JANOLI International Journal of Applied Engineering and Management
(A publication unit of Shanti Educational Research Foundation)

The Greater Risk to Startups in the Buyer Arena is Security

Narendra Kumar
NIET, NIMS University, Jaipur
Email: drnk.cse@gmail.com

Abstract: The study article that follows expands on our knowledge of a start-up's confidentiality issues from the viewpoints of two parties. The first viewpoint reflects that of a start-up, which means that the business should maintain the confidentiality of the personal details of its consumers. The other point of view is that of a businessperson, which means that the concept of the start-up should remain private. Thus, protecting your concept and information for a new company becomes a demanding task. To reach the only goal of starting a start-up, one of the most important steps that must be given thoughtful consideration is safeguarding and preserving one's concept and data relevant to their startup company. We will also comprehend the significance of confidentiality in the consumer environment and the potential repercussions should such security be violated or abused by businesses. We will also learn how these businessmen and start-up businesses defend their own against these kinds of security lapses and data stealing. This paper will undoubtedly go into great detail on all the issues and probable remedies pertaining to the security of an entrepreneur's and client's data.

Keywords: Consumer space, secrecy, Service providers, Stealing

INTRODUCTION:

Having an estimated 1.2 billion citizens, India is the world's second-most populous nation. There is a vast job possibility in the market to take use of this large humanity, but recent Progress Surveys have shown that India is falling short in terms of hiring young people, and this situation is expected to persist for thirty-five years. Our leader, PM Narendra Modi, urged individuals to create their own businesses in order to address the lack of jobs in the market. The region's economy has grown significantly thanks in large part to entrepreneurship. A great number of data-driven start-ups have achieved rapid climb within the past few years. Start- ups have become a significant technology vendor in the market due to its innovation and thrive to push within the commercial space. As we know most of the start-ups are directly or indirectly developed in a co-working environment and are data-driven so privacy of data and idea itself becomes a threat for a start-up. As technical start-ups are mostly data oriented it is mandatory for them to seem after their data and protect it to avoid any sort of damage to the entrepreneur and to safeguard the personal information of the consumers. So, securing your idea and data for the start-up becomes a strenuous job. Protecting and preserving one's idea and data related to their start-up is one of the most essential stages that should be given thorough attention to achieve the sole purpose of initiating a start-up. We will examine privacy from two distinct perspectives in the next study. We will first discuss the potential for a business's information security to be compromised and then the likelihood of a businessperson abusing their privacy. We will also discover why privacy is crucial for new businesses, the kinds of privacy dangers to be mindful of, why privacy poses the greatest risk to consumer start-ups, and the potential consequences of violating someone's privacy.

Privacy the Bigger Threat for Start-Ups in Consumer Space: Before going in further details, we need to understand three terms and a relation which are as follows: -

- Privacy
- Start-ups
- Consumer space
- Relation between start-ups and privacy

In broad terms[11], security is defined as the capacity to safeguard and obscure personally identifying or confidential data. In plain English, it refers to a person's right to decide how their private data is gathered and applied. A start-up is essentially a concept on which one or more entrepreneurs collaborate to create a special product or service, which is subsequently introduced to the market. The term "consumer space" refers to a specific place where services are provided for an individual's requirements. It might be a setup where several employees from various businesses share a same workspace. Regarding the connection between new companies and privacy, Regarding the former, it can be said that startups rely heavily on anonymity. During the last several years, a large number of start-ups fueled by data have seen exceptional growth. Due to their inventiveness and ability to grow in the business world, startups have emerged as a major player in the field of technology. However, because technological start-ups primarily deal with data, they must take precautions to secure their data in order to prevent harm to their founders and to protect the privacy of their clientele. Now after putting some light on the above topics some questions strike our minds like –

- Why is privacy so important in start-ups?
- What happens when privacy or personal information is exploited by companies?
- How do start-ups protect their privacy?

There are two quite different ways we may approach this subject.(6) We will first address this subject from the standpoint of why consumer privacy has to be fully protected. The solution can be given in the debate that as: The global and Indian rules pertaining to data protection are changing quickly. New rules that will expand people's rights and improve the national information security agencies' ability to enforce them are being implemented in India. If controllers attempt to compromise the data, they will be held accountable. In the worldwide economy, personal data is constantly being collected, retrieved, and saved in several places across various countries. As a result, businesses should abide by the regulations that various countries have put in place regarding data exportation. Regardless of the size or makeup of the company, privacy regulation applies to all sectors and organizations.

