IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPACT OF CYBERSECURITY IN HOSPITALITY INDUSTRY IN INDIAN CONTEXT A CASE STUDY ON OYO ROOMS

PRATIK ANURAJ,

PGDM- SYSTEMS/IT,

SRI BALAJI UNIVERSITY, PUNE, INDIA

Abstract: Oyo Rooms and hotels started in 2013 as an Indian startup by Mr. Ritesh Agarwal is into Hospitality business. The issue of data breach came into the picture in the month of Oct 2019, when a person wrote about the leak of customer's personal data including mobile no, booking IDs, location, number of people staying, etc. in the public forum. The person had stayed at the Oyo hotel and got to know about this vulnerability as he was able to brute-force the login credentials while executing the Captcha and can access all the past data.

The study is about the data breach in Oyo cyber space which was published last year in 2019 and its consequences. I also studied the concept of cyber security and provided some remedial solutions which can be taken after or before the breach to reinforce the security of the Oyo cyber space in near future.

Index Terms – Oyo rooms, Cybersecurity, Data Breach, Cyber Attack, IT ACT

I. INTRODUCTION:

The purpose of this study is to understand the Oyo's case of data breach with respect to cyber security along with the concept of Cyber security. I had also made an attempt to provide some remedial measures which can be taken after and before the breach.

For this study I had taken some articles published in the economic times and also in the various websites. From these articles I got to know about the security issues with the OYO. Then I applied my studies from post-graduation subject cybersecurity to understand the issue, concept and to give some remedial measure.

Oyo Rooms, also referred as Oyo Homes & Hotels, is an Indian hotel chain which is the world's 3rd largest and fastest-growing hospitality chain of leased and franchised hotels, homes and living spaces. It was founded in 2013 by Mr. Ritesh Agarwal, headquartered at Gurugram and mainly consisted of budget hotels initially. But within a span of six years, this startup expanded globally with thousands of hotels, vacation homes and many rooms in many cities of India, Malaysia, UAE,

Nepal, China, Brazil, Mexico, UK, Philippines, Japan, Saudi Arabia, Sri Lanka, Indonesia, Vietnam, U.S and more.

II. CASE DATA:

Oct 2019, Oyo's customer data was susceptible to a breach as there was a flaw in its security systems, a cyber-security researcher revealed on professional networking site LinkedIn. The info includes booking IDs, phone numbers, the number of individuals stayed at a room, date of booking and location.

Jay Sharma reported the vulnerability of data by writing on LinkedIn that, when he stayed at Oyo for the first time, after check-in, it had been made compulsory to enter booking ID and telephone number to access the WiFi. He also said that why should anybody within the room be forced to share personal information via OTP verification to use WiFi?

He researched more and located that the HTTP & SSL ports were open, with no rate limit for the IP which was hosting this. Captcha was a 5-digit number generated by math.random(). He then wrote that he created how to brute force the login credentials while executing the captcha. Once login was brute-forced, all the historical data dating back to a couple of months was accessible.

An Oyo official said a statement that, Oyo employs and invests heavily for the best cyber security mechanisms in the industry, including in-house security operation centers, internal and external vulnerability scans and network penetration tests, training developers on secure development practices, etc. Any vulnerability, regardless of how limited-time or small it is, taken very seriously and looked into.

This post also gathered criticism on social media, since the flaw in privacy also meant that Oyo failed to provide adequate privacy to the couples, as their details and location could been accessed, although the founder of this hospitality chain had said it was, indeed, couple-friendly.

Another issue in previous year, 2018 Feb was, OYO has had filed a criminal complaint against the founders of another budget hotel group – Zostel, alleging breach of trust, cheating and misinterpretation of data.

OYO was in a deal to acquire Zostel Hospitality Pvt Ltd's budget hotel business Zo Rooms in an all stock deal since 2015, but had cancelled the deal on September 2016.

