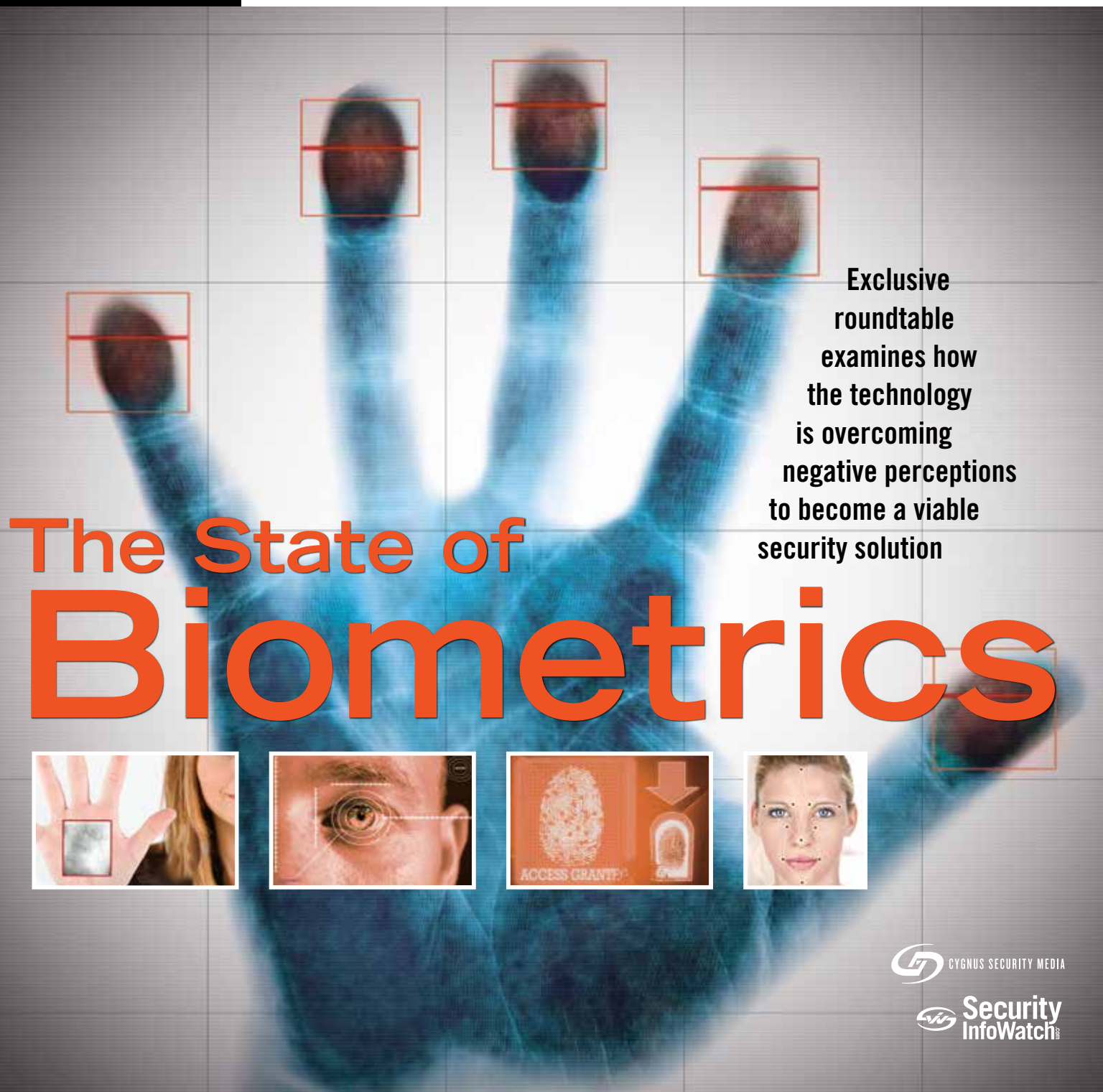
Supplement to
Locksmith Ledger International, Security Dealer & Integrator, Security Technology Executive
www.LocksmithLedger.com
www.SecurityInfoWatch.com

July/August 2014

ACCESS CONTROL
TRENDS & TECHNOLOGY



Exclusive roundtable examines how the technology is overcoming negative perceptions to become a viable security solution

The State of Biometrics

CYGNUS SECURITY MEDIA
SecurityInfoWatch.com

212,000
SQUARE FEET OF WAREHOUSE SPACE

30 YEARS IN THE INDUSTRY

YOUR 1 SOURCE FOR EVERYTHING *you need.*

Experienced technical sales reps. Ready to help you now.

You need door hardware for a job right away. Security Lock Distributors has the inventory and the expertise you can count on to get you precisely the product you need, when you need it.

seclock.com | 800-847-5625

ALLEGION™

Authorized Allegion Distributor

SCHLAGE ■ aptiQ ■ XceedID ■ LCN ■ VON DUPRIN

SECURITY LOCK DISTRIBUTORS

Request information: www.SecurityInfoWatch.com/10215009

THE ONE BOX SOLUTION

THREE ITEMS WILL COVER 90% OF INSTALLATIONS

4100

TRINE ACCESS TECHNOLOGY

1 - 3/8" Shallow backset

Why cut for a deadbolt 100% when it's only used 5% of the time.

4 FACEPLATES INCLUDED

4850

HANDLE 1/2" & 3/4" LATCHES WITH ONE BOX

ORDER 4850PoE

1/2" 1/4" 1/8"

All PoE™ Friendly

Low Current Draw

4200

Tall latch cavity alleviates "Field" issues

Latch Design accomodates aux. latch "pin"

4 FACEPLATES INCLUDED

All Included

CHANGE THE FINISH

Request information:
www.SecurityInfoWatch.com/10215438

Checkout trineonline.com for all specifications.

JULY/AUGUST 2014

ACCESS CONTROL TRENDS & TECHNOLOGY

COVER STORY

FEATURES

NEW PRODUCTS

ACCESS CONTROL TRENDS & TECHNOLOGY 2014

3 Huntington Quadrangle, Suite 301N., Melville, NY 11747 USA
Phone: (631) 845-2700 • Fax: (631) 845-2736 and is a supplement to Locksmith Ledger, Security Dealer & Integrator and Security Technology Executive magazines.

PUBLISHER

Group Publisher....Nancy Levenson-Brokamp
nancy.brokamp@cygnus.com

EDITORIAL

Editorial Director....Steve Lasky
Editor, *Security Dealer & Integrator*....Paul Rothman
Editor, *Locksmith Ledger*....Gale Johnson
Editor, *SecurityInfoWatch.com*....Joel Griffin

ART & PRODUCTION

Art Director....Bruce Zedler
Production Manager....Jane Pothlanski

SALES CONTACTS

East Coast Sales, SD&I, STE, SIW.com....John Lacasale
john.lacasale@cygnus.com

West Coast Sales, SD&I, STE, SIW.com....Bobbie Ferraro
bobbie.ferraro@cygnus.com

Midwest Sales, SD&I, STE, SIW.com, Locksmith Ledger, LocksmithLedger.com....Brian Lowy
brian.lowy@cygnus.com

Display/Classified Sales, SD&I, STE, SIW.com, SD&I, STE, SIW.com, Locksmith Ledger, LocksmithLedger.com....Erica Finger
erica.finger@cygnus.com

List Rental....Elizabeth Jackson
ejackson@meritdirect.com

SUBSCRIPTIONS CUSTOMER SERVICE

Toll-Free (877) 382-9187; Local (847) 559-7598
Email: Circ.SecDealer@omedia.com

REPRINTS

To purchase article reprints please contact Nick Iademarco at Wright's Media: 1-877-652-5295 ext.102 or by e-mail at *niademarco@wrightsmedia.com*

CYGNUS BUSINESS MEDIA

CEO....John French
CFO....Paul Bonaiuto
EVP Public Safety & Security....Scott Bieda
VP Events, Public Safety & Security....Ed Nichols
VP Production Operations....Curt Pordes
VP Audience Development....Julie Nachtigal
VP Technology....Eric Kammerzelt
VP Human Resources....Ed Wood

ADVERTISER'S INDEX

Visit Cygnus Security Media on the Web at www.SecurityInfoWatch.com

Access Control Solutions That Go Beyond Security

Kaba offers more than security solutions. Our products accommodate various platforms, integrate into diverse infrastructures, ensure a solid investment, but mostly, provide users and organizations value-added benefits.

Simplex mechanical pushbutton locks **simplify security**– there are no cards or keys to manage.

PowerPlex 2000 self-powered lock **supports sustainability initiatives** with the elimination of batteries.