Stated differently, violating someone's privacy is illegal and hence a serious act. [3]Start-ups primarily leverage the personal information of customers. If a data-driven start-up violates someone's privacy, it is a major crime since the dataset may include personal information on several people. This may have disastrous effects on any firm and will incur penalties. The confidentiality of an entrepreneur's start-up concept might be seen as the second viewpoint to this topic. One of an entrepreneur's most crucial needs is a start-up concept, particularly if they operate in a coworking space. It's a hard job at a coworking space to keep your ideas safe from other ambitious business owners. [2] When many business owners from various backgrounds share an office space, it's known as coworking space or consumer space. This arrangement lowers overall costs and improves convenience since everyone uses the same utilities, equipment, and infrastructure. Although this area offers many advantages, there is also a serious drawback, namely privacy violations. No matter what the situation, entrepreneurs must always prioritize protecting their privacy. The following are the risks an entrepreneur runs when operating under this arrangement:

Idea stealing – Idea stealing is one of the most common problems that can be faced by entrepreneurs working in a consumer space. Let us just think if someone has a great idea for a start-up and this idea may be something useful in future and may earn success then it is very obvious to assume that others will want to get their hands at getting some of that success. When people are working in consumer space arrangement where every individual entrepreneur is working on something under same infrastructure then it is pretty obvious that someone is bound to have taken some interest in someone else's idea for a start-up and that can be catastrophic for the individual who is working on that idea.

Big players – Large enterprises are basically becoming small when they are looking for cyber security for their companies. They are becoming small obviously not in their status but when they are looking for other companies to provide them with cyber security. Large enterprises are looking for small start-up companies to provide them with this facility. At a glance it looks like a good opportunity for start-up companies but for the entrepreneurs who are determined to establish their own company this can be threat because if a large scale company likes your start-up plan then they may propose you to work for them and if denied they may use other means to use your idea. This way privacy can be breached.

Internet and data safety – Data breaches and malware attacks are one of the main problems that is faced by organizations all around the world. Consumer spaces or co working spaces attracts different types of individuals like cooperate clients, freelancers, aspiring entrepreneurs, and it just takes a one malicious user to compromise the data of hundreds. Therefore, it is a priority to ensure that your data is well protected.

Privacy Or Personal Space:

To understand the response to this question, let's look at a scam that the large company Facebook pulled out. [7] This company was involved in scandals, scams, and data breaches in 2019 when the private information of about 42 million members of Facebook and 49 million members of Instagram was found and made public on online databases. According to a study conducted by a patrioticist and cybersecurity investigator, 276,140,456 users of Facebook's titles, user IDs, and phone numbers were among private information found in a website's database. This data may be easily accessed online by any nameless user without the requirement for a password or other form of authentication, which makes it vulnerable to fraud and SMS spam. After learning about the situation, security expert Bob Diachenko contacted the Internet service provider (ISP) and asked them to remove the IP (Internet Protocol) of these information from the servers. prior to the Internet

Service Provider (ISP) might restrict accessibility to the data, yet, the record including millions of individuals was already known to the public for roughly two weeks. It was also found that this data, which was also shared on hacker discussions, was accessible to everyone with an internet connection.

When Diachenko said that "the thieves might have attacked a vulnerabilities in Facebook's App Programming Interfaces (API)," he went into additional detail about this occurrence. Additionally, he said that it's possible that hackers obtained this information without even using Facebook's App Programming Interface (API) information from “Publicly visible profile pages”. Facebook said that it was looking into this incident in response. "We are investigating into possible problems with this occurrence, but we believe it must have occurred before we made improvements to protect user data."

This incident shows how detrimental it can be for both the consumers and the company when personal information is compromised or leaked. This sensitive information might be used in many risky situations. For instance, certain terrorist groups could use it to fabricate identities, putting not just our country but also the person whose real identity is being stolen at risk. Furthermore, the authorities would take harsh measures, such large fines and long jail sentences, if the firm engaged in such schemes. For the aforementioned problem, Facebook was had to pay the Privacy Commissioner's Office back for fines totaling around $5 billion. The implications of such situation may be quite challenging for a new company, particularly when we consider that a little firm was the source of the same type of issue. The hefty penalty associated with these disputes would be expensive for a small, beginning company. As a result, start-up companies that depend significantly on data should exercise extra caution when it comes to data protection. Insolvency may result for anybody convicted of exploiting or breaching another person's private information.