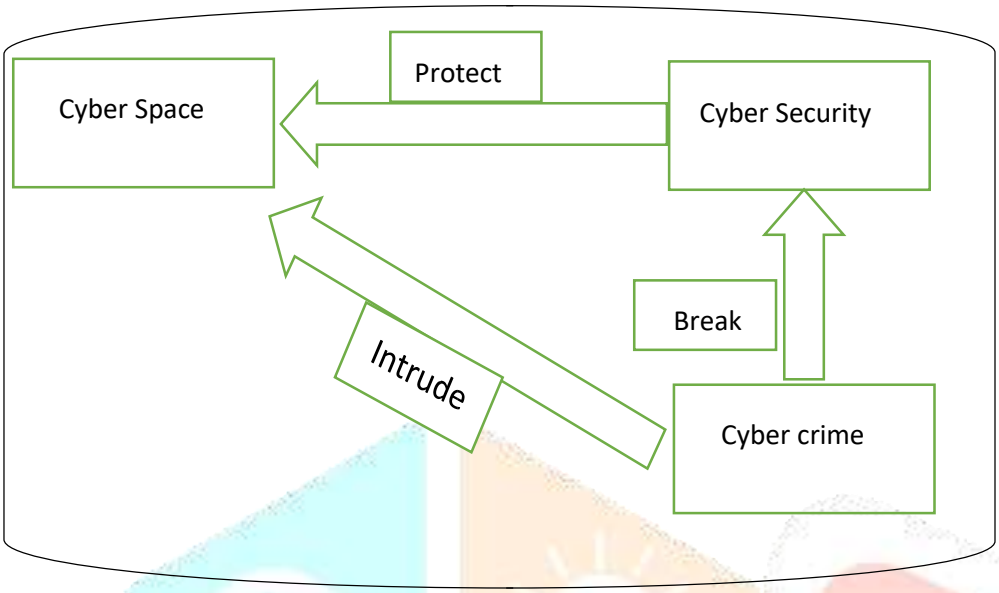
Oyo said in a statement that, Zostel and its directors were continuously harassing the corporates for quite a year and the firm has been trying blackmail Oyo and its investors to get the deal done.

Oyo statement added that Zostel has filed a 'misconceived and baseless' arbitration petition in a Gurgaon Court on 2 February, concerning a long-expired and non-binding term sheet. OYO said that they have filed a criminal complaint against the founders of Zostel under Section 405, 406, 415, 420, 425 and 426, concerning Criminal Breach of Trust, Cheating and Misrepresentation of knowledge on 16th January.

This was the second instance that the firm has filed a case against Zostel for which OYO said they had previously filed criminal cases under section 379, 414, 420 and 120B of Indian legal code and other implications under the IT and Copyright Acts with the Economic Offences Wing & Cybercrime department against senior employees of Zostel for stealing data and other assets including laptops.

According to Oyo the reasons for cancelling the deal last year was that Zostel didn't answered to the list of questions identified during their diligence process, including significant liabilities and unpaid dues.

III. THEORITICAL FRAMEWORK:



IT Act for protection of cyber security and prevention of cyber crime

The Cyber world is made up of by the use of mobile phones, personal computers, electronics and electromagnetic spectrum which is used to store, modify, and exchange data through networks and related physical infrastructures. Cyber world can also be seen as the place in which computer transactions takes place between different computers or networks. The transaction can be of data, databases, record of images, personal information and text on the Internet. It can also be defined as a global spectrum within the information environment consisting of interdependent network of IT 39infrastructure, including computer systems, mobile networks Internet, telecommunications networks and IOT.

Cyber security consists of processes, technologies and controls that are designed to protect systems, networks and data from cyber threats. Effective cyber security prevents the risk of cyber-attacks and unauthorized exploitation of networks, computer systems and technologies. A Well-defined cyber security domain involves implementing controls based on three spectrums: people, processes and technology. These three methods help organizations to protect themselves from both organized attacks and common internal attack such as accidental violations and human errors.

Cybercrime is a sequence of organized manner of attacking network and cyber security domain. E.g. hacking into web applications, computers and stealing personal & payment information, email and internet fraud, identity fraud and ransom attacks, as well as many different domains of profit-driven criminal activity. An attempt to steal financial accounts, credit card or other payment card information also comes under cybercrime. These attacks can take place through a networked system and by clicking on untrusted links, connecting to unauthorized Wi-Fi, downloading software and files from unprotected sites, electromagnetic waves and many other spectrums.

Cybercrime is a criminal activity committed using computers and the Internet. This is done via illegal/unauthorized access, transmission of computer data, to or within computer systems. It can be anything from downloading illegal files to stealing crores of rupees from online bank accounts. In cybercrime Non-monetary crimes are also involved. E.g. Viruses distributing and building on

other systems are exposing confidential business information on the Internet or identity theft, in which criminals use the Internet to steal personal information from other users.