I.AM biometric reader with fingerprint template distribution **improves efficiencies** by eliminating enrolling users at each reader.

79 Locks with contactless credentials **enable convenience;** users engage a lock by simply presenting a fob, keycard or wristband.

E-Plex Enterprise System with Wireless Option **streamlines operations**; locks and users are managed from a central workstation.

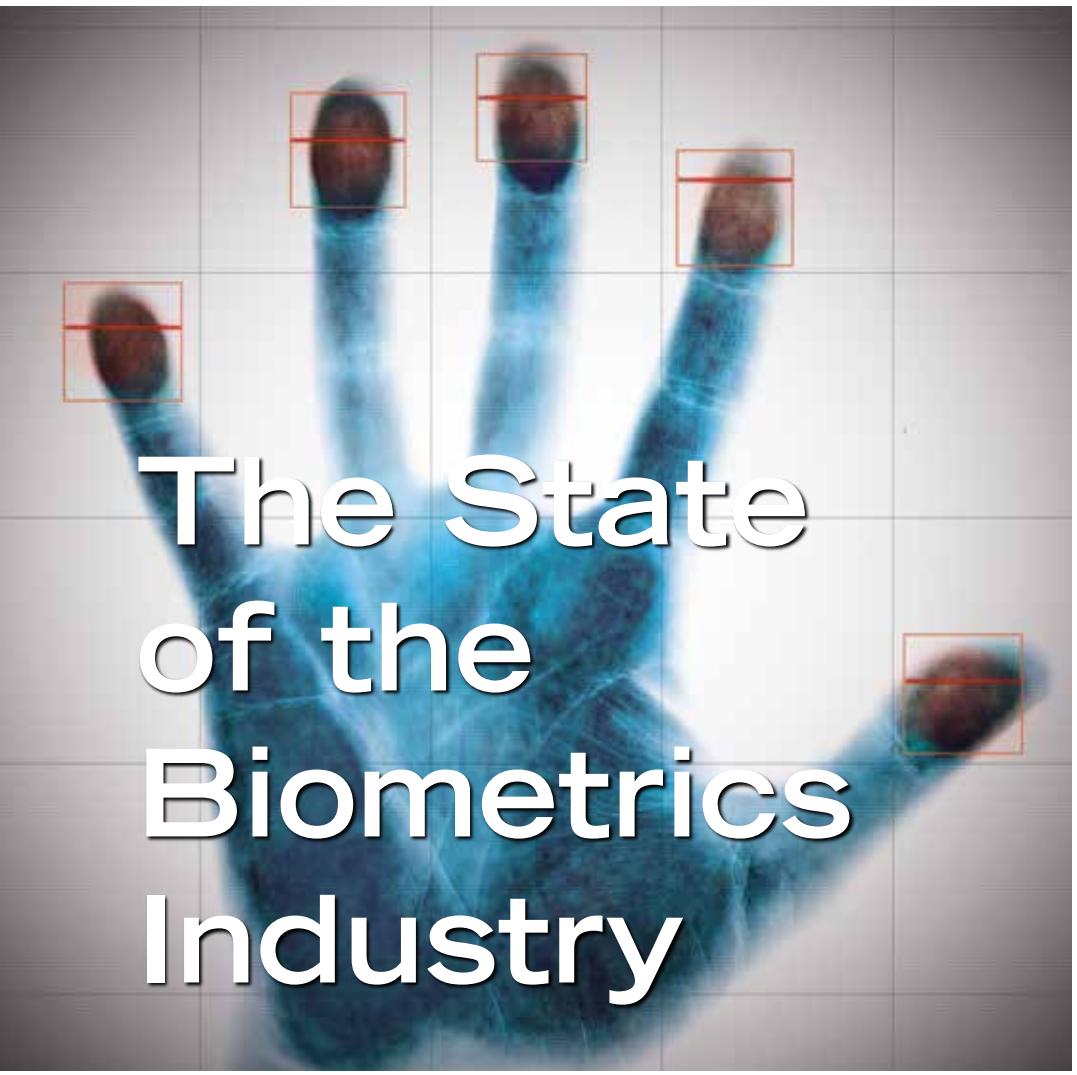
BEYOND SECURITY

KABA®

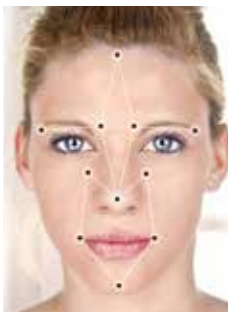
Kaba Access & Data Systems Americas • 1.800.849.8324 • www.kaba-adsamericas.com

Request information: www.SecurityInfoWatch.com/10214145

By Paul Rothman



The State of the Biometrics Industry



Expert vendors discuss where the technology is and where it's going in this exclusive roundtable-in-print

For an access control and identification technology that has been around for so long, biometrics really seems to get a bad rap in the security industry. Past mistakes by some vendors led to bringing some products to market that were unreliable or did not perform up to promised expectations.

Today's biometric technologies have evolved quite a bit — so much so that they have made the quantum leap to security reliability. Readers have become more dependable, false acceptance and rejections are being held to a bare minimum, and new biometric indicators are being introduced all the time. In this rapidly changing technology environment, it would certainly be helpful to today's security practitioners, dealers and integrators to know the "state of the industry" when it comes to biometrics. I recently sat down with four leading biometrics vendors to get the lowdown on where the technology is, where it's going, and overcoming negative perceptions that have plagued biometrics in the past. Participants in this exclusive

Today, managing risk, security & budgets can be a big balancing act

Continental's Integrated Enterprise Access, Video, Locking & Alarm System is the budget-stretching solution

CA3000 flexibly integrates all, in one cost-effective, interoperable high-speed platform. Continental offers enterprise security & facility managers today's leading-edge features in an easy, low-maintenance system, accelerating our own optimized hardware and software, seamlessly scalable for 1 to over 32,000 doors.

Not to bring up the elephant in the room, but unlike other manufacturers who keep discontinuing systems or forcing clients to changeover, Continental systems have earned the enviable reputation for being extremely long-lived, providing painless legacy and retrofit support of multiple technologies, and being field upgradable to grow with you through the years. *New! Optional Yearly Upgrade & Retrofit Rebate Programs, too.*

- Multi-stage threat level- & visitor-management & lock-down
- Software runs as a service
- LDAP Active Directory compliant
- More Choice in Video/DVR partners: Milestone™, Pelco™ DS/DX, Salient™, Hitron™, Integral™
- Trilogy Networx® Access Locks act as single door controllers, built-in HID prox reader, door position, REX & power – no wires.
- Super fast, field-upgradable, 2-, 4-, 8-, 16- Door Controllers
- Remote web management, standard
- FIPS/CAC/TWIC & biometrics

New Accelaterm™ 8 to 16 Door Controller - superfast door open times under ¼ second, and 921 Kbps processing for full data downloads of tens-of-thousands of cardholders in minutes

Continental Access
A Napco Security Group Company

1.800.645.9445 • www.cicaccess.com • salesinfo@cicaccess.com

Request information: www.SecurityInfoWatch.com/10213301

technology roundtable-in-print are:

Mark Clifton, VP of Products and Services for SRI International (To request more info on the company, visit www.SecurityInfoWatch.com/10501284);

Gary Jones, Business Unit Director for Biometric Access & Time Solutions at SAFRAN MorphoTrak (www.SecurityInfoWatch.com/10215933);

Derek Northrope, Senior Consultant and Head of Biometrics at *Fujitsu* Canada (www.SecurityInfoWatch.com/10813662); and

Bill Spence, VP of North America, Europe and Australia sales for Lumidigm, a part of HID Global (www.SecurityInfoWatch.com/10406617).

In the past, some advanced biometric technologies have been overhyped, and others didn't deliver results as advertised. What are you doing to attack this negative market perception issue among security end-users and dealer/integrators?

Northrope: Fujitsu is involved globally in both biometrics standards and industry groups. The only effective way to counter both negative perceptions and incorrect assumptions is through education. Some biometric modalities are not well-suited for certain applications and are likely to fail; other biometrics implementations may fail for other reasons. Either way, "biometrics" is blamed regardless of the root cause of the issues. The main thing we can do is educate through our own customer successes and honest discussions about what biometrics can and cannot do.

