Data protection in a growing tech economy

pwc

Contents

"The eye of Sauron the terrible few could endure"- J. R. R Tolkien, The Lord of the Rings

The above quote always gets me thinking – could the cloaked hacker be the digital age's roving Eye of Sauron? Like Sauron, the hacker is watchful and omnipresent, waiting for an opportunity to steal and misuse your data. With technology-based start-ups transitioning into unicorns, the focus is on creating a unique feature set which captures the imagination of the consumer and helps the start-up grow. Five broad trends related to the growth story of tech start-ups are discussed below:

1

India is home to the third largest number of unicorns worldwide

As per recent NASSCOM and Economic times reports, India has 25 unicorn start-ups today, 15 of which were added in 2018. The number of unicorns is expected to touch 35 by 2020 and grow to 55 in 2024. Currently, India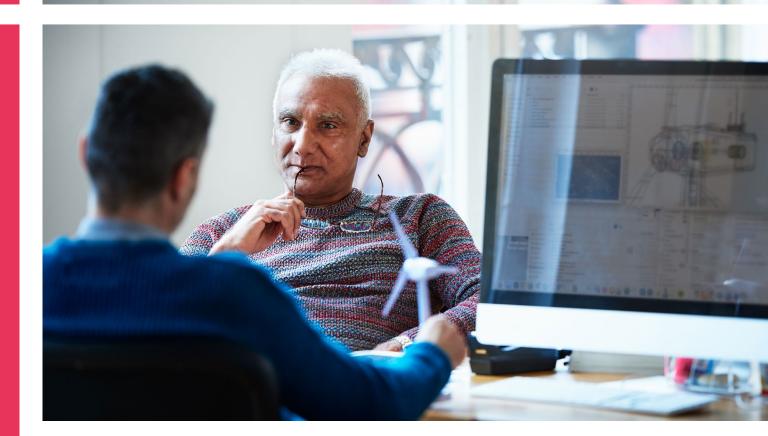 has the third highest number of unicorns worldwide (25 out of around 430), after China and the US.[1] While there has been a gradual increase in B2B-based start-ups, the overall market share of B2C start-ups has remained steady.

---

1 NASSCOM and Economic Times
https://www.nasscom.in/sites/default/files/Industry-Performance2018-19-and-what-lies-ahead_0.pdf
https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/54-tech-unicorns-expected-in-india-by-2025/articleshow/70481870.cms
https://www.business-standard.com/article/companies/india-picks-up-pace-in-producing-unicorns-8-new-startups-join-2018-club-118102501079_1.html

2

Consumer data is the fuel for start-ups, but is there consent

Analytics and artificial intelligence (AI) are the engines driving start-ups. Naturally, to learn consumer behaviours and predict their activity, these start-ups need to collect, store, analyse, process, share and even collaborate on massive volumes of data. What is missed in this race for data acquisition is consent. The individual's decision to share personal information may not be either explicitly or implicitly captured. Even if consent is captured, there is always the question of whether the consumer has provided the same knowingly or if it is lost in fine print. The need to share and collaborate across platforms and technology ecosystems has resulted in digital replicas of consumer information lying on multiple platforms. Although the aim of such duplication may have been to provide relevant information and recommendations to the end user in terms of services (e.g. e-commerce sites), consent for such data sharing is often not obtained, giving rise to a phenomenon called privacy poisoning.

3

The feature vs security conundrum

Technology unicorns are constantly adding to their functionalities in a bid to offer unique first-to-market consumer propositions. Developing these features entails collection of more consumer data (to drive the analytics and AI engines). The constant need to add use cases amplifies the level of risk. Moreover, the need for speed motivates unicorns to collaborate with third parties and/ or freelancers, resulting in an added element of vendor risk. This race to gain the first-mover advantage sees unicorns often making their security programmes the lowest priority. Security is often seen as just a compliance activity rather than a value enabler, which leaves unicorns susceptible to data breaches.

4

The proverbial 'tick in the box'

With data protection being relegated to the bottom of the priority pyramid, regulators globally have stepped in to enforce data protection regulations and guidelines. Some examples of these are the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR) and India's Personal Data Protection (PDP) Bill. The aim is to make companies more responsible by not stopping at compliance and extending accountability to every stage of data collection. Despite these laws, data protection is still seen as merely a compliance activity with the focus on implementing the 'bare minimum' needed to get satisfactory assessment/audit outcomes. A survey byINC magazine revealed that that 60% of small businesses fold within 6 months of a data breach or cyber attack. This worrying finding underlines the fact that data protection, despite regulatory guidelines, is not high on the priority list- irrespective of organization size

5

No one is safe

Data breaches are rather common in today's evolving technology landscape. Massive enterprises that have dedicated security programmes have also fallen victim to data breaches, which are generally the result of improper execution of identified security measures. Such breaches have a direct financial impact, either in the form of regulatory fines or loss of market value.

The misplaced security priorities of unicorns can lead to a loss of competitive advantage. Consumer data and insights are one of the sources of a unicorn's competitive advantage, and theft of this data by a potential competitor

could deal a crippling blow to a unicorn and strip it of the value it was aiming to create.

In conclusion, consumer data is the energy that powers unicorns. However, in a bid to be the first in the market, unicorns often neglect their security programmes, which leaves them vulnerable to data breaches. It is important that unicorns recognise the criticality of data protection and implement the necessary security measures with the dual aim of reassuring consumers and maintaining a competitive advantage, rather than just looking to comply with regulations and avoid financial penalties.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2019 PwC. All rights reserved.

Authors

Siddharth Vishwanath
Leader – Cyber Security
PwC India

Avinash Iyer
Associate Director- Cyber Security
PwC India