

“The Human Factors Involved When Implementing A Biometric System-Part II”

Our last article provided insights to you, the business owner, as to the Human Factors issues you could potentially face from your employees as you implement a biometric security system. This article will describe the various ways in which you can address those issues, and how you can foster a trusting relationship with your employees in regards to your biometric system.

The first Human Factor issue addressed was that about privacy rights, and why it is such a “hot issue” with biometric technology. The reasons cited include the fear of your employees giving up their physical and biological attributes to the biometric system, the biometric data being stored in a “black box”, and that data being shared with third parties.

With regards to your physical and biological parts being scanned-yes, there is a very brief moment in time the biometric system extracts the images of these parts-such as your fingerprint, various facial images, as well as parts of the iris. However, it is important to remember that these physical and biological is not what is stored in the biometric database for subsequent comparison.

These physical and biological characteristics are converted into a mathematical file. It is these mathematical files which are stored in the biometric database, and what is used for verification or identification. For most biometric systems, it is a binary mathematical file that is created and stored-a series of 1’s and 0’s (for example, 1100010101000111100111111 is an example of a biometric template). The template cannot be reverse engineered to recreate the physical and biological images that were captured in the first place by the biometric system. Also, it is important to remember that every time your employees use the biometric system, another template is created and is never the same from the original template. In other words, there are never two templates which are identical for the same person. Therefore, the probability of reverse engineering becomes almost zero.

It is important that you tell your employees this-that their physical characteristics are never stored-nor can the biometric template be reverse engineered. Companies and businesses that implement a biometric system fail in this regard. However, if you the business owner, take the initiative to calm and relax employee apprehensions from the very beginning of system implementation, the resistance to use a biometric system will be greatly diminished, and will result in cooperation on the part of your employees.

The fear of a biometric template being stored in a black box are completely untrue. Biometric devices (especially the fingerprint reader and the hand reader) can operate in a stand alone mode or in a networked environment mode. Therefore, the biometric templates are either stored in the device itself, or at a server in a networked environment. It is just as important that you tell your employees how the biometric system will be configured (there is no need to give all the technical details-just enough to tell them where authentication will take place-at a local level, or in a networked environment).

The bottom line is that your employees should be told exactly where their templates are being stored.

The issue of the disclosure or garnering of biometric data to third parties (such as those companies that prepare mailing lists, telemarketing firms, etc.) needs to be addressed. This will probably be best done in an open forum format. When conducting this forum, use a “real world” or common sense approach. For example, if the biometric template were compromised in some way and given to a third party what can it possibly be used for? The answer is absolutely nothing. The template cannot be reversed engineered. Really, if you think about it, what kind of ID theft can take place with just a series of 0’s and 1’s?? You really cannot do any marketing with it, as you can with a phone or mailing list.

Also remember, each biometric vendor has their own proprietary algorithms for enrollment and verification. For example, if your database of biometric templates were stolen, and used at an ATM machine where another biometric system was in place-the chances of the ATM biometric system accepting the templates that were stolen is almost zero-because each vendor’s product has their own algorithms. Think about it this way: We commonly give out our Social Security number, and routinely give out our Credit Card number when making purchases. Why are we not concerned about these being compromised and misused, instead of getting nervous about a series of 0’s and 1’s being stolen?

The next Human Factor issue brought up was if the biometric system can cause any physical ailments to your employees. To my knowledge, there have been no documented cases. Obviously, if you know of employees who are sick and use your biometric system, you will want to clean the device per the vendor’s suggestions-so that nobody else can contract the germs. But also remember, in the business world, we are exposed every day to things that could cause sickness-such as public transportation, shaking hands with customers and business contacts, etc. Also, to my knowledge, there have been no reported cases of a biometric system actually causing physical damage to a user. Some of the technologies can be considered user invasive to a certain degree, which could cause discomfort. This is particularly true with retinal scanning devices. Users would have to put their eye into a receptacle, and an infrared light beam would be shone into the pupil of the eye. With iris scanning, the technology is not as invasive-a user can stand as far as three feet away and still have their iris scanned by the camera. Again, there will be squeamishness among your employees about having their eyes scanned. But the key thing to stress to your employees is that they cannot go blind by simply having their eyes scanned. The technology is *very safe* to use. Iris scanning devices are being implemented worldwide, especially at airports to expedite the process of immigration and customs. And, I too, had my eyes scanned at a biometrics trade show a couple of years ago. To be honest, even I was a little apprehensive (it’s only human nature to be), but everything was fine.