Spence: We do two things. First, we explain and show how multi-spectral imaging is a sophisticated technology specifically developed to overcome the fingerprint capture problems that conventional imaging systems have in less-than-ideal conditions. This more-effective technology is based on the use of multiple spectrums of light and advanced polarization techniques to extract unique fingerprint characteristics from both the surface and subsurface of the skin. That subsurface capability is important because the fingerprint ridges seen on the surface of the finger have their foundation beneath the surface of the skin, in the capillary beds and other sub-dermal structures. Unlike surface fingerprint characteristics, which can be obscured during imaging by moisture, dirt or wear, the "inner fingerprint" lies undisturbed and unaltered beneath the surface. Secondly, we reference customers who use our biometrics on the front end. Lumidigm readers are used at several of the world's most famous amusement parks, at the Hong Kong border crossing, by the South Korean Immigration agency, tracking the vaccinations of children in developing countries and at ATMs throughout Brazil and Argentina, among others.

Clifton: SRI is working the ease of use, accuracy, and cost ends of the problems. Historically, the intrusive nature of traditional biometrics solutions contributed to inefficiencies; in fact, many of the programs we have won are a result of the customer being sold a biometric solution that simply does not work or does not apply in a particular circumstance. For example, if a biometric system requires contact, it should not be used in an unclean environment such as a construction site. SRI is focused on overcoming negative market perception through the development and commercialization of non-contact iris biometrics solutions that eliminate many impediments to free flow access by operating within the natural process people use to enter, traverse and exit facilities. These biometric solutions are unmatched in reliability — a person's irises are stable from age 3, and each iris has more than 250 points of identification, resulting in one of the lowest false accept rates of any biometric. We are also continuing to educate the market through hands-on demonstrations and pilot programs.

Jones: Morpho counters this negative perception by developing high-quality products and investing heavily in R&D. We invest 9 percent of annual revenue, and 30 percent of Morpho's workforce is dedicated to research and development. The importance we place in R&D permeates all aspects of our business. Morpho fingerprint algorithms are NIST #1-ranked for enrollment and matching accuracy; and with iris and face identification, Morpho was also ranked #1 by NIST for accuracy and #2 respectively. We've created a robust optical fingerprint sensor with a large acquisition area for high quality image capture. This durable optical sensor combined with the accuracy of our fingerprint algorithms ensures successful implementations in harsh and challenging environments. This year we're launching a small table top device that achieves contactless four finger the acquisition in a single motion. We've already integrated this contactless acquisition device into our access control enrollment process. A final example of hard-driving R&D is the launch of a combined Morpho/Bioscrypt biometric reader, the MorphoAccess SIGMA, less than two years after integrating L1 Bioscrypt.

"As biometric solutions reach lower price points, people become more knowledgeable of the value, and the products become easier to use, the accessible markets will expand exponentially."

— Mark Clifton of SRI International

920/920P

Stand Alone Digital Access Control

SDC's EntryCheck® heavy duty digital keypads* are designed to control a single access point up to 500 users. There's even a wireless, electronic battery solution for up to 3,000 users. When paired with other SDC access control components, compatibility is guaranteed!

For details and specifications: SDCSecurity.com/Solution23

Recessed

Narrow Design

High Security

Wireless

Multi-Application Product Line™

5 YEAR WARRANTY

shipQUICK®

SDCSecurity.com • 800.413.8783 • service@sdcsecurity.com

SDC Security Door Controls

* All EntryCheck® keypads are Uniform Keyboard Programmable™ for convenience and available with optional HID ProxCard or ProxKey fob compatibility.

Request information: www.SecurityInfoWatch.com/10214991

Should there be a set of accepted biometric standards in the security industry? Would this help to quell some of the negative perceptions mentioned above?

Clifton: Today, end-users cannot objectively compare the speed, accuracy, or efficiency of different modality biometric products given how differently each one is specified. Accepted biometric standards would make it easier for end-users to compare and understand the available products and how they would satisfy their requirements. Clear standards enable end-users to make informed decisions that will eliminate these negative perceptions.

Jones: Yes, the security industry would greatly benefit from agreeing biometric standards, particularly for enrollment. Quality enrollments are the most important aspect of any biometric system. Some of this work is already achieved through the groundwork of the Personal Identity Verification (PIV) section of the Federal Information Processing Standard Publication 201-1 (FIPS 201-1). Also the biometric algorithm testing done by the National Institute of Standards and Technology (NIST) needs to be brought to the fore, as does the Image Quality Standards (IQS) and testing carried out by the FBI on fingerprint scanners. The adoption by the wider security industry of aspects of these established standards would be a good way to build industry trust in biometric technology.

"The security industry would greatly benefit from agreeing biometric standards, particularly for enrollment. Quality enrollments are the most important aspect of any biometric system."

— Gary Jones of MorphoTrak

Spence: There are some standards that can help the industry, such as those that define a consistent way to store a user's biometric data. These are called template standards and provide for interoperability of biometric data across sensors from different manufacturers. Some standards could have a negative impact. If the standard tries to define how to capture the biometric, it would stymie innovation. For example, if the standard insisted on using the direct contact method of fingerprinting, people would continue to have problems with dirt, humidity and dryness. Unfortunately, standards that would impose performance requirements would be troublesome as well, given the huge array of applications. The needs of a nuclear power plant are very different from the needs of a theme park. Integrators need to determine what aspects of performance are important to their customers and understand how well a particular device meets those needs.

Northrope: As the saying goes, "The best thing about standards is there are so many to choose from," so it really depends on whether you are asking about global, local or industry standards and, further, whether they are capture, processing, privacy, data transfer or storage standards. By and large, there are standards at every horizontal and vertical, and often more than one. The issue tends to be understanding all of the complexities and the different standards, and being knowledgeable enough to appropriately educate others.

"The only effective way to counter both negative perceptions and incorrect assumptions is through education. The main thing we can do is educate through our own customer successes and honest discussions about what biometrics can and cannot do."

— Fujitsu's Derek Northrope

Taking the market perception into perspective, what's your pitch to end-users on moving to a biometric solution, especially as it relates to TCO and ROI?

Jones: Strong biometric technology is an investment that can easily last 10 years or more as demonstrated with most of our large clients. The equipment requires little or no maintenance and can dramatically reduce administrative costs often associated with traditional PIN- or token-based systems. For ROI, biometric-based solutions reduce card management costs, reduce fraud and time-and-attendance abuses like "buddy punching." For service-based companies like fitness clubs, a biometric ensures paying customers receive services.

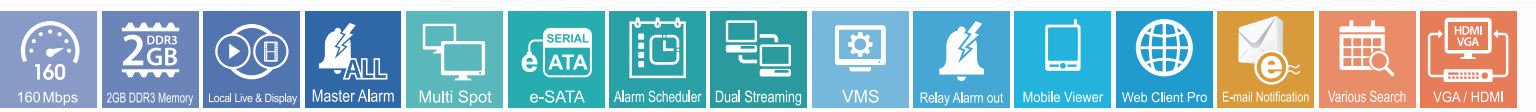
Northrope: Our perspective differs for different markets. If it is a government client, TCO is less important than identity assurance. For certain industries, TCO can be tied to compliance risks, and for others, it is a straight ROI conversation. It is important to note, however, that TCO/ROI

We'll Make You Easy

Premium Standalone *NVR*

NS3552 Standalone NVR

NH1551 Standalone NVR



Max. **160 Mbps** up to **32CH**

Quick and **Easy** camera connection

Local Live and **Playback**

Intuitive and **User Friendly** operating system

Supporting **Various IP Cameras**

TOPNOS® 14 Goodyear, Suite 110, Irvine, CA 92618, USA **Tel** 1-949-502-0680 **Fax** 1-949-435-6269 **E-mail** info@topnos.com CTR®

Request information: www.SecurityInfoWatch.com/10828857

does not take into account the cost of "NOT deploying" as it relates to security risks like physical/data access or integrity.

Spence: Biometrics provide more security, more certainty about who is transacting, more privacy, ease of use, regulatory compliance, cost savings, more convenience, and on and on. Whether the application or use-case is a serious commercial enterprise application, civil program or just a personal security assistant, the value and benefit of biometrics is and will likely continue to be compelling. The most important aspect of selecting a biometric technology is whether or not it actually works in the application. Integrators should beware of selecting a biometric reader based on cost alone. What is the cost to the integrator of having the customer continually complain and having to make service call after service call? What's the cost when asked to remove a system that doesn't work?

"The most important aspect of selecting a biometric technology is whether or not it actually works in the application. Integrators should beware of selecting a biometric reader based on cost alone."

— Lumidigm's Bill Spence

Clifton: Traditional access control approaches are not meeting increasingly complex and multi-faceted security challenges. Codes and cards are easily lost, forgotten, stolen or shared. Estimates vary, but simply resetting or replacing passwords and cards can cost between $150 and $200 per employee or customer per year. Badges, PIN codes, and even some biometric solutions can impede the free flow of facility access. Traditional access control methods may tell you what has happened in the building (i.e., a badge has been swiped or a PIN code has been entered into a door lock), but do not provide certainty that the individual associated with the product is the one in fact using it. Non-contact iris recognition solutions like SRI's Iris on the Move provide the speed of swiping an access card with the unmatched security of biometrics.

