**WHERE'S THE "BEEF"?**

*By Larry Reed, CEO, ZKAccess*

In other words:

. . . Where are the sales opportunities today in the security industry?

. . . How can I differentiate myself from the other sales guy/gal?

. . . What products do my customers need which still generate a decent profit?

These questions are foremost on the minds of all security sales professionals.

So, where IS the beef?

If you’re a millennial, perhaps you might not remember this catch-phrase made popular in the 1980’s.  But anyone born before 1970 certainly remembers this 1984 television commercial which starred three elderly ladies examining an exaggeratedly large hamburger bun topped with a minuscule hamburger patty. Two old gray-haired ladies poked at it, exchanging bemused comments ("It certainly is a big bun. It's a very big bun. It's a big fluffy bun. It's a very big fluffy bun.") before being interrupted by the third old lady who exclaimed loudly for all the restaurant staff to hear . . . “***Where’s the beef??***”

So, “where’s the beef” in the security industry??

It’s certainly not in surveillance cameras or DVR hardware anymore.  Camera sale profits have nose-dived dramatically due to fierce competition and price wars waged amongst competing vendors, especially from overseas manufacturers and suppliers.

The beef WAS in access control 10 years ago.  And although prices for [access control panels and card readers](http://www.zkaccess.com/product-category/c3-access-control-panels/) have come down significantly, the recurring revenue from consumables (i.e., cards) remains attractive to dealers.  But today’s customers are examining their operations more closely.  And many by now have reached that line in their accounting ledgers which notes the ongoing replacement cost of [prox cards](http://www.zkaccess.com/product-category/accessories/).  So does the access control “beef” go away if/when customers finally stop purchasing cards?  How can the access control industry maintain its “beef” as it appears to become equally commoditized as the surveillance camera industry?  The answer is [BIOMETRICS](http://www.zkaccess.com/product-category/standalone-wiegand-readers/).

Biometrics has grown into a $26 billion industry according to ABI Research.  Yet many reluctantly cautious security integrators still refrain from recommending biometrics to clients due to three unsubstantiated reasons I hear all the time:

1.      Perception/excuse that Biometrics is cost-prohibitive for commercial customers

2.      Perception/excuse that Biometrics would be rejected by customers due to its complexity

3.      Perception/excuse that Biometric accuracy/identification read-rates are unacceptable

The reality is, [BIOMETRICS](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) is NOT that expensive.  There are many competing fingerprint reader manufacturers today driving down the cost of fingerprint readers.  Some of these vendors can produce fingerprint readers which approximate the cost of today’s prox card readers.  Even face readers aren’t relatively that expensive.  If you do your research, you’ll find biometric vendors who can deliver quality products at prices customers can easily afford, at least when it comes to restricting access to their high-value assets (i.e., cash rooms, warehouse, computer room, etc.).

[BIOMETRICS](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) is no more complex than 25-year-old keypad technology.  For the most part, biometric readers share the exact same wiring, power and communication requirement as do keypad and card readers (i.e., 12V power, TCP/IP/RS485 communication, 12V relays and Wiegand output).  From keypad to iris recognition, readers differ only by their sensor (i.e., PIN code, card sensor, fingerprint sensor, face sensor, iris, etc).  So, let's rule out the notion that “complexity” inhibits the adoption of biometrics.

Biometric accuracy has improved dramatically the past three to five years, primarily due to improved image capture technology and faster processors.  Anyone with a bias against biometric readers either hasn’t tested one in the past three years, or haven’t tested enough vendors.  While some vendors’ technology lags, other vendors have stellar, reasonably priced biometric technology.

The above three obstacles no longer exist.  So if integrators want to gain market share from their competitors, further differentiate their company, increase their profit margins and gain further credibility with their clients . . . they need to drop the excuses and look for the “beef”.

Also, don’t lose sight of the fact that if you are not offering biometric technology as an option, your competitors could very well be stealing YOUR beef.  For example, if you’re a traditional card access control supplier who doesn’t offer biometrics . . . when your customers seek out a biometrics supplier, that biometrics supplier can very well steal your card access business.   Customers like one-stop shopping.  So why risk sending your customers to a competitor?  Don’t share your beef, either.

So, here are some places you can find (or make) the “beef”, in which profit margins can be preserved and you can really differentiate your company from your competition:

Best place to start your search for the beef?  Find areas in which biometrics preserves your clients’ revenue streams:

**Health/membership clubs**.  Proprietors charge members a fee for access to amenities such as the golf course, workout room, laundry room, swimming pool, spa, etc.  But you know members have friends who they share their membership card with.  That’s a potential loss of membership fees the proprietor could have normally collected.  Having members use biometrics ensures only paying members are accessing amenities and paying for the proprietor’s beef. For instance, check out any of [ZKAccess’ stand-alone biometric readers](http://www.zkaccess.com/product-category/standalone-wiegand-readers/)

Next, find areas in which biometrics can reduce your client’s expenses/liabilities:

**Payroll / Time & Attendance Clocks** sold to customers with hourly-wage employees. Employees who use cards/badges when punching in/out of a time clock can easily defraud their employer by not reporting to work while asking a co-worker to punch in for them.  The unearned pay received by the absent employee is called “Buddy Punching”.  Considering payroll often accounts for 10% of business operating expenses, preventing buddy punching is paramount when protecting a business’ bottom-line.  Installing biometric time clocks can save employers thousands of dollars (in other words, a LOT of beef), depending on how large a work staff they employ. For instance, check out affordable [biometric time clocks from Processing Point.](https://uattend.com/time-clocks/)

