SECURITY SPECIAL

# IT NEXT

NOVEMBER 2010 / RS. 75
VOLUME 01 / ISSUE 10

MEDIA FOR THE NEXT GENERATION OF CIOs

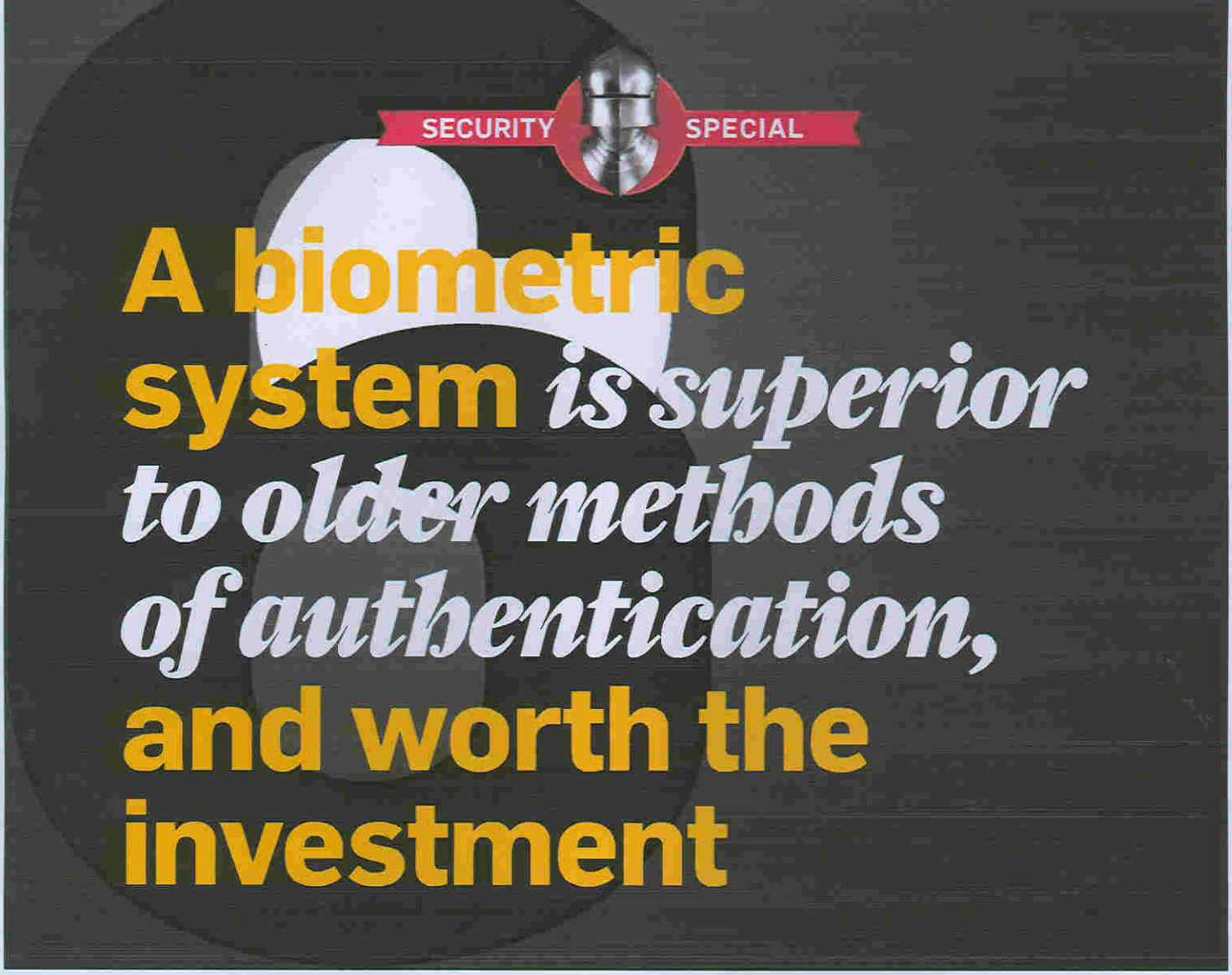


## ARE YOU *Really* *Secure?*

**Changing Nature Of Security Threats Could Endanger Your Vital Enterprise Assets.**

*Gird up for the battle*

A 9.9 Media Publication



SECURITY SPECIAL

# A biometric system *is superior to older methods of authentication,* and worth the investment

I'm sure most people reading this article have entered a data centre at some point in time. And I am quite certain that a lot of you have heard of 'Aadhar', the Indian government's initiative, for a unique ID programme for all citizens. What's common among all of them is security, which has been deployed and strengthened by the use of biometric systems!