As a whole, where does our industry stand as far as pricing for biometrics? If the cost to deploy a system has come down, what are the reasons for that decline?

Spence: As with any type of hardware, technology and the volume of production will lower price; but this is a topic that can get integrators into a whole lot of trouble. The biometric being sold must meet the true needs of the application. If the biometric does not work all of the time on the smartphone, the world doesn't end. It has an easy override. But, if the biometric system isn't working at a border crossing with 400,000 people a day using it, there are big problems. When viewed in that context, the cost of a few extra dollars for the reader that works vs. the reader that doesn't will be negligible to the end-user.

Jones: Cost has reduced significantly over the past 10 years due in part to the evolution of key components such as processors, memory and displays. In addition, the U.S. market is aggressively priced. We pass on the cost savings to our customers that were provided by lessons learned. For example, we train end-user staff in best practices for a quality biometric enrollment, which helps ensure fewer false rejections/acceptances, faster identification and greater overall user acceptance.

Clifton: Iris biometric products are benefiting from the commoditization of high-performance cameras and the continued price reduction in processing capabilities and memory. This trend will continue over the next decade. It is anticipated that within the next three years we could see iris biometric products become ubiquitous for access control, time-and-attendance and critical infrastructure. The confluence of these technologies will see iris biometric hardware costs drop by an order of magnitude in the not too distant future.

Northrope: The reasons are fairly consistent across the market and include — Economies of scale: Delivery models like "cloud" or SaaS-based offerings; Innovation: End-point devices featuring biometrics modules (iPhone, Samsung Galaxy S5, etc.), as well as apps on those devices that can perform biometric functions (face, voice, etc.); and ROI on research cost over time.

Does the increase in biometric methods available beyond fingerprinting add or detract to the market as a whole?

Northrope: Without a doubt, the increase in biometric modalities adds to the market. If you ignore cultural or privacy concerns around fingerprints and focus just on environment factors, in areas where dirt, disease or extreme cold can rule out a standard fingerprint sensor, the ability to have a non-contact biometric is critical in filling those gaps. In addition, the ability to provide multi-modal solutions that incorporate both fingerprint and other, non-traditional modalities enhances security significantly.

Spence: Competition is good. When looking at a biometric solution, the integrator must balance the needs between security of the system with

access control for your Whole Facility without the Holes

DKS Wireless expansion boards can connect card readers and keypads to a DKS telephone entry or access controller without digging or trenching to run wiring. This is a great time, labor and money saver! Visit the link to find the perfect solution to wireless access control in even the most remote locations, or where wiring is impractical.

New Wireless Option

For more information:
doorking.com/turnkey

DKS DOORKING

Parking Control | Access Control | Telephone Entry | Gate Operators

Member: AFA, DASMA, NAA, IDA, NOMMA, NPA, SIA, SSA

Request information: www.SecurityInfoWatch.com/10213482

ease of use of the system. That's the bottom line and the more people who invest in creating solid biometric systems that fall between those needs, the better it is for end-users, integrators and the biometric industry itself.

Clifton: The addition of iris biometrics to the marketplace satisfies a market segment that fingerprinting cannot satisfy — specifically those applications where the end-user prefers a contactless solution and requires the authentication accuracy of iris biometrics.

Jones: While consumers consider other modalities such as facial and iris recognition, and as biometric algorithms and capture hardware improve, fingerprint will continue to be the most robust, least expensive biometric — easily adaptable to environment with the smallest template footprint. Unfortunately many of the negative experiences caused by weaker fingerprint technologies in the early 2000s are being replayed in other biometric modalities where the inexperience of newer vendors results in lackluster performance. This risk needs to be carefully managed through education of dealers and end-users.

How are vendors making it easier to integrate biometrics into existing access control infrastructures?

Jones: We facilitate all kinds of biometric technology integration, not just access control, by providing SDKs with APIs. This allows infrastructures to associate biometric with UN and PW, User and ID. In this way, we take advantage of existing systems with the concept designed for the specific operations and business logic. We also incorporate multiple communication interfaces into our readers that allow information exchange with new and legacy systems.

Spence: Since biometrics are often added to existing systems, integrators need to look at how new networking technologies can make a big difference in the cost of adding biometrics. Options such as wireless connectivity and Power over Ethernet (PoE) can reduce installation costs dramatically. Using the read/write capabilities of existing access control cards enables a user's template be placed on the card, potentially eliminating the need to connect the biometric readers to a network.

Clifton: SRI recently introduced a new IOM product specifically designed for integrating biometric identification into existing security systems. Additionally, we continue to expand the number of access control back ends that the IOM systems are integrated and certified with, such as AMAG Technology's Symmetry v7.0.1 Security Management System access control software.

Northrope: We are seeing more and more physical devices that can bolt straight onto existing security infrastructure via wiegand, card readers or IP connections.

Most of us know that government is a leading adopter of biometrics — in what other markets can dealers/integrators find sustained success in deploying them?

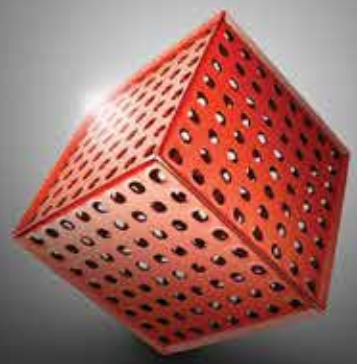
Northrope: We are seeing a large uptake in industries where there is a large amount of government compliance, high-security requirements or large amounts of fraud. These include healthcare, retail, financial services, mobility and data centers.

Clifton: As biometric solutions reach lower price points, people become more knowledgeable of the value, and the products become easier to use, the accessible markets will expand exponentially. It is reasonable to believe that we will see biometrics become commonplace in consumer, industrial, mobile, and automotive applications over the next few years. We are also seeing adoption by major financial institutions, educational institutions, amusement venues, construction sites, and industrial industries —really any place where a higher-level authentication is necessary and where throughput and convenience are required.

Jones: Many verticals can benefit from the security and convenience biometric technology has to offer: Social Services: Childcare, financial support benefits to eligible clients — when fraud is reduced more individuals receive services providing a better ROI for taxpayer dollars; Industrial environments, where only individuals with training and certification are allowed to modify or take control of machinery; plus manufacturing, mining, construction, agriculture and other wage-based market sectors.

Spence: Beyond government customers, we're finding biometrics in a variety of applications. The accelerated use of electronic data for health records, prescriptions, drug interaction checks, clinical decision support and other systems has created the need to validate the identity of the person who is requesting access with the right level of assurance at all points of access. In medical settings, multispectral imaging biometrics even let workers keep their gloves on when using the reader. Data centers also require high security combined with convenience for the user. Amusement parks use biometrics for entry into their facilities. Convenience-oriented applications provide great opportunities for biometrics, such as at time and attendance stations or at athletic clubs where the biometric can be the only credential used. Kiosks for self-service applications and visitor control are naturals for biometrics. In banks, biometrics provide easy access for customers to enter the safety deposit area. Casinos use biometrics to enter cash rooms. The list is infinite. ■

Paul Rothman is Editor-in-Chief of Security Dealer & Integrator (SD&I) magazine. Visit www.secdealer.com to read the latest issue.



What's in a box?

The legacy that 22 years of leadership brings.

The reassurance of the most proven subsystem in the industry.

The knowledge that what is supposed to work, always works.

The quality that comes from an ethic of pride in engineering.

And thanks to the flexibility of an open platform,

the promise that we will never build obsolescence,

or force our partners

into a box.

AUTHENTIC MERCURY™

Mercury Platinum Elite Partners: your valued source for Authentic Mercury .

