SCHOLEDGE International Journal of Business Policy & Governance
ISSN 2394-3351, Vol.06, Issue 3 (2019)
Pg 25-29.
DOI: 10.19085/journal.sijbpg060301

Published by: SCHOLEDGE Publishing
www.theSCHOLEDGE.org
Email: editorial@thescholedge.org

Digital Entrepreneurship vis-à-vis Managing Customers' Data: Available Ways & Means to Protect the Online Presence of the Businesses

Sunil Sharma
Fellow, The Institute of Company Secretaries of India, New Delhi, INDIA.

Abstract
The modern day businesses are having an inevitable online presence to ensure to grab every possible opportunity to do business. Even the businesses who do transact purely offline are also having their online presence by having their business websites. And those businesses which have an entire gamut of their services or digital products to offer only via online channels have to ensure near to perfect online set-ups to stay in the businesses. Online businesses receive thousands of gigabytes of data from their users or customers on a daily basis altogether. This data contains specific information about the geographics of the users, their financial information, KYCs, their investment and other key profile based data. What will happen if that enormous data lands in the hands of some unscrupulous people? The user and customers' data will get compromised affecting them negatively. Many of the users may incur financial losses due to that mishandling of digital data. And last but not the least, the digital businesses will have all the possible dents of bad reputation leading to even boycott of their businesses by the users on a massive scale. All this is sufficient to shatter the dreams of the digital entrepreneurship. This paper seeks to point out how the digital entrepreneurs can better identify key data of their users and customers, how they can keep safe custody of that data and how to manage and protect the confidentiality of the users and customers.

Keywords: Digital Entrepreneurship, Digital Data, Data Protection, Web Threats, Managing Data

Why the Users' Data is Important?

Like every other business, the digital (online) businesses do also have their own relativity with their users' data. In fact, for digital businesses, the most important segment of the business's marketing strategy is its users' data. With users' data in hand, the digital businesses are sometimes more successful in winning businesses in comparison to even more established businesses with no or lesser data of their users.

Users' data presents a huge opportunity to learn and unlearn lots of the things which the users or customers were appreciating or criticizing. With users' data, digital entrepreneurs can form more concrete and well-informed decisions about the ongoing and future offerings of their business.

By users' data, they have the opportunity to categorize their offerings' market on geographical, financial, cultural and social acceptance levels. They can identify their most promising category where they would like to work more aggressively and to learn to excel in the market categories where could not perform so well in the past. So, in one line answer, the data is business.

Cases from the Recent Times

Case of Facebook

Following media alerts, Facebook in April 2018 confirmed that personal data of nearly 87 million of its users have been improperly shared with a third party, a consultancy firm Cambridge Analytica.[1] In April 2019, again it is Facebook making a headline on the same tune. A security analysis firm, UpGuard has claimed that nearly 146 gigabytes of 540 million records containing likes, comments, tags etc have been compromised this time again via a third party, Cultura Colectiva, a Mexico based media consultancy firm.[2]

Reaction

There have been consequences for this mishandling of data by Facebook. Many parliaments across the globe have directed Facebook to be present before their parliamentary committees to clarify why their services shouldn't be banned in their regions. It has been a very tedious and hard task for the Facebook to convince the governments worldwide that it will address to all the security risks and do its best to protect its users' data from any security breach.

The users, advertisers and other civil society organization worldwide have criticized Facebook for the recent data leaks though via third parties.

[1] Facebook says data leak hits 87 million users, widening privacy scandal. Retrieved from https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM

[2] Losing Face: Two More Cases of Third-Party Facebook App Data Exposure. Retrieved from https://www.upguard.com/breaches/facebook-user-data-leak

Case of Google+

In October 2018, the private data of nearly 52.5 million Google+ users have been exposed via an API bug as admitted by Google.[3]

Reaction

Google had to force the scheduled closure of its social platform, Google+ even before the pre-notified dates. Many have blamed and criticized Google for hiding the data breach information for long.

