Announcements

IBM Future of Identity Study Finds Millennials Disrupting Digital Identity & Authentication

• Indian respondents are more technology-inclined compared to their global counterparts

• Respondents in India are more knowledgeable and receptive to biometric authentication

• Young adults lax on passwords, more comfortable with biometric and multifactor authentication

Bengaluru - 29 Jan 2018: IBM Security today released a global[1] study examining consumer perspectives around digital identity and authentication, which found that people now prioritize security over convenience when logging into applications and devices. Generational differences also emerged showing that younger adults are putting less care into traditional password hygiene, yet are more likely to use biometrics, multifactor authentication and password managers to improve their personal security.

With millennials quickly becoming the largest generation in today's workforce,[2], these trends may impact how employers and technology providers provide access to devices and applications in the near future. Overall, respondents recognized the benefits of biometric technologies like fingerprint readers, facial scans and voice recognition, as threats to their digital identity continue to mount.

Key India findings include:

• Respondents in India are most comfortable using new technology (86% vs. 73% Singapore and 66% Australia)

• Indian respondents (43%) are far more likely to use a password manager than those in Singapore (24%) and Australia (21%)

• Respondents in India use 8 passwords on average (vs. 9 globally)

• When it comes to online marketplace apps, Indian respondent equally prioritize convenience (42% and security (44% while globally security (54%) outweighs convenience (32%).”

• 82% of respondents in India (versus 69% globally) are willing to use more than one password/way for authentication

• Related to the work environment (and compared to the global average) Indian respondents see more of the benefits of biometric authentication, and are more likely to agree it would be helpful to access their work computer/laptop by using a finger/hand print (86% vs. 70% globally), or facial/retina (eye) scanning (77% vs.

59% globally)

The IBM Security: Future of Identity Study surveyed nearly 4,000 adults from across the U.S., Asia Pacific (APAC) and Europe to gain insight into consumer viewpoints around authentication. Some key findings from consumers include:

- **Security outweighs convenience:** People ranked security as the highest priority for logging in to the majority of applications, particularly when it came to money-related apps.[3]
- **Biometrics becoming mainstream:** 67 percent are comfortable using biometric authentication today, while 87 percent say they'll be comfortable with these technologies in the future.
- **Millennials moving beyond passwords:** While 75 percent of millennials[4] are comfortable using biometrics today, less than half of are using complex passwords, and 41 percent reuse passwords. Older generations showed more care with password creation, but were less inclined to adopt biometrics and multifactor authentication.
- **APAC leading charge on biometrics:** Respondents in APAC were the most knowledgeable and comfortable with biometric authentication, while the U.S. lagged furthest behind in these categories

The evolving threat and technology landscape have created widely-known challenges with traditional log-in methods that rely heavily on passwords and personal information to authenticate our identities online. In 2017, data breaches exposed personal information, passwords, and even social security numbers for millions of consumers. Additionally, the average internet user in America is managing over 150 online accounts which require a password, which is expected to rise to over 300 accounts in coming years. [5] "In view of the multiple cyber theft and breach scenarios, our personal identification data is no longer fully secure. As consumers realise that passwords may not suffice to fully secure data and prioritise security over convenience, the time is ripe to adopt advanced and multi-layer security strategy", said Kartik Shahani, Integrated Security Leader, IBM India & South Asia

Future of Identity

Analysis in the report by IBM Security details that attitudes regarding authentication vary widely, and while acceptance of newer forms of authentication like biometrics is growing, concerns persist – particularly amongst older generations and people in the U.S.

IBM advises organizations to adapt to these preference by taking advantage of identity platforms that provide users with choices between multiple authentication options – for example, letting users toggle between a mobile push-notification which invokes fingerprint readers on their phone, or a one-time passcode. Organizations can also balance demands for security and convenience by using risk-based approaches that trigger additional authentication checkpoints in certain scenarios, such as when behavioral cues or connection attributions (device, location, IP address) signal abnormal activity.

The data also reveals that younger generations are placing less emphasis on traditional password hygiene, which poses a challenge for employers and businesses that manage millennial users' access to data via passwords. As millennial and Gen Z employees begin to dominate the workforce, organizations and businesses can adapt to younger generations' proclivity for new technology by allowing for increased use of mobile devices as the primary authentication factor, and integrating approaches that substitute biometric methods or tokens in

place of passwords.

IBM Security provides tips for consumers on how to secure their digital identities in a blog post here.

For additional details on the study and advice for companies to prepare for the future of authentication, download the full report at: ibm.biz/FutureOfIdentity

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and has been granted more than 3,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @ibmsecurity on Twitter or visit the IBM Security Intelligence blog.

About the Study

The study was designed with Ketchum Global Research and Analytics. Data collection was conducted by Research Now. The survey was conducted between October 21 and November 5, 2017, with a margin of error of +/- 2.0 for the U.S. sample and +/- 3.07 for the EU and APAC samples, at the 95% confidence level.

The 15-minute online survey totalled responses from 3,977 adults across the United States (U.S.), European Union (EU) and Asia-Pacific (APAC) regions, including:

- U.S.: 1,976 respondents
- EU: 1,004 respondents (United Kingdom, France, Italy, Germany, Spain)
- APAC: 997 respondents (Australia, India, Singapore)

###