Honeywell · LENEL United Technologies · OPEN OPTIONS ACCESS TECHNOLOGY · RS2 Technologies

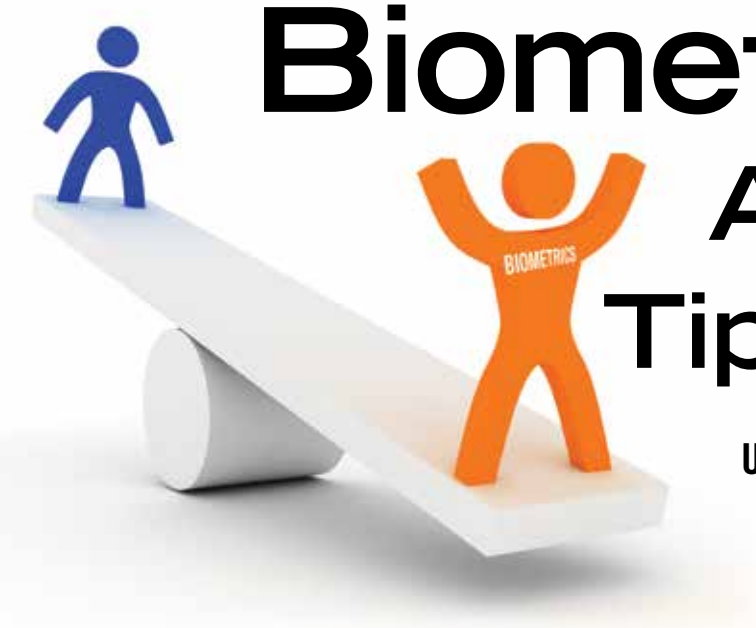
Give your access control solution wings.

MERCURY™ SECURITY

Request information: www.SecurityInfoWatch.com/10214361

By Gale Johnson

Biometrics At The Tipping Point



Using biometrics in multiple-factor authentication provides a higher level of security and faster throughput

Biometrics is not a new phenomenon. Drawings made during the cave man era show a palm print identifier made by the artist. Five hundred years ago the Chinese used palm and footprints as a means of child identity. Certain skull measurements and lengths of fingers were used to assist in identifying individual criminals during the 19th century.

A popular use for biometrics during the 20th century has been to maintain identities of criminals. Any other use for biometrics was seldom considered due to the extended amount of time it took to manually search fingerprint records in order to find a possible match. Today's electronic systems can search through thousands of fingerprint files within seconds, and manufacturers have quickly found new ways to add biometric devices to the list of available access control credentials.

Credentials used for controlling access come in several forms. A long-standing credential has been a mechanical key. Electronic devices are taking an increasing share of the access control field and keypads requiring PINs were one of the earliest credentials to be used. Card access systems have an increasing role as an access control credential. Early cards contained bar codes. Bar code cards evolved into magnetic stripe cards. Proximity card usage has become predominant over the last decade while smart proximity cards which contain additional security against cloning are slowly supplanting the original proximity card systems. A current addition to the list of access control credentials is the smart phone.

Additional security can be gained by requiring dual credentials such as a keypad code and a card. But keys, keypads, cards and smart phones have one thing in common. A PIN or a physical object such as a key, card or phone can be transferred from one person to another. When a key, card or PIN code is used, there is no way to be certain that only the authorized person has used one of these transferrable credentials.

Non-Transferrable

Biometric credentials are not transferrable. A biometric credential cannot be lost or stolen. Authorization for gaining access depends on 'who,' 'what' and 'why.' Biometrics is the only available credential today which can positively answer the 'who' question.

Biometric measurements are said to be different for each person in the world. Even a close similarity is estimated to only occur in one case out of 60 billion humans.

Biometrics can be used in two different ways. Police use biometrics for identification. Fingerprints taken from a criminal are compared to a huge database of fingerprints. If a match is found, that criminal can be positively identified. The same is true for DNA. But the high cost of equipment used for searching large databases and the time involved in conducting the search make biometrics identification an unwieldy system for building access control purposes.

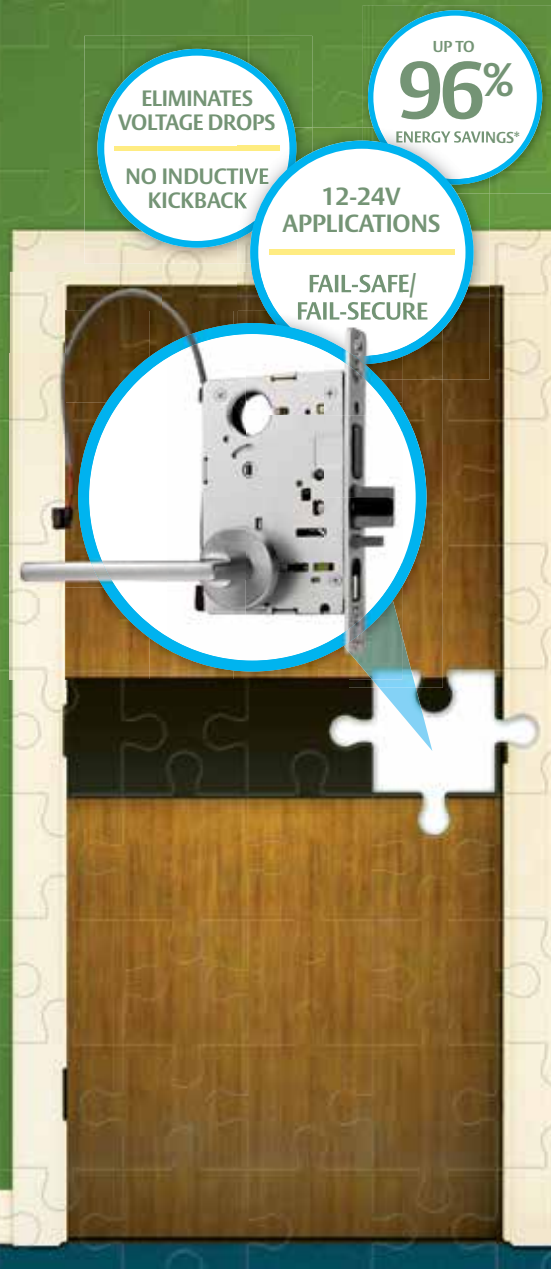
Because the police use fingerprints for identification, some people have grown to believe that fingerprint readers could be an invasion of privacy. People may think that a fingerprint used by an access control system may somehow be added to a police identification program. But biometric Information contained in an access control system is saved as a mathematical formula, not as a real fingerprint picture. Information from a fingerprint or hand scan is changed to a similar mathematical formula and the mathematics are compared. Mathematical access control biometric readings are not usable by the police for identification purposes.

Authentication

Biometrics can also be used for authentication. By developing a small list of biometric scans only for the group of people who are allowed to enter a given area, the authentication search through this short list can be completed in milliseconds. If two credentials are used, such as a proximity card and biometrics, a search is only required to cross-reference the card holder to the one biometrics listing for that individual and the search process can be accomplished even faster.

Always The Right Fit.

Introducing The Ecoflex™ Lock.



*Versus standard electrified mortise locks

The versatile mortise lock that fits all of your needs.

ASSA ABLOY

Discover the Ecoflex™ Lock, an innovation in mortise lock technology that makes your job easier. With the strength and durability of Grade 1 hardware from CORBIN RUSSWIN and SARGENT, this single lock can be field configured to fail-safe or fail-secure.

SUSTAINABILITY
Get up to 96% energy savings with lower operating cost, fewer power supplies and improved battery life.

VERSATILITY
Reduce costs and inventory space with a single field-selectable lock for fail-safe/fail-secure and 12-24V applications.

RELIABILITY
Eliminate voltage drops and inductive kickback, while increasing performance and peace of mind.

Available from ASSA ABLOY Group brands: **CORBIN RUSSWIN | SARGENT**

Find the key to simplifying lock deployment:
www.intelligentopenings.com/ecoflex

Scan this QR code using your mobile phone to learn more.

The global leader in door opening solutions

Request information: www.SecurityInfoWatch.com/10212899

Q & A: Zwipe's Kim Humborstad

Zwipe puts the fingerprint reader on the smart card

Zwipe is an example of how biometrics technology is being utilized in the access control field. Zwipe technology consists of a small fingerprint reader mounted into special cards. Zwipe cards can be configured to operate with an existing building card-based access control system. A card holder must touch the fingerprint reader on the card while using the Zwipe card. Cards are activated and access is granted only if card-holder biometrics data matches the biometrics data pre-enrolled on the card.

Fingerprint data is captured by the on-card fingerprint scanner and is thereafter encrypted and stored only inside the card. No exchange of data is conducted with external systems. This provides secure template management since the fingerprint never leaves the card. It also eliminates user concerns with privacy issues. The card is unique to the user and only the authorized card holder can activate card communication with the reader. When a positive match occurs, the Zwipe biometric card will activate encrypted communication with the lock or reader in the same way as other ISO 14443 contactless smart cards.

Zwipe CEO Kim Humborstad answered our questions about Zwipe.

What technology is the Zwipe credential? It there proximity capability?

Zwipe is compatible with 125 khz Prox, 13.56Mhz Mifare Classic and 13.56 Mhz Mifare Desfire.

Where has this product been deployed?

It is deployed in commercial office buildings (banks, lawyer offices, etc) and universities (to protect labs).