The Information Technology Act (2000), amended by IT Act (2008) contains provisions for the protection of electronic data. The Act lays down "cyber contraventions" which attracts civil action under the Section 43 (a to h) and "cyber offences" which attracts criminal action under the Sections 63 to 74. The earlier category included gaining unauthorized access to, and downloading or extracting data from, computer systems or networks. The later covers "serious" offences like tampering with computer source code, hacking with intent to cause damage and breach of confidentiality and privacy. In April 2011, Indian Ministry of Communication and Technology publish 4 sets of rules containing certain provisions of the Information Technology Act (2008) called as IT Rules (2011), framed under section 43A of IT Act, and put down procedure for corporate entities which collect, process or store personal data. This rules also distinguish "personal information" from "sensitive personal information".

Section 43 of the IT Act, lays down penalty for doing any of the following acts:

• If anyone accesses or secures access to such computer, computer system or computer network.

• If anyone downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

• If anyone introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

• If anyone damages any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

• If anyone disrupts or causes disruption of any computer, computer system or computer network;

• If anyone denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means, provides any assistance to any person to facilitate access to computers, PC system or network in contravention of the provisions of this Act.

• If anyone charges the services availed by a person to the account of any other person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages to the person so affected.

• If anyone destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

• If anyone steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Section 65 of the IT Act lays down that whoever knowingly or intentionally conceals, destroys, or alters any source code used for a computer, program, computer system or network, when the source code is required to be kept or maintained by law for the time being in force, he/she shall be punishable with imprisonment up to three years, or with fine which may extend up to Rs 2,00,000, or both.

Section 66 says that if anybody, dishonestly or fraudulently does any act as mentioned in section 43, he/she shall be punishable with imprisonment for a term which can be of three years or fine which can be up to Rs 5,00,000, or both.

Section 72 of the IT Act lays down penalty for breach of confidentiality and privacy. The Section states that somebody who has secured an access to any electronic data, books, register, correspondence, information, documents or the other material without the consent of the person concerned and discloses such material to the other person, shall be punishable with imprisonment for a term which can extend up to two years, or with fine which can extend up to Rs 1,00,000, or both.

Some important sections substituted and inserted by the IT Amendment Act, 2008 are:

1. Section 43A – Compensation for data protection failure.

2. Section 66 – Computer Related Offences.

3. Section 66A – Punishment for sending offensive messages in electronic form.

4. Section 66B – Punishment for receiving stolen computer resource or any communication device in dishonest way.

5. Section 66C – Identity theft punishment.

6. Section 66D – Punishment for cheating by personation by using computer resource.

7. Section 66E – Punishment for violation for privacy.

8. Section 66F – Punishment for cyber terrorism.

9. Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

10. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act in electronic form.

11. Section 67B – Punishment for publishing or transmitting of material depicting minors in sexually explicit act in electronic form.

12. Section 67C – Preservation and Retention of information by intermediaries during a transaction.

13. Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.

14. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource.

15. Section 69B – Power to authorize to watch and collect traffic data or information through any computer resource for cyber security.

In Oyo's case a person easily got an access to all the past customer's data which might be used against the customer. These exposed data may be employed by hacker to tap the customer and harass them or can even cause financial loss.

As per the study, typically data security breach takes very less time to be executed and 93% of successful data breaches occurs within few seconds. Yet, 80% of companies takes weeks to comprehend that a breach has occurred. Data breach can cause an awfully expensive consequences, that is why 86% of business believes that cyber security threats like weak data security, are concerning.

According to me in this case, some of the major consequences to Oyo because of data breach can be:

1. **Revenue Loss**: As because of breach of information people are going to be aware that their personal information isn't secure with Oyo and hence conversion rates will decrease. This may end in revenue loss. Moreover, studies show that 29% of businesses that face a data breach end up losing revenue.

2. **Damage to Brand Reputation**: Security breach of the Oyo's data can even damage the Brand image amongst the people. Customers value their privacy and breaches often involve customer payment information. Hence, potential leads are going to be hesitant to trust the business with a history of poor data security. Thus, the Brand becomes untrustworthy for the people.

3. **Loss of Intellectual Property**: Intellectual property are the intangible property of a business-like designs, strategies, blueprints, name, logo, trademarks, etc. Hackers can even target this stuff and can cause damage to business. Loss of intellectual property can impact the competitiveness of the business. In Oyo's case rivals can take an advantage of stolen information and may also use these for extortion.

