

# Biometric Systems

## The Next Big Security Opportunity

By Michael Richarme

Since the events of September 11 and subsequent terrorist activities, corporations have placed a renewed emphasis on trying to control entry to their workplaces. There is a rapidly growing realization that the low-cost security measures of the past are not adequate protection against a determined and clever terrorist assault. It is relatively easy for a thief to steal or acquire a company identity card, bypassing the beleaguered security, guards at the front door. This is true for physical location security as well as a much more vulnerable and potentially more catastrophic nexus: the information systems that handle the firm's finances.

Destruction of a corporate complex housing thousands of employees, as happened to many companies in the World Trade Center tragedy, causes horrific personal loss and suffering. Without backups to corporate records at secure physical locations away from their corporate facilities, the disaster would be complete, not only in the loss of key employees and friends, but also totally destroying the future (without the records) for all survivors. Fortunately, many firms have already learned to protect their future in this manner. One large bond trader, devastated by the September 11 tragedy, was able to set up shop at a remote location and resume trading when the bond markets reopened.

Current cyber security protocols include firewalls, changing passwords, encrypted data files, and a variety of similar protections. Yet clever hackers are finding ways to defeat these protocols, because the protocols are not intelligent. The protocols don't recognize that the person presenting entry codes is not authorized to get into the system. One way to address this shortcoming is the use of biometrics embedded into critical information systems.

Biometrics—the process of using the unique physical features or characteristics of a person to confirm identity—has been around for quite a few years in various forms. The most familiar modes are photographs on identity cards or fingerprints. Less familiar modes, often relegated to extremely high security areas or James Bond films, include retinal scanning, voice print authentication, or palm print scanning.

How might this appear in the corporate world? Physical security is a good start, with retinal and palm scanners required for access to physical equipment areas like server farms. These would also make sense at corporate entry points, supplementing the physical ID badge. Some firms with high security data processing facilities, like American Airlines, already deploy sophisticated but costly biometrics systems. The same corporation uses physical ID badges for access to theoretically secure airplane maintenance and baggage handling areas, not to mention actual airplane cockpits.

One fact is clear. Protecting physical facilities but not information systems, or vice versa, is not adequate for today's world. Companies need to evaluate their corporate security from both a facilities and from an information system perspective. It is no longer enough to rely upon security protocols that have been shown to be easily defeated.

For the casual or remote connection to the information system, other options are available in addition to the myriad of passwords that a corporate citizen must memorize. Good quality cameras are available at relatively low cost. Microphones are also fairly inexpensive. Software currently exists that allows recognition and validation of a person by exam-



1.817.640.6166 or 1.800. ANALYSIS • [www.decisionanalyst.com](http://www.decisionanalyst.com)

ining the face and comparing certain unique characteristics, like the distance between the temples or the width of the mouth. Additional software compares a spoken word or phrase to the voice patterns stored in the security file. Voice recognition software has been in use for many years, and is rapidly spreading to the mobile phone market.

Both of these tools would allow a very high level of security for individual work stations outside the core IT community. The use of multiple modes of authentication is important to overcome the occasional mismatch due to a cold or other physical ailment. As computer processors become more capable and as software becomes more sophisticated, the ability to fool biometric systems with photographs or audio-tapes goes down dramatically.

Some might say that this type of security protocol is a violation of privacy. Another way to look at this, however, is that an individual's security is being protected. Having a database containing a photograph of one's face or a voiceprint of one's name would appear to be nothing more than personal protection as one goes about his or her daily life. A very valid concern exists that this might be another step toward the Orson Wells vision of the future, with Big Brother observing one's every movement. Prior to the tragedy of September 11, the tradeoff of privacy versus security might have tilted more in the direction of privacy. After the events of that fateful day, however, the pendulum

appears to have swung rapidly and severely in the direction of security.

Implementation of these types of measures will create a significant opportunity for security system manufacturers, stimulated by the increases in computer processing power and the dramatic reduction in associated costs over the past two decades.

**B**iometric security systems, still in their early development stages, have already been successfully employed, giving corporations key insight into ways to affordably and effectively employ the newest of security technologies. Companies like El Al have employed sophisticated security measures out of necessity, and have shown that the investment can prevent airplanes from being hijacked. Unfortunately, in our society, it often takes a tragedy to create safeguards against similar tragedies. Biometric systems may not have been enough to prevent the September 11 tragedy from occurring, but they may have been enough to frustrate the terrorists to finding a less dramatic means of enacting their terror. El Al has never had an airplane hijacked, because hijackers see their security protocols and look for a weaker or more vulnerable target. And that is, after all, the end game for security people around the world. Just make it so difficult for a bad action to take place that the perpetrator goes elsewhere.

## About the Author

Michael Richarme is a Senior Vice President at Decision Analyst. The author may be reached by emailing [mrichar@decisionanalyst.com](mailto:mrichar@decisionanalyst.com) or by calling 1-800-262-5974 or 1-817-640-6166.

Decision Analyst is a leading international marketing research and analytical consulting firm. The company specializes in advertising testing, strategy research, new product ideation, new product research, and advanced modeling for marketing-decision optimization.



604 Avenue H East • Arlington, TX 76011-3100, USA  
1.817.640.6166 or 1.800. ANALYSIS • [www.decisionanalyst.com](http://www.decisionanalyst.com)