What are the benefits for the user?

No PIN numbers to remember, no external databases (fingerprint data never leaves the card), easy to operate.

What are the benefits for building management?

Lost or stolen cards no longer pose a security threat. Cards cannot be passed from person to person which creates an ironclad audit trail. The system operates with existing contactless readers and is highly secure and trustworthy.

If the credential is stolen, what prevents the fingerprint template from being cloned?

It is impossible to get the fingerprint template.

How is a fingerprint enrolled?

It is similar to enrollment on an iPhone 5. Enrollment is directly on the card. The first time a person uses the card, he or she must touch the sensor on the card several times until a complete template is made.

What fingerscan algorithm is used and can its parameters be 'tuned'?

The algorithm is proprietary to Zwipe. It has been developed over a five-year period and is patent protected. Some of its features include ultra-low power consumption and a robust detection method. It will only detect live fingers.

How durable is the finger scanner?

It is tested mechanically with more than 10 million usages (in a machine).

Is special apparatus or software required to deploy or manage the credentials?

No special apparatus or software is required. However, we do offer a web-based tool to support the enrollment process. Standard access control equipment is used for implementing the card into the existing card access system.

Do end-users enroll more than one finger (in case the primary finger is injured)?

Yes, it is possible to enroll all 10 fingers in our new card.

What is the advantage of offering this product to their access control customers?

You are now able to offer a biometric solution to customers who already have a card-based access control system and generate a new revenue stream.

Where can Zwipe products be purchased?

Cards are sold through the Farpointe channel in the United States. For more information, visit www.zwipe.com.

Fingerprint identification is the most widely recognized type of biometrics. A simple finger touch on a small reader screen begins the authentication process. Security product manufacturers are also offering products for conducting hand geometry scans, facial geometry scans and iris scans. Some scanning systems only require a user to be in close proximity to the viewing screen. As example, a user might put his hand on a wire rack and the reader will take an image of the hand characteristics for authentication. In the work-a-day world many people are not prepared to stand patiently in front of a facial viewer or spread their fingers as needed for a hand scan. Improvements in the usage comfort level of these products may be required before they gain wider acceptance.

Drawbacks To Biometric Authentication

Drawbacks to biometric authentication include limited amounts of individuals who can be enrolled in a access control system before the authentication process becomes too slow for normal usage. At one time a generally accepted figure was approximately a maximum of 200 users. Maximum users allowed in an access control system have increased as the capability of computers has increased. Access control systems on some college campuses now have biometric users ranging in the tens of thousands.

Accuracy in biometrics readings is measured by False Rejection Rate (FRR) or False Acceptance Rate (FAR). FRR is a measure of the percentage of authorized persons who are rejected by the system and cannot enter. FAR is a measure of the percentage of unauthorized persons who are wrongly allowed to enter. Manufacturers have developed several methods of using smaller or larger amounts of biometric information to determine authentication. When using more information, authentication may be more accurate but the process may be slowed. When using less information, authentication may be determined more quickly but the chances of a false reading may increase.

Modern fingerprint sensors use multiple spectrums of light to determine fingerprint characteristics from both the skin surface and below the skin surface. Moisture, dirt and blemishes can obscure readings on the skin surface but lower levels of the skin can provide added information to fill in any missing information before authentication.

Past and present access control credentials have closely followed public demand. Keys, keypads, cards and even cellphones are devices which can be touched and held. As public awareness of the electronic evolution continues to grow, increased acceptance of new and different ways of personal identification will follow. Use of biometrics in the access control field is a logical progression of events whose time has come. ■

Gale Johnson is Editor-in-Chief of Locksmith Ledger magazine. Visit www.locksmithledger.com to read the latest issue.

The Goal of Access Control

How to attain a high level of school security without it looking like a prison

No one will argue that keeping students, faculty and staff safe during and after school hours is a top priority. Most schools have some security measures in place that limit or control access to a campus as well as monitor or restrict students' or visitors' actions on campus. These measures can include: Video surveillance, identification badges, access control systems, telephone/emergency call systems, electronic notification systems, metal detectors, and school resource officers.

According to the *2012 Indicators of School Crime and Safety Report* from the U.S. Department of Education, many public K-12 schools had already deployed security solutions by the 2009-10 school years:

61 % use one or more security cameras to monitor the school;

63 % of faculty and staff are required to wear badges or picture IDs;

92 % have controlled access to the building during school hours;

74 % have telephone systems in classrooms;

63 % use of an electronic notification system for school-wide emergency notification; and

43 % reported the presence of one or more security staff at their school once a week during the school year.

While these security choices vary in scope and scale, decisions to use any as a singular or multi-part solution should not compromise the learning experience or the community environment. But what is the right recipe for success? *How do schools attain a high level of security without looking like a prison?*

An access control system is a good start — it is unobtrusive yet effective. In practice, an access control system regulates the entry of people and property in a building, and in some cases, monitors movement and captures data. Systems can range from traditional mechanical lock and keys to more sophisticated electronic access control systems.

In a perfect world, an access control system would keep out all unauthorized individuals or intruders under any circumstance. Unfortunately, there is no perfect world. The Sandy Hook shooter, for example, gained access into the Connecticut school by breaking through a glass panel that was located next to the school's *locked* front entrance doors. Still, an access control system that enables the remote closing and securing of doors or lockdowns can limit an intruder's access to potential targets.

There are several lockdown methods, including manual with a key, local with a remote fob, or centralized via computer. When applicable, lockdown enables teachers to lock the outside lever without ever opening the door to the corridor, while still allowing free egress.

Case in Point:
Linden School No. 10

Linden Public Schools serve more than 6,000 students from pre-kindergarten through 12th grade via one high school, two middle schools and ten grade schools. Like all schools in New Jersey, they are required to follow fire and school security drills in accordance with the School Security Drill Law enacted by New Jersey's Senate and General Assembly.

According to the 2010 law, schools must conduct one fire drill and one school security drill each month during

Linden School No. 10's gymnasium was also equipped with the E-Plex 5700 locks.

school hours. Twice a year, schools are also required to hold a drill that addresses: active shooter scenarios, evacuation (non-fire), bomb threats and lockdown.

Following a local bank robbery that put the suspect within the vicinity of the Linden School No. 10, district officials called in Maffey's Security Group, Elizabeth, N.J., to implement an access control system. "After the bank robbery, the school decided to install an access control system that included a lockdown feature," says Jeff Strangio, a Maffey's account executive. "The bank robbery caused a lockdown, which is an appropriate response when a dangerous person(s) is thought to be on or near the premises — it minimizes the risk of exposing the students to danger and demands a law enforcement response.

"Prior to joining Maffey's, I worked as a locksmith for the board of education," Strangio continues. "I understand the day-to-day operations of a school as well as standard drills, including fire and security — and my experience helped me recommend a system that would accommodate the school's everyday use and emergencies."

At School No. 10, Maffey's installed the Kaba E-Plex Enterprise Access Control System with Wireless Option and E-Plex 5700 Locks. The system employs Kaba ZigBee Gateways and Routers, which enable communication between the locks and the school system's main server. "The system runs off PoE (Power over Ethernet) through the backbone of the school," Strangio notes. "The system does not piggyback on WiFi; it operates in the 2.4 GHz frequency and has 16 available channels."

Maffey's installed five Gateways/Routers — two outside in NEMA 4 enclosures and three inside the building. This configuration ensures maximum communication coverage. In this installation, Maffey's employed resources from both sides of its business: the mechanical side for lock installation and the electronic side for cable installation to the Gateways/Routers.

Maffey's installed E-Plex 5700 Locks on 13 perimeter doors and 29 interior doors, including classroom and office doors, the library, gym, nursery and storage area. The locks' "LectroBolt" technology allowed Maffey's to easily install them on doors with no wires to or through the door. Enterprise Software installed on the system administrator's computer enables school officials to monitor and control access points from a central location. The software can accommodate up

Maffey's installed E-Plex 5700 Locks on 13 perimeter doors and 29 interior doors at New Jersey's Linden School No. 10.

The system administrator can remotely log into the system and initiate lockdown.

E-Plex ZigBee Gateways and Routers enable communication between the locks and the school's main server. For maximum coverage, two were installed outside in NEMA 4 enclosures and three were installed inside the school.

to 3,000 users, 16 access schedules, 32 holiday/vacation blocks and 30,000 audit events. The wireless capability delivers near real-time functionality and eliminates Linden personnel from visiting individual doors when adding/deleting users or changing lock attributes. The main dashboard provides a visual representation of the system's performance and events, such as door status, signal strength and emergency lockdown/unlock commands.