Some solutions:

Startups can protect their privacy in number of ways [1]:

Information technology must be visible and aware – Company must always make IT visible and aware about what the employees are doing with the company data, where the data is stored and what type of tools are being used. Sharing and syncing of data must be done regularly.

Create data security policies – Every start-up company should establish some data security policies that include all kinds of norms that describe how the files should be shared. Hackers and cyber criminals mostly target small scale companies because many of them do not give importance to these issues and don’t tackle them properly.

Training of employees – Priority for any company let it be small scale or large scale should be to train their employees that can defend any sort of cyber-attack and can prevent any sort of data to be stolen from the company’s dataset. Significant time and money should be used to train employees.

Encryption – One of the most effective and efficient way for a start-up company to protect is data and information is to use encryption. Encryption information is very cheap but is very effective. All the sensitive data and personal information like credit card numbers, email IDs, phone numbers, etc. should be encrypted.

Penetrating testing – This technique should be used by start-up companies as it can protect them from data breaches. Number of penetrating tools can be bought at a cheap price, so this technique also comes in handy.

If a start-up company opts for all the methods that are mentioned above, then the company will most likely prevent all the breaches and will be able to protect its private information and data from cyber criminals.

Protection of Privacy:

Jumbo – Jumbo, an application for iOS and Android, propelled in 2019 with the guarantee that it would slice through the problem of privacy of consumers. The offer was straightforward: download the application, check a couple boxes and it would naturally secure your protection settings on stages including Facebook, Google, Twitter, and Amazon. Instead of chasing down each individual inclination screen and interpret which settings were harmless and which were just intentionally stated to sound harmless, the application would do it for you.

Conclusion:

We may infer from the aforementioned report that one of the major threats to client start-ups is security. After reading the article, we gained an understanding of how important privacy is to cyber security and how it may ruin a person's life if ignored. We gained an understanding of consumer space, start-ups, privacy, and the relationship between the two. When we discuss this issue, we should pay particular attention to these concepts and their relationship. Additionally, we discovered why privacy matters so much to startups. We approached it from two distinct angles: first, from the standpoint of the user, explaining why it is so crucial to safeguard their personal information, and second, from the viewpoint of the business owner, outlining the privacy issues that arise when they operate in the consumer sector. Additionally, we learned about the potential consequences of user privacy breaches and the problems that might arise in the future for both the customer and the company itself. We discovered the controversy involving the major corporation Facebook. After knowing about this story, we realized that the consequences of these hacks and leaks might be disastrous for all parties concerned, and that the punishments meted out to those who commit these crimes may end up ruining their whole life. Finally, we comprehended how startups may safeguard their privacy. Thus, it is reasonable to assume from reading this report that one of the largest risks facing a start-up in the consumer area is privacy. Thus, if ambitious business owners want to be successful with their beginning product or service, they need pay close attention to the security of both their own and their users' data.

References:

Pooja H. Ramchandani (2017), A descriptive study of opportunities and challenges of Startup India Mission, Vol-2 Issue-3, ISSN(O)-2395-4396, Pg-61-65. C-1440 www.ijariie.com

Shailja B., Vivek S.(2016). Startup India- New Opportunities for the Entrepreneur, 3rd International Conference recent Innovations in Science, Engineering, and Management, Conference Proceeding, Pg-1473-1476.

Badra,Shailja, and Sharma,Vivek(2016).Startup India- New Opportunities For The Entrepreneur: International journal of Science Technology and Management (IJSTM). Vol.5, Issue1. ISSN: 23941537 2.

Andaleeb, Uruba,Singh, S.D. Dr. (2016). A study of Financing Sources for Start-up Companies in India: International Review of Business and Finance Volume 8, Number 1. ISSN 0976-5891.

Report title “Start – Ups: What You Need To Know” (2016) by Nishith desai associates. Mumbai.

Wagh, Madhura (2016). Government initiative for Entrepreneurship development – Start up India Stand up India: IRACST – International Journal of Commerce, Business and Management (IJCBM),.Vol. 5, No.1, JanFeb 2016. ISSN: 2319–2828.