Original Research Article

CYBERSECURITY CHALLENGES AND SOLUTIONS FOR GIG ECONOMY PLATFORMS

*** Sayali Pradeep Birje & ** Dorris Manuel Gonsalves**

*

Abstract:

The gig economy has revolutionized the global labor market. It provides short-term bases and freelance work environments. Gig economy is mainly a term used to describe online work from remote places. This nature of the gig economy makes it dependent on digital platforms, which introduces a risk of cybersecurity. This research paper examines the cybersecurity challenges faced by gig economy stakeholders, including data breaches, user privacy concern, fraud, phishing attacks and lack of standardization. It also states various solutions such as using strong passwords, installing security software, educating employees, encryption of sensitive data, and time-to-time data backup. The paper concludes with how a sustainable gig economy ecosystem can be achieved.

Keywords: *Gig economy, cyber security, encryption, data breach, phishing*
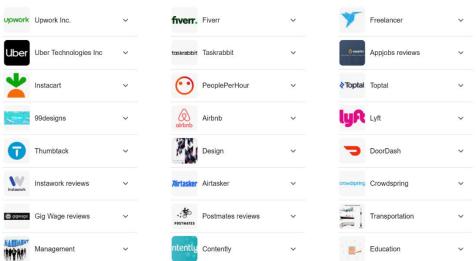
Introduction:

1. Gig Economy:

A gig economy is an economy that is flexible means of earning on a temporary basis. Organizations hire temporary workers and freelancers. It has no systematic schedule. Companies such as Uber, DoorDash, and Airbnb work with similar structure. The result of a gig economy generates faster means of earning without any commitment for longer time with an organization. In addition, it completely operates on internet making it a demographic choice for youngsters.

2. Gig Economy Platforms:

The gig economy is rapidly growing each day. The following are some gig economy platforms:
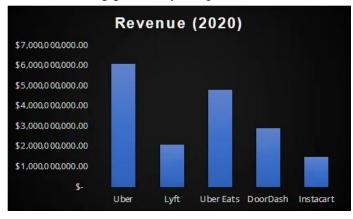
Shown below are some of the most renowned gig economy companies with revenue earned in 2020:

Revenue (2020)

3. Cybersecurity:

Cybersecurity is the practice of protecting data or information from intruders and attackers. It's also known as e-information security.

The term "cybersecurity" applies in a variety of fields and some of them are listed below:

1. Network security:

It deals with protecting your data on internet by any unwanted access or unwanted attack. The data when it travels through internet may be prone to different attacks like loss of integrity, Denial of Service, lack of availability. To protect your data from such attacks there are various encryption techniques used.

2. Application security:

It mainly focuses on protecting various applications working on application layer. Securing any application before it is ready to deploy is the main aim of application security

3. Information security:

It protects the integrity of data which is been stored in the database as well as the one which is travelling into a network.

4. Operational security:

It mainly deals with protecting the data assets. How much access should be given to each user for the different types of data is set here for security needs.

5. Disaster recovery:

It mainly defines how organization recovers after any disaster and continues with the business. The policy of disaster recovery states how to resume the business back to normal on facing any disaster. To continue the business with minimum or no resources is the main aim under recovery.

6. End-user awareness:

End users should be educated about risk and consequences of any sort of cyber-attack. They should be made aware about not downloading any attachment from an unknown site or unknown email, should not plug-in anyone's pen drive as it may contain malicious code or virus.

Literature Review:

In today's fast-growing technology and variety of choices for job, gig economy has achieved a wider interest and support. Most companies are interested in contractual workers instead of hiring full timers, which has mainly increased the demand for gig economy.

In a study done by NITI Aayog(National Institute for Transforming India) 2020-2021, 7.7 million Indians opted for gig economy, which was 2.6% of the non-

OPEN ACCESS   **Original Research Article**

agricultural workforce or 1.5% of the overall Indian workforce.

The gig economy facilitates variety of job opportunities for freelancer and part time workers. As gig economy is mainly an online mode of job with internet facility, there exists many cybersecurity risks. As companies hire contractual employees, they do not want to invest much in buying devices or providing infrastructure for them. So, employees use their own devices on which they are accessing the company's data. The company's data is easily accessible on end user device. Hence, this may pose a great threat to the company's data. As a measure the company should learn the risks associated with the same and take some security measures to protect the data which can be easily available online on internet.

Challenges with the Gig Economy Platforms:

1. Data Breaches:

In cybersecurity, a data breach means confidential or sensitive data or information is stolen or lost with unauthorized access.

Intruders trying to cause a data breach often attack companies with large or bulky databases. Such large databases normally include sensitive data such as login credentials or financial information or credit card details of employees as well as customers.

