



On Board with Biometrics: Setting the Record Straight

Biometrics is one of the fastest growing technologies in the Time and Attendance industry. Virtually all new Time and Attendance systems offer some biometric technology, such as fingerprint verification, hand recognition, or iris scan.

The reason? Biometrics provides increased accuracy and security in a single solution. To start, biometric time clocks increase employer profits by keeping employees honest: no more buddy punching or manipulation of manually-recorded data. As well, payrolls can be calculated automatically, eliminating human error. And the data collected by biometric Time and Attendance solutions offer accurate insights into what is typically a company's greatest single expense: labor costs. Understanding these costs is the first step toward controlling them.

However, some managers run into resistance on the part of employees to embrace a new, high-tech biometric system.

Why the Resistance?

There are several reasons why employees resist using a biometric Time and Attendance system. Some employees feel that moving to an automated biometric Time and Attendance system means that the company doesn't trust its employees. Sometimes, employees feel that providing a scan of their finger or iris is an invasion of privacy or poses a health risk. There may even be religious opposition as some people claim that biometric devices leave 'the mark of the beast' (Revelation 13:14-17) on the hand of the users. Employees may worry that germs can be picked up by touching the same device used by others.

Clearing up Misunderstandings

The best way to overcome resistance to biometric technologies is to educate employees about how the technology works. When people understand how the biometric technology works, their fear diminishes. In addition, managers should stress that the accuracy provided by biometric technology is a benefit to employees as well as to employers.

To help ease your employees' concerns, here is a chart of some common misconceptions about biometrics, and the facts to set the record straight.

Misconception	Reality
The company is installing a biometric system because the management doesn't trust me.	In almost all cases, a biometric system is being installed for greater accuracy in the company's payroll department. Biometric units help ensure that all employees are being paid accurately. In addition, biometrics can add a level of security for employees as well as employers, since only authorized personnel can gain entrance to biometric-secured facilities.
The image that the biometric clock takes can be used to send my information to government agencies.	The image that a biometric unit takes does not store enough detail to be used by any government agency. In addition, in most cases, the biometric system is being used to verify, not identify, the employee. This means that an employee's biometric information, presented in conjunction with a Smart Card or employee number, simply allows the system to verify that the person who owns the card or employee number is actually the person he or she claims to be, based upon the physical characteristics of the biometric image.
Biometric time clocks record my fingerprint as an image, which a computer hacker could access and abuse.	The time clock DOES NOT store the fingerprint as an image or picture. The fingerprint image is converted by the system and stored as a 350-byte data record, or algorithm, containing symbols, numbers, and letters. The data record is absolutely useless outside of the time and attendance system.
The new time clock leaves the 'mark of the beast' (Revelation 13: 14-17) on my hand when I use it.	A biometric unit DOES NOT put a mark on an employee's hand, and it is completely safe to use, based on independent laboratory research. Additionally, a hand or fingerprint image cannot be duplicated from the clock; as the image is converted into algorithms before being stored (see above).

<p>I'll get a disease or germs from touching the clock.</p>	<p>Touching the sensor on the clock is no different than touching a telephone, doorknob, or computer keyboard. The sensor on the time clock can be cleaned easily by using alcohol and a cotton swab.</p>
<p>If I have a cut or a band-aid on the finger I clock in with, I won't get paid.</p>	<p>The clock's program actually compensates for minor cuts and scrapes. Unfortunately, the clock can't read through a band-aid. However, the system can be set up to store two fingerprint templates, so that an alternate can be used in situations such as this.</p>
<p>My finger's image is sent over the network where anyone can see it and save it.</p>	<p>The finger's image is NOT sent over any network. All images that are scanned by the clock are stored as algorithms in that clock. The only thing that is sent over a network is an employee identification number.</p>