Lesson

What we learn from the above-mentioned cases is that even the major players in the market had to suffer much from their data breaches. What will happen if it occurs with relatively smaller and new digital businesses? They may probably lose their businesses entirely.

Way & Means of Data Management

Implementation of Data Encryption

The digital businesses must have to have systems in place to encryption the data of their users and customers. Implement state of art encryption technologies. Having an SSL is a must for the websites processing online payments and hosting e-commerce businesses. The digital entrepreneurs need to make sure that they regularly scan their web properties for identifying and detecting any possible vulnerability. Pre-scan the data what the digital businesses want to host on to their data servers. For this, effective anti-virus software can come handy to run a local scan.

Users' Awareness

The users of digital businesses are the most vulnerable if they don't have digital hygiene with them while transacting online. The digital business need to make it clear to inform its users about the good habits of digital hygiene like frequently changing passwords, having secure passwords, using Two Factor authentication when it is available, to not to use password protected services on public systems, if they need to, make them aware to securely log-off from the service when they leave that particular public system.

Have Transparent Privacy Policy

Having a privacy policy is a must nowadays. Post implementation of GDPR by EU in 2018, it is mandatory to have one if your offerings have a market in the EU region.[4] Mention in clear terms that what data the digital businesses need to receive and how that

[3] Google will shut down Google+ four months early after second data leak. Retrieved from https://www.theverge.com/2018/12/10/18134541/google-plus-privacy-api-data-leak-developers

[4] The GDPR Regulations. Retrieved from https://eugdpr.org/the-regulation/

DOI: http://dx.doi.org/10.19085/journal.sijbpg060301

data will be used. What measures are or will be adopted to keep that data protected. In case of a data breach, proactively notifying users and customers has become a responsibility now. The digital businesses need to assist its users to facilitate them to get their data removed from the servers if the users request for the same. All this reposes confidence among the users and customers that they have been well-taken care off to the best efforts of the businesses with which they have a business relationship.

Offline Data Backup

The digital businesses need to keep a local offline regular backup of the server data for its usage in case of web lock-outs or in a security scenario. The businesses also need to keep the local data in closed and restricted access to avoid an insider data leak.

Data Breach? What to do?

As per GDPR Regulations, the digital businesses having customers from EU regions, if come across a data breach, need to notify to their EU users and customers within 72 hours of the data breach awareness.[5] Non-EU region customers and users are also getting similar rights based on various local data privacy laws and regulations. So, it will be equally fair to notify every customer and users about the data breach.

Now, the users and customers should be advised by the breached businesses as to what should be done on their part (customers/users) to help them (businesses) to make the data breach ineffective. Digital businesses should proactively take the data control and make their web properties work as usual. The entire server data should be scanned to do away any infected data.

Conclusion

The users' and customers' data is an asset for any digital business. And it should be taken care off just like other business assets. At the same, users' data is also a liability which a digital business needs to take care off on a regular basis. The higher the confidence of the users and customers, the longer their relations will be with the businesses. The users' data shouldn't be taken for granted and should in all possible circumstance be used for effective business planning, marketing strategies and in reaching out to the users on an ongoing basis. The threat to the users' data is a threat to the business. In this, both the users and the businesses have their own roles to play to ensure a safe and secure digital space. And these roles should be complemented with mutual interests.

References

[1]. Facebook says data leak hits 87 million users, widening privacy scandal. Retrieved from https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM

[5] Breach Notifications, The GDPR Regulations. Retrieved from https://eugdpr.org/the-regulation/

[2]. Losing Face: Two More Cases of Third-Party Facebook App Data Exposure. Retrieved from https://www.upguard.com/breaches/facebook-user-data-leak

[3]. Google will shut down Google+ four months early after second data leak. Retrieved from https://www.theverge.com/2018/12/10/18134541/google-plus-privacy-api-data-leak-developers

[4]. The GDPR Regulations. Retrieved from https://eugdpr.org/the-regulation/

[5]. Breach Notifications, The GDPR Regulations. Retrieved from https://eugdpr.org/the-regulation/

DOI: http://dx.doi.org/10.19085/journal.sijbpg060301