**Reduce Retail Shrink**.  It’s hard enough for retailers to grow their business, but even more daunting to reduce “shrink” attributed to both shoplifter and employee theft (i.e., stolen beef).  With traditional key/card systems, employees can easily gain access to their managers’ keys and subsequently also to cash rooms and stock rooms (where retailers store their beef).  By placing biometric readers in front of these high-value rooms, you can now limit access and thereby reduce “shrink”.  Help your retail clients prevent their beef from walking out of their store. Place a [biometric reader](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) on any door safeguarding valuable assets.

**Reduce Liability / OSHA compliance**.  Retail stores operate dangerous equipment (i.e., cardboard balers, forklift truck, freight elevators, etc.).  Not only can untrained people get hurt by incorrectly operating this equipment, OSHA also levies heavy fines when they discover unsatisfactory safeguards. I know a Loss Prevention manager fined by OSHA $200k because someone left the key in the ignition switch of an electric cardboard baler.  Easy fix?  Install a biometric in front of each piece of dangerous equipment so that only authorized employees can activate the equipment (and not get their beef/limb accidentally chopped off).  The biometric can act as a “kill switch” and prevent unauthorized start-up, thus protecting employees and customers. Place a [biometric reader](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) on any device which could cause injury if operated by unauthorized personnel.

Next, find places where you can make money:

**RMR (Recurring Monthly Revenue).**  A major reason integrators prefer card access systems is because cards need to be replaced whenever the cards become lost, stolen or damaged.  So although biometric credentials (i.e., fingerprint, face, finger/palm-vein, iris, etc.) cannot be lost, stolen or damaged, there still actually exists RMR opportunities with biometrics.  Biometric credentials need to be enrolled into the access control system, at times removed from the system, copied to multiple readers . . . "Biometric management” can easily be incorporated into the overall access control management services an integrator can bill customers monthly for.  That means monthly beef in your pocket. You can easily host an access control system in your own office by purchasing an tiny affordable [access control appliance](http://www.zkaccess.com/product/inbridge-server/).

Next, find places where your customer can make money:

**Increase customer revenue**.  Retail stores produce a ton of recyclable material which can be redeemed for money.  But too often, employees & customers throw away all their garbage.  That’s like throwing money out the window.  To reclaim this lost revenue, all you need do is install a ZKAccess biometric reader before the trash compactor.  This will allow only authorized users to operate the trash compactor and prevent employees from throwing away your client’s beef. Place a [biometric reader](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) on any device which could create/save money when operated by unauthorized personnel.

Next, find places where your customer can protect their beef:

**Biometrics is great for retail customers dependent on Unassisted Delivery**.  If your clients’ business depends on receiving deliveries after-hours, by installing biometric security you never again have to worry about dispatching someone (employee, night watchman, security, guard, etc.) to let the delivery guy in.  Simply enroll the delivery drivers’ fingerprint(s) into the biometric access control system and restrict the drivers’ door access to associated after-hours time periods. This reduces the cost of manpower. Place a [biometric reader](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) on any door which delivery drivers require access.

**Biometrics is great for Pharmacists**.  Whether caused by employees or external thieves, drug theft is rampant.  Biometrics is a great way to prevent unauthorized parties from accessing drug safes.  The safe can be programmed only to open after the authorized user presents his valid biometric credential(s) and a drug code.  An audit trail of users accessing the safe can subsequently be created and viewed on demand.

**Improve security for the customer while also enhancing productivity and convenience of employees**.  Everyone knows, employee keys, badges and access codes can be shared, forgotten, lost, stole, etc.   By placing biometric readers on the doors, you’ll improve security and improve productivity and convenience for employees since they can no longer be accidently locked out.

**Energy conservation.**  Consider how much money is wasted on generating light and heat in offices buildings when no one is actually in the building.  By using biometrics, you can program an “intelligent” building to maintain light and temperature based on who actually is in the building.

**Safety**.  Use biometrics to prevent unauthorized access to homeowner’s gun safes.  Who can remember the combination or key to gun safe when under duress casued by an intruder in your home?  Using a fingerprint, instead, ensures fast safe access to your gun safe.

**TV Remotes**. Worried about children viewing inappropriate TV shows while you’re away? Use a biometric TV remote control, programmed according to parents and children’s fingerprints.

**ATMs.**  Card fraud is always in the news and unavoidable.  You try to hide your PIN code while you punch it into an ATM keypad, but inevitably there’s a person eavesdropping on you, who then later uses your code to access your money.  For this reason, many ATM manufacturers are now incorporating biometrics into their ATM machines.

Place a [biometric reader](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) on any device which can either protect people/assets or create a revenue stream.

These are just some of the ways that [BIOMETRICS](http://www.zkaccess.com/product-category/standalone-wiegand-readers/) can help preserve your profit margins and differentiate your company from your competition. Keep in mind that biometrics accuracy has improved markedly in recent years, and biometrics technology continues to become more affordable and accessible. So where’s the “beef”? Consider how you can incorporate any of the above applications in your business offering.