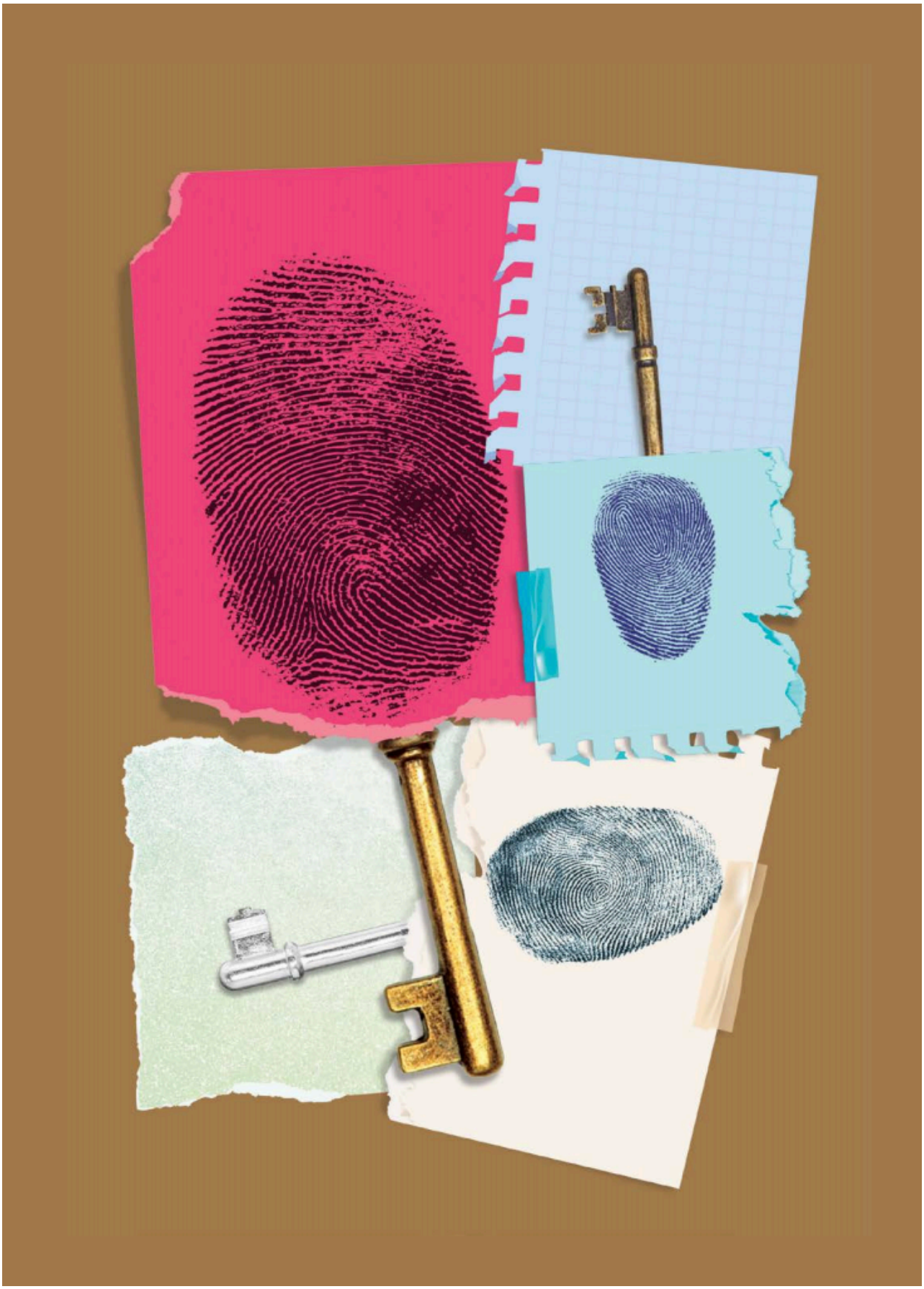
BYPASSING THE Pa55w●rd

Rising cybersecurity threats have opened up a huge market for companies offering passwordless authentication services

BY **NIDHI SINGAL**
ILLUSTRATION BY **RAJ VARMA**



IT TAKES INDIAN ORGANISATIONS nearly 228 hours, or nine-and-a-half days, on average to detect a cybersecurity breach, nearly double the global average of 117 hours, according to a survey by US cybersecurity firm CrowdStrike last year. Couple that with the fact that about 75 per cent of Indians — the highest among all countries — surveyed admitted their organisation suffered a ransomware attack in the last year, and it paints a dismal picture of the state of digital security in Indian companies.

It's not too surprising then that nearly every other day there is news about a cyber incursion. This year's list alone includes confectioner Haldiram's, hyperlocal concierge service Dunzo, Air India, and e-grocer BigBasket.

One of the easiest ways to infiltrate an enterprise's computer network is through an employee's account. Or more specifically, through password phishing. IBM's Security X-Force survey showed that 82 per cent of the 22,000 global respondents reuse their email and password combinations. While this makes it convenient for one to access multiple accounts, it is a bane for enterprises when the practice spills over into the workplace. And rather than sending out periodic reminders to employees to adhere to digital security protocols, enterprises are increasingly opting to minimise the employee's role in the security equation.

