced and exposed cybersecurity vulnerabilities. Home computers often lack the security protocols found in the office. Firms that use third-party vendors to monitor and address cyber threats may find that these solutions do not extend seamlessly to remote work.

Cybercriminals have exploited these gaps. The US Federal Bureau of Investigation reported the number of cyberattack complaints in 2020 increased by 400% from pre-COVID rates, reaching as many as 4,000 per day. One cybersecurity vendor reported more attacks on corporate networks in the first half of 2020 than in all of 2019. The use of ransomware increased significantly. These new vulnerabilities will require enterprises and other organizations to adapt and to educate employees on how to avoid and minimize threats while working remotely.

Impact of Covid on Cybersecurity

Approximately 20% of hacks used malware or techniques that had not yet been seen before the pandemic. The ratio has increased throughout the outbreak to 35%. Some of the new attacks make advantage of a type of machine learning that can change to its surroundings while avoiding detection. For instance, phishing assaults are getting increasingly complex and utilising many mediums, like SMS.

In order to tackle the threat posed by the rise in sophisticated cyberattacks, new "cutting edge" detection technologies are needed, such as "user and entity behaviour analysis" (UEBA). This examines how users typically behave and uses that understanding to look for occasions where abnormal departures from the norm take place.

Many small and medium-sized businesses have had difficulties as a result of remote working since they were not adequately prepared for the rise in sophisticated cyberattacks, and more has to be done to increase cybersecurity awareness. Before the pandemic, some businesses were hesitant to permit remote work, especially when it came to accessing sensitive information (e.g. banking client personal data). Companies had to expand their capacity and capabilities for remote work in a relatively short amount of time. Unfortunately, when remote working capabilities were quickly implemented, cybersecurity wasn't always given first consideration.

Example of Damages to Companies Affected by Cyber Attacks and Data Breaches

eBay:- Between February and March 2014, eBay was the victim of a breach of encrypted passwords, which resulted in asking all of its 145 million users to reset their passwords. Attackers used a small set of employee credentials to access this trove of user data. The stolen information included encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers, and dates of birth. The breach was disclosed in May 2014, after a month-long investigation by eBay.

Cyber Security Attacks:-

Thousands of cyber attacks were recorded through 2021, including ransomware, cryptocurrency theft, data loss, and supply chain attacks. Insight from the Identity Theft Research Center (ITRC) shows that recorded data breaches increased by 17% in 2021 compared to 2020. Examples of recent cyberattacks 2021 saw include:

1. ProxyLogon Cyberattack

One of the most damaging recent cyberattacks was a Microsoft Exchange server compromise that resulted in several zero-day vulnerabilities. The vulnerabilities, known as ProxyLogon and initially launched by the Hafnium hacking group, were first spotted by Microsoft in January and patched in March.

2. MeetMindful Cybersecurity Breach

Dating app MeetMindful suffered a cybersecurity attack in January 2021, resulting in data of more than 2 million users being stolen and leaked. The hacking group behind the event managed to steal information like users' full names and Facebook account tokens.

3. Tether Attack

In March 2021, cyber criminals threatened to leak documents from the Tether cryptocurrency. The attackers claimed the data would "harm the Bitcoin ecosystem" and demanded a settlement fee of around 500 Bitcoin ($24 million), but Tether refused to pay.

4. CAN Financial Breach

A ransomware attack on insurance firm CAN Financial left employees locked out of their systems and blocked from accessing corporate resources. The attack in March 2021 also involved company data being stolen, which led CAN Financial to reportedly pay the $40 million settlement fee.

5. Facebook Cyberattack

Data of more than 530 million Facebook users, including their names, Facebook IDs, dates of birth, and relationship status, was published online in April 2021. Facebook, now Meta, said the information was obtained through scraping in 2019.

6. Audi and Volkswagen Cybersecurity Breach

In June 2021, Audi and Volkswagen revealed a data breach had affected more than 3.3 million customers and prospective buyers, who were primarily U.S.-based. The breach was blamed on an associated vendor, which was purportedly responsible for exposing the data between August 2019 and May 2021.

