BIZCOMMUNITY

Biometrics is booming - but is your solution really secure?

By Kobus Le Roux

4 Jul 2013

Biometric access control technology has experienced phenomenal growth in adoption in South Africa over the past few years, with an estimated 80% of all access control solutions using fingerprint readers and other biometrics to enhance security. The popularity of these solutions can be attributed to many factors, including the nature and size of many blue-collar workforces, for example in the mining industry.

Biometrics has also been adopted successfully in white-collar environments, preventing fraudulent access to buildings and areas where sensitive information is stored. However, simply installing a biometric access control solution and then failing to maintain the system can lead to security breaches and unnecessary risk. Maintaining both the hardware and software of these solutions is critical in mitigating risk across all areas, including security, operations, health and safety, and reporting.

Access control has long been used to ensure that only authorised personnel are permitted into buildings or in certain areas. However, card-based solutions are prone to fraud, as cards can easily be stolen or switched, giving the wrong people access. For this reason, biometrics has grown in popularity across all industries and sectors in South Africa. These solutions assist not only with preventing access, but also with time and attendance, and health and safety, ensuring that people are not permitted to access hazardous areas. They are also an aesthetically pleasing solution and can be integrated with CCTV solutions for a visual trail of access control.

The risk is cumulative over time

However, while these solutions are highly effective, failure of any component in the system will compromise the integrity of multiple areas of the business, which introduces risk, particularly if errors are not picked, as the risk is cumulative over time and the system may continue to degrade. The reality is that not enough emphasis is placed on the need to set up and maintain these solutions properly. Not only do the systems need to be set up, installed, integrated and configured correctly, they also, like any piece of equipment, need to be looked after. They are touched by hundreds of people every day and may be situated outside, exposed to the elements, so deterioration in the effectiveness of the reader is likely over time if proactive maintenance is not conducted. Aside from the physical aspect, the software and the database need to be kept up to date for optimal functionality.
When it comes to the set-up of biometrics systems, accurate registration of identifiers, such as fingerprints or irises, depending on the solution used, is critical. If this process is not completed correctly, or the process is faulty, the system will deliver false positives or erratically deny access. This can permit unauthorised personnel from accessing areas and prove frustrating for users who cannot access the areas they need, and also should access be routinely denied to permitted people, this can cause security to become lax and allow people in even if they are unauthorised.

A security threat to organisations

The database also needs to be proactively maintained on an ongoing basis, to ensure that registered personnel are kept up to date. This is particularly important in high-staff-turnover environments like contact centres. If, when staff leave the organisation, their information is not removed from the database, they will still be able to access the organisation. Similarly, if and when the status of employees change, altering the areas they are allowed to access, the database must be updated to ensure access control follows their profiles. If this is not done, it poses a security threat to organisations. Biometric databases also have a limit to the number of registrations they can efficiently process and, if this number is exceeded, the system will slow down, stall and begin to fail, again opening the organisation up to risk. Administration of biometric access control databases must be meticulous to ensure maximum security and optimum functionality.

Maintenance of the hardware itself is equally important, as wear and tear on the readers will have an impact on their efficiency. Fingerprint readers are touched by hundreds, if not thousands of people every day, and can build up a film of oil on them that can prevent them from reading properly. Exposure to harsh environments, such as hot, dusty or humid conditions, can cause damage to the system and its circuits, which again can cause erratic denial of access, if not outright failure of the solution. For these reasons, all of the physical components that make up a biometric system should be regularly assessed for mechanical or other failure.

Regular maintenance as often as use demands is critical in eliminating these challenges, optimising performance and extending the life of systems. Appointing a service provider with the appropriate technical skills and understanding of biometric technology and related systems ensures that biometric systems remain as secure as possible throughout their lifespan, mitigating risk and closing security loopholes for improved efficiency.

ABOUT KOBUS LE ROUX

Kobus Le Roux is national sales and marketing executive of Jasco Security Solutions.
- Biometrics is booming - but is your solution really secure? - 4 Jul 2013

View my profile and articles...