Enter passwordless authentication. This technology verifies a user account using a combination of more secure authentication factors such as a fingerprint, PIN, device specifications or its location, and digital tokens, among others.

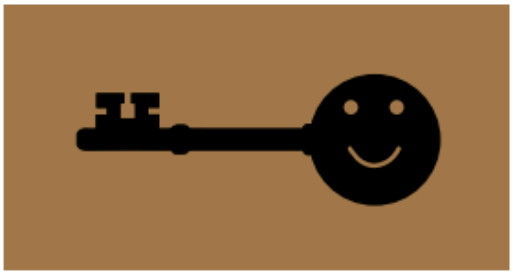
"It is perfectly safe to use passwordless authentication, and it can even be safer than the traditional username/password approach," says Mark Risher, Director of Product Management, Identity and User Security, Google. The tech behemoth has adopted a passwordless authentication standard called FIDO, or Fast Identity Online, for its employees and temporary vendor base globally. "Since doing that in 2017, we've had zero cases of password phishing. We have since been working on ways to roll this out for our users externally," says Risher.

The need for a robust security system became even more pressing during the Covid-19 pandemic that forced almost every single white-collar employee to work from home. Employee accounts are more vulnerable outside the protected confines of a company's internal network. As it was for Infosys, whose data-centre security didn't support the dispersion of employees. The company switched to Cloud connectivity and adopted a zero-trust framework, including passwordless authentication and certificate-based authentication of devices, for all its employees.

While still in its nascency, the passwordless authentication market was estimated to be worth $35.5 billion globally in 2019, according to Next Move Strategy Consulting. As more and more companies adopt the technology, the research firm expects the market to explode to top $450 billion by 2030, at a 29 per cent compounded annual growth rate (CAGR) from 2020. Meanwhile, Gartner estimates that by next year, 60 per cent of large enterprises and 90 per cent of mid-sized ones globally will implement passwordless authentication in over half of their use cases.

None more so than Indian companies. "By 2030, India is expected to lead the growth of passwordless authentication in the Asia-Pacific market along with China and Japan," says Vishak Raman, Director, Security Business, Cisco India & SAARC. The adoption, he says, will be given a huge fillip by the pervasiveness of smartphones with in-built facial and/or fingerprint recognition technology.

Cisco has deployed a zero-trust architecture for all its employees globally and their 120,000 managed devices, enabling them to access on-premise and Cloud applications without using a virtual private network (VPN). It has also helped a power station in India transition to secure, remote work quickly and seamlessly using its technology, including a solution that uncovers malicious domains, IPs, and URLs even before they are used in attacks.



GLOBAL PASSWORDLESS AUTHENTICATION MARKET

$35.48

BILLION IN 2019

$456.79

BILLION BY 2030

CAGR of 29.1% from 2020-2030
Source: Next Move Strategy Consulting

PASSWORDLESS AUTHENTICATION IS BEING ADOPTED BY FINANCIAL, IT, TELECOM, RETAIL AND HEALTHCARE COMPANIES AS WELL AS BY SOME GOVERNMENT SERVICES, SUCH AS AADHAAR

Open Sesame

For nearly six decades, passwords have been the key to unlocking any online account, at work or at home, as well as access applications, on the Cloud or on the phone. However, what was once a security barrier to protect against a hacker has almost become a gateway for them. And this not only because people tend to use easily hackable passwords, but also because it is difficult, nigh impossible, for an organisation to differentiate between an employee and a hacker. That has forced the rise of passwordless authentication, with a much more secure process involving multi-factor authentication.

But it is not as if multi-factor authentication is brand new. In fact, two-factor authentication has been an option for many years on several email accounts. Moreover, using any combination of a password, PIN or biometric along with a one-time password (OTP) is widely prevalent, and even necessary, for most consumer apps, especially financial ones. However, this still requires a human to do all the legwork. What passwordless authentication aims to do is remove as much of the human element as possible.

"This type of authentication requires two or more verification factors that are secured with a cryptographic key pair to sign in. The device creates a public and private key when registered," explains Irina Ghose, Director, Cloud Solutions, Microsoft India. The private key can only be unlocked using a local gesture such as a biometric or a PIN, while the public key is an encryption, like a large numerical value, that is either software-generated or provided by the organisation and made available to all employees.

Any system is as strong as its weakest link, which is the employee in most enterprise security systems. This has become all the more glaring, and exploitable, as an increasing number of people work from home.

"We saw once we shifted to work from home on remote access technologies, the weakest link was the passwords that you needed to access your network," says Neehar Pathare, Chief Information Security Officer and Vice President, Information and Communications Technology, 63 Moons Technologies. "With today's social engineering skills, it's not very difficult to get a user's passwords. We needed an additional layer of security." This layer, for the Mumbai-based financial services firm, was deploying passwordless authentication ranging from basic Windows authentication for terminals using Azure to Citrix remote access solutions.

