



CONNECTIONS
and Conferencing Technologies Ltd

*Biometric
Access Control*

***Biometric Management
in Your Organization: A Guide for Businesses***



Introduction

Biometric Access Control Units are a ***minute step*** into ***the world of digital technology***. Biometric Systems verify an individual's identity based on unique biological features (fingerprint, face-print, iris, and vein, to a name a few).

Biometric Systems were once reserved for the highest level militaries and government organizations around the world. Recent advances in technology, however, have led to reduced cost of these intelligent devices, increasing adoption rates across the business world.

We wrote this guide to help you take advantage of the potential opportunities modern day Biometric Systems can present to your organization. We hope the guide will help you make informed decisions while moving your company forward.

What you'll find in the following pages:

- How Biometric Systems can Drive Growth in Your Organization
- 4 Things to Consider When Buying a Biometric Access Control Unit
- Keypads, Cards Readers, and Biometrics: Which System Is Right?
- 3 Tips for Choosing A Biometric Installer

How Biometric Systems Can Drive Growth In Your Organization


Measuring Time and Attendance

An individual's productivity is measured based on **how time is spent**. In most cases, the monitoring of such activities can be **difficult, and prone to human error and simple forms of circumvention**.

Biometric Access Control Systems give organizations a consistent method for quantifying time spent and monitoring the following activities:

- Consistency in attending work
- Time of arrival and departure from work
- Duration of lunch breaks
- Access to selective departments and facilities

Smart Biometric Systems are data acquisition tools which allow users to extract key data insights about an organization. This data can be used to make informed and intelligent decisions about the future of your company.

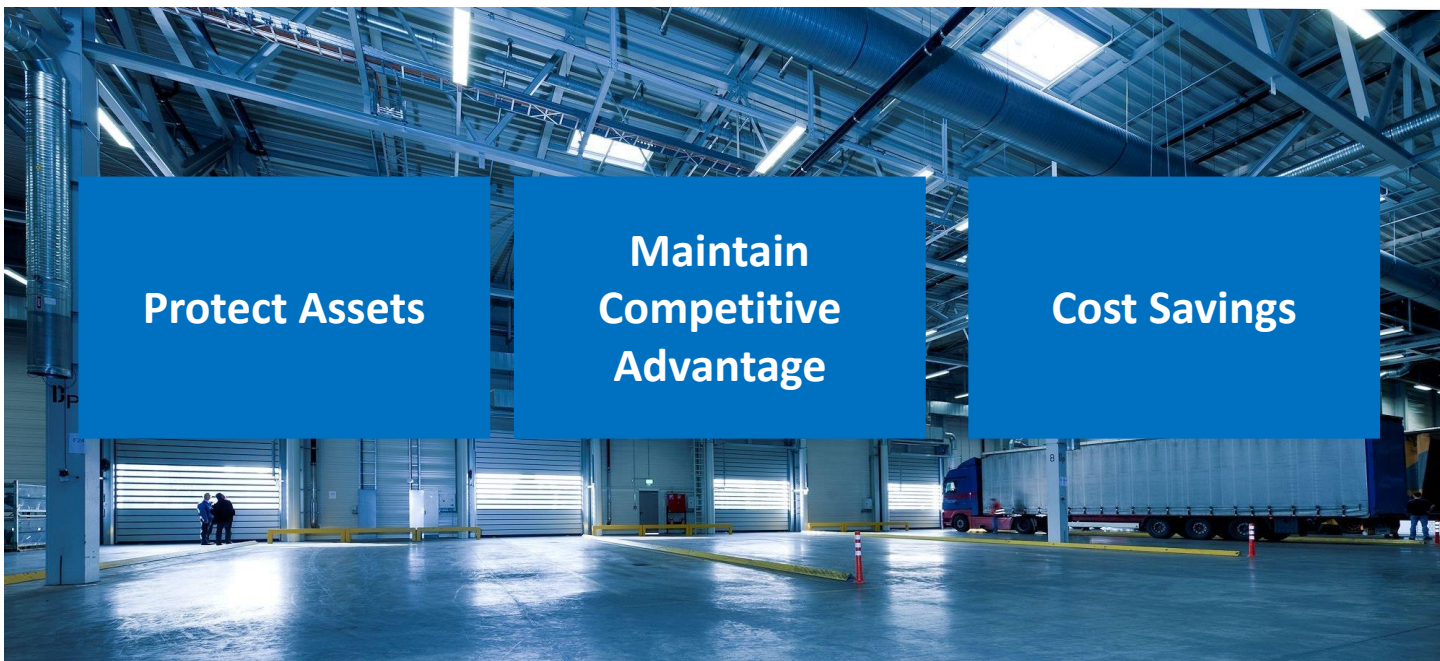
A low-angle, black and white photograph of a modern glass skyscraper, showing the grid of windows and the building's structure reaching towards the sky.