"Once we had the system up and running, we tested its lockdown feature," Strangio says. "It was great — after initiation, it took only nine seconds for the locks to go into lockdown mode." To activate lockdown, authorized user(s) simply click on the System Lockdown icon, which is located in the lower right-hand corner of the dashboard. Once in an emergency lockdown state, the mechanical override key or Normal Operation command on the dashboard will open the lock; and no other valid user credential will open the door unless the system settings have been customized and key override is not the default.

"The system administrator can also log into the system from a remote site and initiate lockdown," Strangio adds. "We also installed a keypad outside the principal's office, which allows the principal or secretary to initiate a lockdown. In addition to the lockdown feature, it was important that the system have high availability. Since the system runs 24/7 on the district's main server and the locks are battery powered, we are assured that the system does not go offline.

"The teachers find it easier to get in and out of the building as well as find the building more secure," Strangio continues. "Before the Kaba system, teachers used keys to enter their classrooms; now they just enter their PIN into the lock to gain access."

E-Plex 5700 Locks can accept either a PIN, PROX card or both and offer several user parameter options, including code length, anti-tamper lockout, and re-lock time. The school has not migrated to PROX cards; however, the system is flexible and modular, so the school can integrate them at a later date.

Linden Public Schools assigned School No. 10 a full semester to use and test the system and currently there are no bugs to work out. "I am confident that once the other schools see what School No. 10 has implemented, they will go with what works and what has been proven," Strangio says. ■

Editor's note: To request more information about Kaba access control systems, please visit www.SecurityInfoWatch.com/10214145 or www.LocksmithLedger.com/ 10173518.

Systems without Limits,
INNOVATION without BOUNDARIES

Keyscan's innovative "hybrid" approach to network appliance-based access control architecture provides unmatched flexibility when handling new installations or legacy system takeovers.

Keyscan gives cost effective ways to replace existing access control infrastructure while, in many cases, utilizing existing cabling, readers and credentials allowing you to easily revitalize aged or failing access control systems.

For new installations that demand an IP "at-the-edge" solution, our line of network appliance-based access control units, as well as our single-door PoE equipped controller, conveniently address these requirements without the need for extensive cabling runs and increased installation time.

It is this "hybrid" approach that keeps Keyscan at the forefront and further distinguishes us with our uncompromising approach to the access control marketplace.

For the very best in access control, contact Keyscan today.

WWW.KEYSCAN.CA 1-888-KEYSCAN (539-7226)

KEYSCAN ACCESS CONTROL SYSTEMS FROM KEYSCAN INC.

Access Control Management Software

Readers & Credentials

Centrally Managed & Hosted Services

Door and Elevator Floor Controllers

Request information: www.SecurityInfoWatch.com/10214172

By Fernando Pires

Key management systems are ideal for use in a data center facility security plan because they offer a variety of control and usage options.

(Image Courtesy of BigStock.com)

Key management systems enhance data center's physical security

Employing a multi-layered approach optimizes physical protection of highly sensitive areas

Protecting data centers from hackers, unauthorized access by employees or other threats demands constant attention, proactive thinking and implementation of today's best technology. While definitive precautions are usually taken to secure the network, basic physical security procedures for securing the data center itself are often not as well thought out.

For many organizations, the answer lies in multiple layers and types of safeguards including physical measures such as video surveillance or mantraps and established policies and procedures that limit physical access such as the use of key management and access control systems.

Systems offer reliable industry standard features

Key control systems are designed to securely hold keys and automatically track key usage. They are an industry standard in casinos used to secure access to cash and chips; in prisons to secure and automate access to facility keys; and in housing complexes, automobile dealerships, hotels, school campuses and myriad other applications. Advanced systems can also secure card access badges as well as provide safe storage for smaller valuable items such as cash boxes, mobile devices and weapons.

To access a stored key or badge, the authorized user simply enters his or her personal identification code on the keypad. When the system verifies the user, the door will open and the location of the requested key will light up. Key control systems can also be configured with card readers or biometric readers and can be networked for centralized control. At any time, security operations can view the

MARKSUSA®

We at Marks USA are here to supply your business with quality products at competitive prices.
Let Marks USA be your ***"Independent Locking Source"***.

Grades 1 & 2
Cylindrical Survivor Leversets


195/26D


195


LocDown™ by MARKSUSA
LA318GJ

BHMA CERTIFIED


175/26D

LifeSaver™ by MARKSUSA


5SS19FD/32D

1SS55N/32D


195SSF/32D

BHMA CERTIFIED

- **BHMA Certified**
- **Heavy Duty ANSI UL Listed Grade One Product**
- **Manufactured by Marks USA and Meets "Buy America"**
- **Lifetime Mechanical Warranty**

NOVA Series Mortise Locksets


5DR96FD/32D

BHMA CERTIFIED


5RR57FD/26D

Hospital Push/Pull Paddlesets


1PDN/32D


5PDN/32D


Schlage® Large Format

HI-SECURITY™ Cylinders


Mortise Rim Combo


Key-In-Knob

Custom Lockset Division


The Plaza


Barbizon Plate


Lucida Lever


Trump Tower

Grade 1 Panic Devices


M9900

Access Control


iQ WIK LITE

www.MARKSUSA.com • 800-526-0233 • 631-225-5400 • Fax: 631-225-6136

status of any key in the system; quickly locate any key in the system; determine who currently has which keys out and for what area and when they are scheduled to be returned; or determine who has had keys out, for what areas and when. Keys can be returned to any cabinet in the system, but if a key is not returned when scheduled, e-mail alerts and text messages can be sent to selected individuals to enable quick action.

Versatile designs offer 24/7 safeguards and protection

Key management systems are ideal for use in a data center facility security plan because they offer a variety of control and usage options. A basic application would entail enrollment of individuals based on their function. For example, an operations center engineer can be authorized for 24/7 key access, whereas a technician may be restricted to accessing a particular key at certain times and for specific amounts of time.

The versatility of the key control systems also lends itself to more complex applications in larger data center environments, as when multiple pieces of identification are needed to move about the data center. For example, a general access badge would allow the employee entrance to the building and a second badge would be used to access internal areas of the data center facility. To maintain tight security, the internal access badge would be secured in a key cabinet when not in use by the authorized employee.

Retrieving the internal access badge from the key cabinet would require the employee's general access badge, along with any other access credentials, such as biometric ID or a PIN code, to open the key control cabinet. Once the employee's identity and permissions have been verified in the system, the location of the person's badge would light up and the locking mechanism would automatically allow removal of the internal access badge and insertion of general access badge, securing it in the same location. The reverse process would apply when the employee left the building, with all activity automatically recorded for auditing purposes.

As the world continues to virtualize, more and more sensitive information is being stored on the cloud. This data can be extremely sensitive and is continually under attack from outside and inside influences. Although there is no simple one-stop solution for protecting electronic files, a well implemented key management system can be a valuable tool in the ongoing battle to safeguard this data.

Fernando Pires is vice president of sales and marketing for Morse Watchmans. To request more information about the company, visit www.securityinfowatch.com/10214428.

Multi-Function Door Alarm

STI's Exit Stopper series helps solve the problem of unauthorized exits and entries of fire or emergency doors. The multi-function door alarm alerts if a protected door is opened by emitting an ear piercing alarm for 30 seconds, three minutes or continuously (preset by the user). Another option is annunciator mode. A key operated override will silence the alarm and allow authorized exits.
Request more info at www.SecurityInfoWatch.com//11525737

Security Management Software

Version 6 of the eFusion security management software from Maxxess Systems adds Windows 8.1 and Windows Server 2012 support; hardware support for suppliers such as PCSC, Assa Abloy, Schlage and Salto; and biometric enrollment for L1/Bioscrypt and FaceKey systems. The software can be downloaded via the Maxxess Partner Portal.
Request more info at www.SecurityInfoWatch.com/11386324

Legacy System Upgrade

The Symmetry SR-2000 Controller from AMAG Technology is a four-door control panel designed for plug-and-play upgrade of Picture Perfect and other legacy Casi Rusco and similar systems. It includes a four-door controller board with input/output (I/O), database unit, and it can be installed in existing enclosures.
Request more info at www.SecurityInfoWatch.com/11313684

Digital Door Lock

The RITE Touch digital glass door lock from Adams Rite, an ASSA ABLOY Group company, features a thin, low-profile design and sleek Magic Mirror user interface, to offer sophisticated styling and convenience. It requires no holes or other modifications to the door, making installation quick and easy. The lock offers single or double glass door compatibility and dual credential access control via card reader or PIN code.
Request more info at www.SecurityInfoWatch.com/11313651

Request information: www.SecurityInfoWatch.com/10215166

Delayed Egress Maglocks

Dortronics Systems has introduced two electromagnetic locks for use with a variety of door and frame types. The 1107xD maglock is designed to fit narrow style header applications. Its 1¼-inch depth reduces the need for angle mounting brackets and filler plates, lowering installation time and costs. The 1107xEDR delayed egress actuating maglock operates with the 7101-P Delayed Egress Panel and is designed with a field-adjustable actuator that senses door movement.