Probably the biggest thing you can do as a business owner to increase the acceptance and to quell other fears (such as the presumption of guilt, restriction of freedom of movement, etc.) among your employees is to be up front about everything as it relates to the biometric system, and to have a good training program. In being up front, tell your employees about your intentions of implementing a biometric system, especially the advantages and benefits that are to be gained. Tell your employees how it will improve security at your place of business. Don't just do this by distributing a business memo- have an open group forum, where your employees can speak openly.

As the biometric system is being implemented, you ***must*** provide for a training program for your employees before the biometric system goes live. By having a good training program, many of the fears, objections, and anxieties will be overcome. Also, your employees will have acquired the necessary knowledge in how to properly enroll and verify themselves before going live. What should be included in the training program? You should design the training program to suit the needs of your employees. However, the topics that should be covered include a brief primer into the science of biometric technology, as well as conducting pilot runs so your employees will know how to use the devices properly. Also, you may want to give your employees printed material which consists of the key points covered in the training program. This can be used as a reference later on.

Although having a training program may sound like a lot of work and effort on your part, you will be saving a lot of money, frustrations, and headaches in the long term. There is a biometric management methodology called BANTAM-which stands for Biometric and Token Technology Application Modeling Language-it was developed by biometrics pioneer Julian Ashbourn from England. This methodology contains a training program which you should consider using. For more information about BANTAM, click here (<http://www.htgadvancessystems.com/Advance/services/index.html>), or contact me at rd@htgsolutions.com.

Another Human Factors issue raised was the use of biometric technology as a form of high level "electronic tattooing". You must give your employees the choice of whether or not to use the biometric system-it cannot be forced upon them. For example, if you address employee fears and have a good training program, most of your employees will be accepting of the biometric system. However, there could be a small number of employees who will just object outright to using such a system, or you may have some employees that simply cannot use a biometric system because of physiological reasons. In these cases, you must have a back up system in place (such as a manual ID check, etc.).

With regards to the fears of "Big Brother" watching, really about the only thing you can do is to make sure your employees have the knowledge they need to use the biometric system effectively. The stigma of Big Brother watching is a worldwide one, and only time can take care of this issue. It is the media which fuels the fear of Big Brother watching, and the government misusing biometric data. For example, the days after 9/11, biometrics received a great boon by the media, by making claims that this will be the

ultimate security tool-especially facial recognition. In fact, even the stock prices of major biometric companies skyrocketed to unprecedented levels. However, a few months after 9/11, and after facial recognition technology failed to live up to its high expectations, the media went totally negative on the use of biometric technology. This happened because the media did not look at the use of biometrics objectively or try to understand it. People were under the impression that facial recognition technology would be as good or even better than the human brain in terms of identifying people. The human brain has evolved over thousands of years, and when facial recognition technology is compared to this timeline, it is still in its infancy stage. This is a prime example of the media over hyping and totally condemning the use of a particular technology.

Finally, as you approach and embrace the use of biometric technology at your place of business, remember to look at it from an objective point of view. Remember, it is only a piece of technology. There is nothing mysterious or wonderful about it. It is just another security mechanism that can be used like any other-such as CCTV, card swipe, smart cards, etc. Biometric technology has its flaws just like any other technology-computers, cell phones, PDA's, etc. The bottom line is that why should we be afraid to use biometric technology if we use these other types of technology everyday in our lives?

This article concludes our series on biometric technology. We have covered the subject of biometrics from two different perspectives: (1) A Technical Series Track, where articles were written on how each of the major biometric technologies work; and (2) A Business Series Track, which was geared towards the business owner, focusing upon the implementation of biometric technology at a place of business.

Our next series of articles will be focusing upon more general security topics. Starting in 2005, our next topic of focus will be upon E-Commerce security.