As passwordless authentication not only offers a secure login environment, but also eliminates weak and bad actors, it is being increasingly adopted by Indian financial, IT, telecom, retail, and healthcare companies as well as by some government services, such as Aadhaar. This growth is being driven by digital transformation initiatives, the alignment with zero-trust initiatives for

> By 2030, India is expected to lead the growth of passwordless authentication in the Asia Pacific market along with China and Japan. Growing penetration of smartphones and technologies such as facial and fingerprint recognition will be significant factors"

VISHAK RAMAN, Director, Security Business, Cisco India & SAARC

> Most organisations already use basic identity and access management (IAM) systems for both their employee and customer authentication needs. Most passwordless authentication technologies can be deployed on top of existing IAM systems"

VISHAL KAMAT, Director, IBM Security, IBM Software Labs, IBM India

digital identity, the adoption of a decentralised identity model, as well as the need to bolster defences against ever-rising, more sophisticated cyberattacks.

"Overall, the growth in the adoption of passwordless technologies is going to accelerate in the next three-five years ... with the adoption of stronger authentication standards," says Vishal Salvi, Chief Information Security Officer and Head of Cybersecurity Practice, Infosys.

Penny Wise, Pound Foolish

Bad actors need to gain access to a company's network only once to create havoc that could cost the company dearly in the form of hefty regulatory penalties and millions of dollars in ransom. The CrowdStrike survey revealed 34 per cent of Indian organisations paid between $1 million and $2.5 million in ransom in the last 12 months. Besides, a compromised company also pays an intangible price as they lose brand image and client trust. In that light, any expense on passwordless authentication offers a tremendous return on investment. However, not everyone sees it that way.

"Most companies hesitate to reassess their security systems either assuming a 'this-could-never-happen-to-me' mentality or are intimidated by the thought and presumed cost of implementing a new system. This is a misconception," says Siddharth Gandhi, COO, Asia Pacific, 1Kosmos, a cybersecurity solutions provider. "Passwordless and biometric technology can be easily integrated into enterprises of any size for flat yearly fees and can be built upon as the necessity grows. Rather than patch-working existing systems, organisations can build their passwordless authentication from the ground up without extensive retraining or implementation costs," explains Gandhi.

New Jersey-headquartered 1Kosmos has deployed its BlockID platform at Hitachi Systems Micro Clinic, a system integration company that itself sells security solutions to Fortune 500 companies in India. All of its 2,000 employees are using passwordless authentication for various software such as Windows, ERP, and all web-based or intranet applications. "Passwordless authentication not just takes care of all our headaches in terms

“Passwordless and biometric technology can be easily integrated into enterprises of any size for a flat yearly fee and built upon. Organisations can build passwordless authentication from the ground up without extensive retraining or implementation costs”

SIDDHARTH GANDHI,
COO-Asia Pacific, 1Kosmos

THE BIG USERS

Google has deployed FIDO (Fast IDentity Online) for its employee- and temporary vendor base; it has not seen any case of password phishing after this

Hitachi Systems Micro Clinic has deployed Block ID for biometrics (by 1Kosmos) for all 2,000 employees in India

Cisco has implemented zero-trust architecture organisation-wide (including 120,000 managed devices) to access on-premises and Cloud applications without connecting via VPN

63Moons is using this for basic Windows authentication

of remembering credentials and passwords, it also fits in very well from the security viewpoint. We are working on deploying the service for the entire Hitachi Group,” says Anuj Gupta, CEO, Hitachi Systems Micro Clinic. Gupta also plans to roll out passwordless authentication to its customers.

Forget the cost of a breach, it is already quite an expensive proposition to maintain the robustness of the most basic of defences: resetting passwords. Every time an employee does so — due to a periodic requirement or because they have forgotten their old password — the company incurs a soft cost and a hard cost. The hard cost is the time an IT department takes to reset a password, while the soft cost is the lost productivity while an employee remains locked out of the system. And these costs add up.

For instance, Microsoft estimated it lost productivity worth $6 million and spent $3 million in hard costs before it switched to passwordless authentication. Today, about 90 per cent of its employees globally sign in to corporate systems, resources, and applications sans a password. “As a result, we have reduced hard and soft costs by 87 per cent,” claims Ghose of Microsoft India. She adds, “As our costs go down, the attackers’ costs go up, and Microsoft is less of a target.”

Besides, there is little to no hassle in adopting passwordless authentication as most hardware products today already use some form of biometrics recognition. “Most organisations already use basic identity and access management (IAM) systems for both their employee and customer authentication needs. Most passwordless authentication technologies can be deployed on top of existing IAM systems,” says Vishal Kamat, Director, IBM Security, IBM Software Labs, IBM India.

All said and done, companies can no longer afford to consider security tools such as passwordless authentication as “nice to have” accessories. Neither can they avoid their adoption. To do so would tantamount to self-sabotage, and make them another statistic in the next cybersecurity survey. BT

@nidhisingal