4. **Hidden Costs**: After the breach occurs, business needs to encounter many hidden costs like legal fees other than costs of hiring security specialists and engineers to seal the breach. Also, there may be need to spend more on public relations and investigations. Regulatory fines are another reality that several businesses overlook.

5. **Online Vandalism**: In some cases, a security breach might only cause few word changes on the company's website like, a hacker might change some letters or numbers on the contact page or they'll add vulgar content to some of the webpages. This can tarnish the name of the business.

IV. SOLUTIONS:

Based on the study in Cyber security some of the remedial measures which can be taken to enhance the security of Oyo's Cyber space are as follows:

• Develop a full-fledged bug bounty program, to encourage more and more independent security researchers to find a flaw and report.

• By creating awareness, as technology is advancing so more people rely on the Internet to store sensitive data's such as banking/credit card information, criminals are trying to steal that information. Hence, there must be an awareness about how information is protected and the tactics used by criminals to steal data.

• Use of cryptography: It is most often associated with scrambling of plain text (ordinary text, also referred as clear text) into cipher text (encryption), then back again to original form (decryption).

• Use of robust network firewalls and anti-malware software can prevent the system from unauthorized attacks.

• Ensure that HTTP and SSL (Secure Socket layers) are enabled for secure data authentication and encryption over internet.

• User Authorization & Accessibility, ensure that employees are only given access to files that are necessary for them to complete their jobs.

• To prevent hackers from un-authorized access, implement multiple levels of authentication and re-routing of IP address.

• Use genuine software's and keep them updated regularly.

• Ensure high security with the help of CCTV camera and physical control at the place where data is stored like Data Centre/ confidential file rooms to ensure there is no physical theft of equipment/data.

• In case some equipment like hard disk gets damaged ensure that it should be destroyed beyond recovery of contents.

• Regular Audit of IT assets.

• Background check of people working with sensitive data and control room operations including backup, restore and maintenance.

• Non-disclosure agreement (NDA) to be obtained from all employees dealing with Oyo's Information Technology initiatives.

V. SUMMARY:

The main problem of the Oyo is about the information breach which occurred because of lack of security in Oyo's cyber space. As Oyo stores all the customer data in an electronic form in its cyber space, so how can it be protected against theft in near future. As discussed within the case somebody got hold of all the historic personal data of the customers by easily brute forcing the login and getting into the Oyo system. All the data of customer either personal or financial are within the cyber space of Oyo but it's the right of the individual that the data are kept in privacy. Oyo needs to take steps to strengthen its cyber security and there are many ways in which it can be done.

So, any online business firms should ensure that their IT framework is strong enough to tackle external as well as internal attacks in the network. To do so they must follow some of the basic security steps as mentioned above. As Data is money and money are business so protecting the data is very essential in today's cyber world.

VI. ACKNOWLEDGEMENT:

I take this opportunity to thank all the people who have helped me through the course of my journey towards completing this study. I sincerely thank my mentor Dr. Shrikant Ratley and Mr. Quresh Moochala for his guidance and encouragement in carrying out this study. I would also like to thank all the teaching faculties for imparting knowledge and making me capable of understanding the concepts and completing this study. At last I would like to acknowledge the support and encouragement of my friends and family. This study would not have been possible without the confidence, endurance and support from them.

VII. REFERENCES:

- https://tech.economictimes.indiatimes.com/news/startups/oyo-leavescustomer-data-exposed-due-to-a-security-flaw/71394350, Oct-2019.
- https://www.thequint.com/news/business/oyo-files-case-against-zostel-forcheating-data-theft, Feb-2018.
- https://craft.co/oyo-rooms/metrics
- https://en.wikipedia.org/wiki/Oyo_Rooms
- https://www.whizsky.com/2018/09/case-study-oyo-rooms-full-growth-story/
- https://www.businesstoday.in/current/corporate/oyo-rooms-fy19-loss-rises-6fold-to-rs-2384-crore-on-higher-expenses/story/391001.html,Nov2019
- https://www.mondaq.com/india/Privacy/655034/Data-Protection-Laws-In-
- India--Everything-You-Must-Know
- Volume-1 | Issue-2 | July 2019 23, World of Cyber Space: Cyber (Crime, Security, Law) and Cyber Solution, Vishal Kumar.
- https://www.godaddy.com/garage/whats-an-ssl-port-a-technical-guide-forhttps/
- https://www.theamegroup.com/security-breach/