How to Protect your Organization Against Cybercrime

It is possible to boost security and lower the danger of cybercrime by taking these easy steps:

1. **Educate Staff:** Most of the data breaches were the result of human mistake. The vast majority of data breach instances might be prevented if staff members were taught how to recognise and appropriately react to cyber threats. Such training initiatives might also raise the value of all investments in cybersecurity solutions since they would stop personnel from carelessly disabling costly security measures to aid in cybercrime.
2. **Sensitive Data:** Invest in tools that prevent information loss, keep an eye on vendor and third-party risk, and regularly check for data exposure and compromised credentials. If data leaks go unchecked, fraudsters may use them to infiltrate corporate networks and compromise sensitive data. Implementing a data leak finding system that can also monitor leaks is crucial.
3. **Implement a Third-Party Risk Management (TPRM) Solution :** Utilize technology to cut costs, such as by automatically distributing vendor assessment questionnaires as part of a comprehensive approach for assessing cyber security risk. Instead of asking why cybersecurity is necessary, businesses should be asking how they can make sure their cybersecurity procedures are enough to abide by the GDPR and other laws and safeguard their operations against sophisticated cyberattacks.

EFFECTIVE MEASURES AGAINST CYBERSECURITY ATTACKS

One of the best solutions is to maintain as much defensiveness as possible. The easiest way to deal with this problem is to keep your firewalls, antivirus software, and security measures up to date. Every day, hackers improve their skills and come up with new ways to steal your personal data. The only way to do this is to keep abreast of all security measures. A single email attachment that includes a virus can infect the entire LAN, despite the use of all practical precautions and major investment in the best security solutions.

The majority of the time, small businesses do not view this as a serious issue that they may one day have to handle. However, now is the moment to make the most pro-active investment to safeguard him or her SMB.

The advantages of putting cybersecurity policies into place and maintaining them are:

- Business protection against cyberattacks and data breaches.
- Network and data protection.
- Restricting access by unauthorised users.
- Shorter time it takes to recover after a breach.
- End-user and endpoint device security.

• Adherence to regulations.

• Continuity of operations.

• Increased trust among stakeholders, consumers, partners, employees, and developers in the company's reputation.

People working on the data over internet should implement following cyber hygiene practices:

- Antivirus Protection
- Cybersecurity awareness
- Phishing Awareness
- Home network security
- Use a VPN (Virtual Private Network)
- Frequent reviews
- Proper Encryption techniques

Findings:

1. It is highly beneficial to strengthen everyone's cybersecurity posture, including businesses, government organisations, and the whole country, in order to lessen the potential loss and harm brought on by cybersecurity breaches.

2. To increase cybersecurity, two different types of activity are required: (a) attempts to make existing cybersecurity knowledge more widely and effectively used; and (b) initiatives to create new cybersecurity knowledge.

3. Until now, publicly accessible data and policy initiatives have not been sufficient to develop a sufficient feeling of urgency and ownership regarding the cybersecurity issues plaguing the United States as a whole.

4. The United States values cybersecurity, but it also has other interests, some of which are at odds with the demands of cybersecurity. Through the political and policy-making processes of the country, tradeoffs will inevitably occur and must be accepted.

5. The employment of offensive operations in cyberspace as a tool to advance American interests poses a number of significant technological, legal, and policy issues that the US administration has not yet openly addressed.

CONCLUSION:

Understanding cybersecurity needs knowledge and expertise from many different fields, including but not limited to computer science and information technology, psychology, economics, organisational behaviour, political science, engineering, sociology, decision sciences, international relations, and law. Cybersecurity is a complicated issue. In reality, cybersecurity is not primarily a technological issue, despite the fact that technical specifics are simple for policy analysts and others to become bogged down in. In addition, knowledge about

cybersecurity is frequently classified along disciplinary lines, which limits the insights that might be gained from cross-fertilization.

This introduction aims to clarify some of these links. It aims to leave the reader with two main thoughts above anything else. Solutions to the problem, limited in scope and longevity though they may be, are at least as much nontechnical as technical in nature. Monitoring and Upgrading cybersecurity is a continuous process.

REFERENCES

[1] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
[2] https://www.innefu.com/blog/how-cyber-security-impacts-businesses-globally/
[3] https://www.upguard.com/blog/cybersecurity-important#:~:text=Cybersecurity%20is%20important%20because%20it,governmental%20and%20industry%20information%20systems.
[4] https://www.google.com/amp/s/www.techtarget.com/searchsecurity/definition/cybersecurity%3famp=1
[5] https://www.ncbi.nlm.nih.gov/books/NBK223216/
[6] https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks
[7] https://journals.sagepub.com/doi/full/10.1177/17816858211059250
[8] http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2021000100001