Example:

In 2020, Twitter accounts of famous personality were attacked. The attackers gained accessed to Twitter's administrative tool by releasing social engineering attack techniques. These tactics made the victims to reveal their sensitive data to attackers out of fear, curiosity or trust. This initial breach gave access to the attackers to enter the database and slowly they went on exploiting other accounts as well which made them collect approximately $117,000 in Bitcoin.

2. User Privacy Concern

Gig platforms gather large amount of data from their workers to improve customer services. This data includes personal information such as names, addresses, contact details, and financial data. Even though this data is necessary for smooth working of a company, but the data which is collected raises several questions like; How it is collected? Where it is stored? How it is used for processing? Workers have little or no idea on these questions.

Example:

Food delivery platforms like Swiggy and Zomato may use employee data to figure out and optimize delivery operations. This benefits the smooth working of the companies but the employees aren't aware whether their data is being shared with any third party or not.

3. Phishing Attack

Phishing is an attack where an unauthorized user or an intruder disguise himself as a legitimate user and tries to get information such as username, passwords, or any sort of bank details from victim by sending emails, messages or by communicating through fake websites.

Example:

A fake email or message pretending to be from "Ola support desk" which may ask the driver to click the link in the email stating that the payment will be halted due to some login issues. On clicking the link, the driver gets redirected to a fake site where he needs to enter login credentials and bank details.

4. Fraud

As more people contribute to freelance and contract-based work, the chances of fraud has increased on gig economy platforms. Gig economy platforms connect people willing to avail short-term jobs with companies offering gig

economy jobs. Even though these platforms offer flexibility and opportunities, it also brings in various vulnerabilities.

Example:

Fraudsters might use a fake identity and sign up as a worker to create some sort of scam. Many a times a fake sign up is used for fraudulent bookings and payments.

5. **Lack of Standardization**

Lack of Standardization is a significant challenge for both employees and organization working within the space. As gig economy is used for freelancer, it is growing rapidly and hence it inhibits lack of uniformity which leads to several threats.

Example:

Different ride-share drivers earn different amount depending on the platform (Ola, Uber, Rapido) they work for. Some platforms offer a fair payment whereas some offer a minimal amount. Gig workers do not have a clear idea of how their payment is calculated.

Solutions for Gig Economy Platforms:

1. **Using Strong Passwords:**

Always use complicated and hard-to-break passwords for your account. Try to keep 2-factor authentication, where a next level of security like OTP (One Time Password) is required. You can refer password manager for generating stronger passwords for different platforms.

2. **Installing Security Software:**

Always install anti-virus on your device and keep it updated time-to-time. Enable firewall on your device once it is connected to internet. Try to use VPN (Virtual Private Network) instead of public wi-fi.

3. **Educating Employees:**

Gig economy platforms should educate their workers regarding protection of their accounts by providing some training sessions. Workers should be trained on identifying scams and securing personal information.

4. **Encryption of Sensitive Data:**

Rather than storing data in plain text, you can generate a cipher text and then store it. There are various encryption techniques available for the same. When attacker tries to access your confidential data, he/she may get the data but will not understand the contents as they are encrypted.

5. **Time-to-Time Data Backup:**

Data should be regularly backed-up to keep it safe in case of any possible attack. If it is not regularly backed-up then we may loose confidential and sensitive data. Also, back-up is required to protect the data from loss of integrity attack.

Conclusion:

The rapid expansion of gig economy has gained momentum for businesses, employees and customers as well. However, this growth has ultimately given rise to cybersecurity threats. Cyber-attacks have significant impact on financial data, company reputation and customer trust. Avoiding such attacks give rise to the need of robust security techniques to use gig economy platforms sustainably. Understanding the various challenges and trying to overcome them will benefit all the stakeholders using gig economy platforms. By using ethical means of work by all individual involved in the workspace, we can easily overcome the challenges and minimize the risk of cyber-attacks. Although the challenges and risks cannot be completely eliminated or diminished, but can be reduced to a greater extent by using various robust tactics which can further enhance reliable, secure and sustainable gig economy environment.

References:

1. Juneja, A., Goswami, S. S., & Mondal, S. (2024). *Cyber security and digital economy: opportunities, growth and challenges. Journal of technology*

OPEN ACCESS   **Original Research Article**

innovations and energy, 3(2), 1-22.

2. *Tsaaro Consulting, IT Services and IT Consulting, Bengaluru East, Karnataka (June 9, 2023), Data Privacy & Cybersecurity Consulting*

3. *https://frontline.thehindu.com/the-nation/human-rights/gig-economy-india-workers-rights-labour-exploitation-surveillance-data-privacy-laws/article69341247.ece*

Cite This Article:

Birje S.P. & Gonsalves D.M.(2025). Cybersecurity Challenges and Solutions for Gig Economy Platforms. .**In Aarhat Multidisciplinary International Education Research Journal**: Vol. XIV (Number II, pp. 25–29).