## UNIQUE AND INDIVIDUAL...

'Biometrics' is derived from the Greek words 'bio' and 'metrics' and a literal translation of it is 'life measurement'. It is concerned with identifying a person based on his unique physiological characteristics. It does not rely on something you have (e.g. a credit card which has the potential of being stolen), or something you know (e.g. a PIN number which again can be stolen), but something you are (e.g. your fingerprint which is impossible to replicate / forge).

It is believed that each human being has a distinct fingerprint. Understanding the value of this fact early is perhaps what led to the invention of the fingerprint reader — the most common and cheapest biometric system available in the market today. Fingerprint recognition is perhaps the most mature of all biometric systems even today. Other biometric systems available today are palm scanners, hand geometry readers, retina scanners, iris scanners, voice print, facial scan readers, hand topography readers, among others.

## WHY IT IS SUCH A BIG DEAL...

Four main reasons can be cited, as to why biometrics is superior to older methods of authentication. Firstly, the possibility of two individuals sharing the same biometric characteristic is virtually not possible (i.e. it is unique). Secondly, a biometric property cannot be shared or duplicated. Thirdly, biometric systems are hard to forge, and finally, the biometric property of an individual cannot be lost (except in extreme rare cases, for example in case of a serious accident).

In businesses, biometric systems may not entirely replace older technology, but work in conjunction with the older systems. In the government sector, biometrics is deployed for applications such as national

*BERJES ERIC SHROFF, MANAGER-IT, TATA SERVICES.*

*"Biometrics does not rely on something you have or something you know, but something you are."*

security, homeland security, border control, enterprise and e-government services, and identity management initiatives, such as 'Aadhar', amongst others. Of course, government deployment of biometric systems for applications such as 'smart passports' are some of the other advancements we might see in the very near future.

In the private sector, biometrics is being used in data centres, warehouses, top nightclubs, access control systems in office buildings, etc. In warehouses and factories, deployment of a biometric system will eliminate the biggest manpower problem which affects productivity – 'buddy punching'. Workers won't be able to inappropriately enter time and labour data for each other, or replicate their colleague's fingerprints or retina and iris records, the way they could use a colleague's punching card to mark false attendance. In fact, many smaller organisations in India today, are deploying biometric systems for security, and also for attendance systems, which in turn is linked to their payroll system. Biometric products definitely provide an advantage over traditional access control methods. They ensure that the authorised user is present, in order for access to take place. The possibility of theft, as may very well be the case with passwords, PIN, access control cards, etc., is eliminated. The deployment of multimodal biometric systems is not uncommon today. This provides more-than-average accuracy and an added layer of security, because two different biometric systems are used, instead of one.

## CHALLENGES

Biometric systems are not completely hassle free, and like all other technologies, come with their share of problems. Also, the data read from biometric readers/scanners is as confidential/secured as the security extended to protect the servers on which this data is stored, from physical or logical compromise.

How do you determine if your organisation does need a biometric solution and how will you justify the Return on Investment (ROI), for it? If your needs and problems aren't identified, justifying the ROI for deployment of a biometric system is not easy.

## SOLUTIONS

Whether you are a government body or a private business concern, the first step is to identify your needs. Then, the trick is to not fall for a vendor's marketing spiel. Ensure that you check the vendor's reference with their customers, to make sure they are satisfied. Also, if you've identified that you do need a biometric system, identify which one will address your needs/ problems the best – it's not the case of one system fits all. A study will have to be conducted of the pros and cons of various biometric systems available, taking into consideration the cost factor involved. Also, if you're planning to marry the biometric system with another application, such as payroll being directly linked to the fingerprint reader, ensure that the hardware and software supports both applications.

Each biometric system has its own merits and problems, both in terms of technology and deployment (for acceptance by the users). But it still is far superior to older methods of authentication, and hence worth investing in. ITNEXT

## BIOMETRICS ON YOUR PHONE

New technology developed by scientists at the University of Manchester in the UK would allow for **mobile phones with front-facing cameras** to utilize facial recognition in lieu of traditional PINs, passwords or patterns for unlocking access to the phone or other protected applications and data contained on it, according to a Wired article. Eventually, it will be **able to tell who the user is**, where they are looking and even how they are feeling. Face verification is already used in laptops, webcams and the Xbox 360 Kinect but this is the first time the technology is being used with such sophistication in mobile devices such as smartphones.