

# at your SERVICE

## A DIRECTORY TO GENERAL SERVICES

Monday, March 15, 2010

South China Morning Post

# Security at the touch of a finger

Even seasoned industry professionals admit the latest advances in security for offices bring to mind early science fiction movies.

Door locks operated by fingerprint recognition, for instance, will become a more common sight, with several Hong Kong companies developing and manufacturing devices to meet the demand for better and more flexible office security systems.

Biometric security, whereby data gathered from fingerprints or even facial definitions is transferred into algorithms and put on a database, is a progression from data embedded on a staff card microchip. Biometric security is also hailed as avoiding the hassle caused by a bunch of keys being mislaid.

As science fiction meets reality, fears can arise over privacy as people feel uncomfortable about undergoing a fingerprint or facial scan.

But security professionals point out that unique and minute characteristics, such as the height of ridges on the thumb's surface or the distances between eye and cheekbone, are converted into complex X-Y co-ordinates that cannot be replicated.

For Chapman Leung, managing director and co-founder of serviced office provider Jumpstart, locks operated by fingerprint recognition mean clients can use the company's new

premises in Wheelock House, Central, without having to remember who they entrusted the keys to and have complete confidence in the security.

"As we have an international client base, including Fortune 500 companies, who have to work outside normal office hours, we found there was a demand for entry systems that offered flexibility," Leung says.

The hi-tech locks complement the Cisco network adopted by Jumpstart that many top global companies favour to ensure the security of data. The global nature of the Jumpstart services also extends to multilingual staff, IP phone system and even the provision of beverages.

With more companies willing to consider the use of biometric technology for office security, options also include eye recognition and hand geometry. But with users having to stay still for a few seconds for scans to be made, wouldn't a basic sense of care and responsibility to look after keys be just as effective?

Mark Hargraves, head of physical protective security for HSBC, says biometric options are usually suited to higher-risk environments and prevent the lending of access cards or keys.

"While a good old-fashioned sturdy lock set in the right kind of door and frame provides suitable security, the addition of technology allows a degree



Biometric scans are now being adapted for office security. Photo: Bloomberg

of convenience and integration that a key-based system does not provide," he says. As for concerns over privacy, Hargraves argues: "The key to effective deployment is to ensure a clear understanding of how the data is stored and that access to that data is secure. Should the data be compromised, then the knowledge that a fingerprint cannot be reconstituted from that stored data

should assuage fears. The technology required to steal fingerprints, and then find an effective use for them, means the abuse of fingerprint information is at the very low end of the risk scale."

Hargraves says a person's identity is at more risk from the interception of mail, grabbing of ID card information or unwittingly revealing passwords or other security details to third parties.

## How systems can check identity

### Face recognition

Many security professionals like this as it works even when the subject is unaware of being scanned. Devices can also search through crowds. It works by analysing specific facial features, such as distance between the eyes, nose width, position of cheekbones or the jaw line.

### Retina scan

There is no known way to replicate a retina as the pattern of blood vessels at the back of the eye is unique and stays the same for a lifetime. Used by US military.

### Iris scan

Provides unique biometric data that is difficult to duplicate, but it also needs about 15 seconds of concentration from the subject.

### Voice analysis

Like face recognition, voice biometrics provide a way to authenticate identity without the subject's knowledge. It can be easier to fake (using a tape recording), but it's not possible to fool an analyst by imitating another person's voice.

Source: [www.technovelgy.com](http://www.technovelgy.com)