Request more info at www.SecurityInfoWatch.com/11363706

Indicator for Rim Exit Devices

SARGENT is now offering an Indicator option on its 8816 Series rim exit device. The 8816 offers an easy way to lock the outside trim of an exit device from the inside without opening the door. The indicator, located on the exit device chassis, displays whether or not the door has been secured by the cylinder on the inside of the room.

Request more info at www.LocksmithLedger.com/11489759

Gate Intercom & Control

The GateGuard Wireless Access Control System from Ritron allows wireless two-way voice communication with visitors and remote control of gates for optimum security and convenience. Portable radio-equipped personnel can talk with visitors and activate a gate from anywhere in a facility. A compact base station radio is also available and provides an AC powered, "fixed" station for two-way communication and remote-control. The rugged, industrial-grade system allows long-range communications (up to 2 miles, line-of-sight), is weather-proof and tamper resistant.

Request more info at www.SecurityInfoWatch.com/11525733

PoE-Capable Locking Hardware

SDC's Power over Ethernet (PoE)-Capable Locking Hardware can be installed and connected to an access control system via ordinary Ethernet network cables, which facilitate power. The products enable installers to forego pulling power lines when electric power is not within reach and installing power supplies and controllers for access control devices. Existing Ethernet cables can also be used. The equipment is part of SDC's earth-friendly line, making them a great green solution.

Request more info at www.SecurityInfoWatch.com/11416159

Restricted Access System

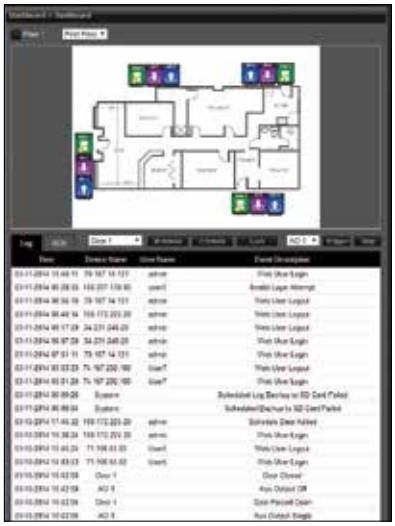
Designed to ensure healthcare facilities can control access in critical areas such as nurseries, operating suites, pharmacies and dementia-care facilities, the Restricted Access System from Detex features a range of door hardware. Components include: Advantex Panic Hardware with a 15-second delayed egress alarm; access control with immediate entry via keypad or card reader; single-person entry (anti-tailgate) that allows only one authorized entry at a time; and door-propped alarms. All components are field-proven to work together.

Request more info at www.SecurityInfoWatch.com/10951394

Wireless Expansion Boards

DoorKing has unveiled DKS Wireless Expansion Boards for its 1830 series of telephone entry and access control products, which make it possible to add up to 16 card readers (or other access devices) to an access control system without the need for additional wire runs. Each board also acts as a repeater station to provide for longer distances, or individual repeater units are available when an access control device is not needed.

Request more info at www.SecurityInfoWatch.com/10876480



Browser-Based Access Control

Linear Enterprise is a browser-based, embedded network appliance and access control system available through select Linear dealers and equipped for large-scale installations. It offers remote management, low total cost of ownership (TCO), an easy path to VMS integration, and a unique license key system that makes integration and expansion easy. A Remote Management Console (RMC) allows dealers to provide secure offsite management for one or many systems without having a server in the cloud.

Request more info at www.SecurityInfoWatch.com/11364475

Networked Locks

Alarm Lock's Trilogy Networx Lock line eliminates door-to-door operations, such as programming up to 5,000 users and/or audit trail collection, by communicating wirelessly via Ethernet or 802.11. Additionally, the locks offer global network-wide features, including system-wide global lockdown/unlock in under 10 seconds from any lock or the network's PC and Remote Management via VPN-connection. The locks integrate with Lenel OnGuard v6.6 and 6.5, as well as with Continental CardAccess 3000, making them an ideal intelligent edge device.

Request more info at www.SecurityInfoWatch.com/10216505

Key Management Solution

The CaptureTech Key Management Solution uses RFID and barcode technology to more efficiently, securely and reliably manage keys. The solution includes KeyCop, a tamper-evident, RFID-enabled seal to which keys are attached; CaptureTech's modular key management software application; and KeyConductor, an Electronic Key Cabinet. Using either barcode or RFID technology depending on the number of keys, the KeyConductor allows authorized users to log into the system via an integrated keypad and display.

Request more info at www.SecurityInfoWatch.com/11525723

ID Card Issuance Software

Card Encoding Engine (CEE) software from CardLogix offers a no-programming solution for chip and magnetic encoding as well as card personalization on a range of ID credentials. Pre-configured to automate smart card encoding without programming, scripts or custom APIs, it saves a card issuer $5,000 to $15,000 per card type. It seamlessly connects with card configuration tools, biometric enrollment software, vetting services, credential management systems, and end-use applications. It includes a dual-interface reader and a variety of cards.

Request more info at www.SecurityInfoWatch.com/11525743

Access Control Management Solution

The Access Manager 300 (AM300) and Door Unit 500 (AD500) system from Kaba ADS enables access control capabilities without the installation of software or servers. An embedded application on the AM300 manages data directly on the device - users type the IP address into a web browser and log into the system for administration, viewing events and running reports. Connect up to eight Kaba I.AM Fingerprint Key Readers, or eight Wiegand RFID readers, or a combination.

Request more info at www.SecurityInfoWatch.com/10987554

Enterprise Access Control Software

ContinentalAccess, a division of Napco Security Technologies, has released CA3000 version 2.9 access control software provides robust access control functionality and seamless integration with alarms, locking and a growing list of video systems. It includes the ability to run the CardAccess 3000 and associated applications as Windows services and the ability to control access to the software's GUI using Lightweight Directory Access Protocol (LDAP). Support for the Continental's Super-Speed 16 door Accelaterm Controller is also available.

Request more info at www.SecurityInfoWatch.com/10834305

Access Control Software for SMBs

Bosch Security Systems Inc. has introduced Access Professional Edition (APE) 3.0 access control software for small and medium enterprises.New features include integrated map viewer support and more flexible enrollment options. The integrated map viewer increases the situational awareness surrounding alarms and can be combined with video surveillance for a better overview. Readers attached to the Access Modular Controller (AMC) can be used for the enrollment of all card technologies and allows for flexible end-to-end solutions.

Request more info at www.SecurityInfoWatch.com/11518097

CREATING THE FUTURE OF SECURITY . . . TODAY

The Security Professionals' first choice for today's security infrastructure, from one room to multi-location complexes around the world. Our reputation is based on a time-honored tradition of rock-solid quality, premium reliability and the integrity of DSX and our network of factory-trained, authorized dealers and support.

When you are staking your reputation on a solution – choose the most powerful and intelligent access control systems in the world, choose the total security relationship with DSX.

- No "Per Seat" Licensing In System Pricing
- LAN/WAN Compatible
- Smart Card and Biometric Integration
- Unlimited Access Levels Per Cardholder
- Integrated Photo ID Badging
- Backup SQL Server

DSX Access Systems, Inc.

www.dsxinc.com

10731 Rockwall Road | Dallas, TX USA 75238-1219
888.419.8353 | 214.553.6140 | sales@dsxinc.com

- Backwards Compatible Architecture
- Alarm Text Message/ E-Mail Notification
- Hot Swap Redundant Communication Server
- High Level Elevator Control Interface
- Integrated Wireless Locksets

Quality. Reliability. Integrity. The Security Professionals' First Choice.

Request information: www.SecurityInfoWatch.com/10214208

Switch to the access control that changes with you.

Move to HID Global's adaptable iCLASS SE® Platform and start using the technology of tomorrow, today.

HID®

When it comes to access control, it can be difficult to stay ahead of changing security concerns and technology demands. Go with HID Global's iCLASS SE® Platform—the new standard in access control that positions you for the future with an open, adaptable solution that easily integrates smart cards, mobile devices and whatever tomorrow brings. Join the revolution in evolution and get greater security, flexibility and simplicity.

Make your change by visiting hidglobal.com/change-STE

Request information:
www.SecurityInfoWatch.com/10213866