

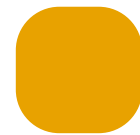
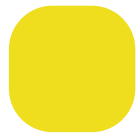
## wOrkplace security biosecurity: sOmething yOu are

by Pam Brenner

It wasn't long ago that card-key access badges — those powerful cards that give you building access, security clearance, debits in the company cafeteria and maybe even a spot in the parking lot — were considered the latest thing in security. Ironically, they were saturated with trust. If lost, the card had a message on the back asking the finder to place it in a mailbox so it could be returned to the originating organization.

For decades, architects, designers, and business professionals have been aware of the need for workplace security. But only recently have companies been re-examining common practices in the quest for a safer workplace. Booz Hamilton Allen, the strategy and technology consultants, report that prior to September 11, 2001, corporate security was viewed as a mid-level concern, ranking 6.0 on a 10-point scale. Post-attack, it rose to 7.5. In a heartbeat, we became more aware of our fundamental need to feel safe. Trust on all levels was challenged, and security once viewed as “intrusive” quickly became commonplace and comforting.

Priscilla Sandler, founder of Sandler Security Consulting, suggests viewing security as layers of concentric circles. The largest circle surrounds the building (location, location, location). Next is the building envelope (doors, stairwells), and finally the reception area (turnstiles, line control). In effect, the smallest circle would be an individual at a desk. How personal is security on a daily basis? Are the techniques we see in the movies (eye scanning, fingerprint detection, etc.) real? Or do they just belong in a *James Bond* or *Charlie's Angels* movie?



Pam Brenner is the editor of Steelcase 360 e-zine and has been reporting news and trends since she was ten years old. She also has contributed to several publications including *Business Week*, *Chief Executive*, *Quality Progress*, *Architectural Record* and *Buildings Magazine*. In her free time she writes poetry, travels to Caribbean Islands and is a connoisseur of blueberry pancakes.



## Biosecurity, continued

### KnOwing, HAving, BEing

Individual identification has had an interesting and overlapping progression. “Verifying” yourself used to just depend on something you knew — a password, code number or bit of personal data (like your mother’s maiden name). Then we introduced something you had — a card key or parking sticker. Now the current focus is on something you are — a biometric.

This third category is the most secure and the most personal. Common physical biometrics include fingerprints, iris, retina, hand or palm geometry, and facial characteristics. Things we take for granted — our signature, voice, keystroke or even gait (long stride, bouncy step) — consist of patterns that, when analyzed, distinguish us from each other.

The basis for security seems to be shifting inevitably from something we know to something we are.

**Did you know?** *In a study conducted during the last two months of 2001, 75 percent of chief executives at firms with revenues of more than a billion dollars a year reported increased concern over day-to-day activities such as mail processing, travel and protection of employees.*

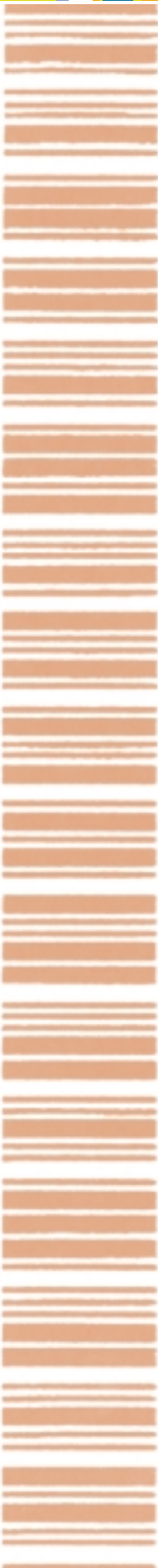
*Australia has allocated \$3 million to test new facial biometric technology by comparing people’s faces with passport photos. The intent is to eradicate potential passport fraud and reduce the risk of terrorist attacks.*

*In 1998 EDS developed and introduced a system at Ben Gurion Airport in Israel that uses hand geometry to identify passengers, who can now go through a separate, quicker security process.*