Increased
Productivity

Increased
Efficiency

Increased ROI

How Biometric Systems Can Drive Growth in Your Organization



Security: Manage Facility Access

To date, there are various methods in place to restrict access based on personnel and their respective occupations. Enforcing them can prove to be a challenging prospect in a hectic work environment whether it's by physical or data entry regulation.

Utilizing a smart system management software, permanent steps can be taken to:

- Restrict access to specific individuals or groups of individuals
- Protect facilities that store sensitive information
- Grant time-sensitive access to high profile facilities
- Prevent internal vandalism
- Prevent theft of sensitive information

4 Things to Consider When Purchasing a Biometric Unit



1. Security Level

Not all Biometric Systems are created equally. Some systems have a single method of authentication (Fingerprint or Face) while others have multiple levels of authentication (Fingerprint/RF Card/Password). Multifactor authentication provides additional layers of security, making it *much more difficult* for unauthorized personnel to access a location or target.



2. Size & Demographic of Your Organization

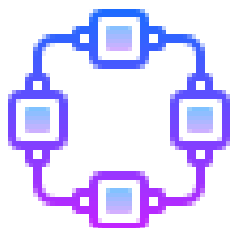
Knowing the size of your organization or department is important. Biometric Access Control Units have a *maximum user storage capacity*. While small systems may be adequate for start-ups and small organizations, they will not work for larger organizations with extensive staffing requirements.

Demographics: Ageing populations are an important factor to consider when choosing a biometric system. Older populations for example, can be susceptible to “disappearing” fingerprints. Individuals employed in certain occupations can deal with the same.



3. Environment

Consider where the unit will be placed. Some Biometric Access Control Units are designed specifically to withstand harsh conditions like wind, rain and extreme temperatures. Others systems are not designed for harsh environments and can easily be damaged by these conditions.



4. Integration & Scalability

Consider how the Biometric System will integrate across your network. Organization can start small but over time may decide to grow. Transfer of employees across departments can also occur frequently. You want to ensure your Biometric Systems are scalable, so they can accommodate these changes.

Keypads vs Card Readers vs Biometrics

What You Know (Password)- Keypads are best suited for garage doors, courtyard gates, and environments that require fairly low levels of security.

What You Have (Card) - Card Readers can provide a moderate level of security to areas but RF cards are frequently lost and can become easily de-programmed. This makes them a difficult option to recommend.

Who You Are (Identity) - Biometric access control systems unlike keypads provide preventative measures against user malice and are suited for high level security environments.

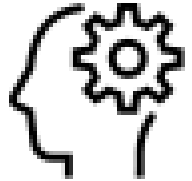


Keypads	Biometrics
Access code can be shared (buddy- punching)	Unique authorization (fingerprint,retina,face)
Constantly changing access code can be forgotten	One time record of fingerprint/retina/face needed to grant permanent access
Access code remains the same after employees leave the job	Users can be added and removed easily using management software
Master Access Code to configure keypad can be shared	Administrators have extra layers of security (fingerprint) to prevent tampering
Keypad is unable to distinguish who enters an access code	Terminal records and stores a log of individuals who enter and exit

3 Tips for Choosing A Biometric Installer

Expertise

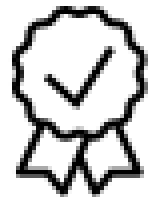
Look for installers who have extensive experience in working with Biometric Access Control Units. Experience solely with Keypads and Card Readers is insufficient.



Biometric installation appears simple but maintenance can be complex. If an error occurs with your system, it can take a great deal of troubleshooting to solve the problem. In those circumstances, you want a qualified team of professionals who can get your system back up as quickly as possible.

Quality of Hardware & Warranty Systems

Ensure your provider uses industry compliant devices that are backed by a manufacturer's warranty. Large-scale Biometric implementation across your organizations can be a significant investment. It is wise to protect yourself with a warranty.



Reputation

Ask your installer for references and testimonials from previous projects. Qualified providers should have little problem providing you with this information. Talking to previous customers can give you insight into how projects are implemented.



Consultation

We hope this guide has helped you get a better understanding of the potential opportunities Biometrics can offer to your organization.

We'd like to offer you a free consultation or assessment on your access control needs. You can contact us today at **868-663-5276** or visit our website at **www.connections-tt.com**



 **CONNECTIONS**
and Conferencing Technologies Ltd
www.connections-tt.com