*The average British citizen appears to be the most widely “snapped” person. Estimates indicate they are photographed at least 14 times each day, as even their streets and sidewalks are monitored by closed circuit TV.*

*Police used facial recognition technology integrated with closed circuit TV when monitoring large crowds during the 2001 Super Bowl and the Salt Lake City Winter Olympics.*

*The U.S. market for physical security equipment is on the rise. The sale of interior security products in 2000 was \$1.31 billion, and by 2007 it is expected to reach \$2.41 billion per year.*





## Biosecurity, continued

### Biometrics in Application

With this trend, card keys have evolved into what are called smart cards, containing fingerprint sensors that confirm identity. Fingerprint identification also touches home security. An access keypad not only logs numbers for proper sequence but also registers the fingers punching in the numbers. If the prints do not match, access is denied.

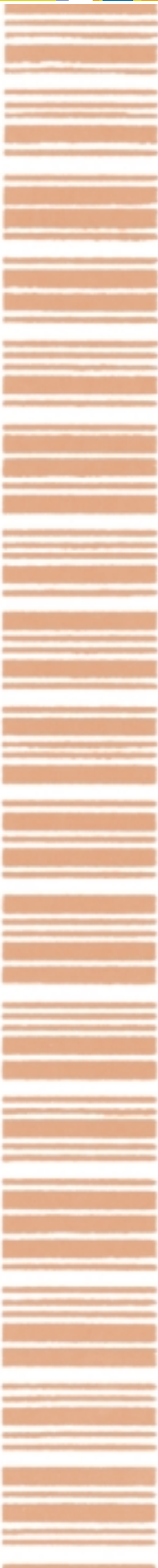
Automatic teller machines that include biometrics have recently been developed to combat fraud. Placing eye to camera verifies identity. Wrong eye equals no money.

Many hot products have also integrated biometrics. For the workplace, these include a mouse with an embedded fingerprint scanner and a computer-mounted security camera that uses iris recognition technology. No longer do you need to remember numerous passwords or PIN numbers — you simply have to remember where you sit and which computer belongs to you.

### Hello, my name is:

But that's not always easy for organizations with a highly mobile workforce. "Two examples that come up right away with security and space-planning are hoteling and free address," says Dr. Vivian Loftness of Carnegie Mellon University in Pittsburgh. "If you take a different desk every day, you might not even know the people sitting next to you. They could be a stranger or not even belong in your area."

And Loftness sees another touchy security problem on the horizon— what she calls the phenomenon of an employee "going postal." "It has to do with job security, inhumane treatment and being bottled up," she says. "Those kinds of security risks are not going away because jobs are becoming less secure, and in many cases, people are being treated less individually." To her point, the Computer Security Institute recently reported that disgruntled employees were the second most likely source of attack on computer systems, after independent hackers. So, while we check fingerprints, scan eyeballs and turn on the cameras, one of the biggest security threats may actually already be on the payroll.





## Biosecurity, continued

**What to do?** business leader strengthen internal security? Bill Boni, chief information security officer at Motorola Inc., has been quoted as saying, “Everybody’s got to be part of the overall protection.” He encourages “converting employees and staffs into deputy security officers” by reinforcing the thought that security is a shared responsibility.

Loftness also believes relationships between coworkers can make for a more secure environment. She states, “For the organization to be truly secure, we need the people within it to recognize and know each other very well.”

These concepts of shared responsibility and relationships relate back to the simple card key. In a subtle way, it delivered much more than just function. At a quick glance, it identified the wearer as belonging to something bigger—an organization. And while trust is inherent in the “please return policy,” the cards themselves do not create or build trust—the people do.

No one would dispute that what really touches our core need to feel safe is often demonstrated trust, coworker support and mutual acknowledgment. In a technical sense, biometrics appear to be the ultimate method of separating the known from the unknown — or the “us” from the “them.” Technology seems the best way to solve the problem. But perhaps in a sense, it is the experiences, relationships and responsibilities we share, not the biometrics that differentiate — which really help form and establish a secure community in the workplace. Only with a shared bond among us can a feeling of security truly be “what we are.” : :

