ACCESS CONTROL 2021

TRENDS & TECHNOLOGY

Supplement to Locksmith Ledger International, Security Business, Security Technology Executive

ACCESS CONTROL

ALL IN WITH DIGITIZATION

www.LocksmithLedger.com
www.SecurityInfoWatch.com

July/August 2021

ENDEAVOR BUSINESS MEDIA

SECLOCK

On this path, choice and compatibility are, well, compatible.

Making building entrances secure is a serious business. So we stock a vast selection of top security systems — and offer deep technical expertise to ensure solutions are compatible.

LCN SCHLAGE VON DUPRIN

info@seclock.com 800.847.5625 seclock.com

Request information: www.SecurityInfoWatch.com/10215009

Universal Access Control (UAC) from Immix® Guard Force

Enable RMR with Professional Access Control Monitoring

Monitor multiple disparate enterprise access control platforms from a single interface

Sync with customers' databases in real-time

Receive only the door alarms/events you want with video verification

Control any door you want

Immix® gives you the CHOICE!

immix

immixGF

One Platform. Unlimited Opportunities.

www.ImmixProtect.com

Request information: www.SecurityInfoWatch.com/21152412

VIKING

SECURITY & COMMUNICATION

PROTECTING WHAT MATTERS MOST SINCE 1969

VIKINGELECTRONICS.COM

715.386.8861

PROUDLY MADE AND SUPPORTED IN THE USA

Request information:
www.SecurityInfoWatch.com/10556843

START HERE

Getting Off Prox?

Transition At Your Own Pace.

Going OSDP?

The Lowest TCO In The Market.

Migrating To Mobile?

Do More. Touch Less.

New Build?

Work With Any Access Control System.

wavelynxtech.com

(720) 572-4963

WaveLynx
technologies corporation

Request information: www.SecurityInfoWatch.com/12388450

ACCESS CONTROL 2021
TRENDS & TECHNOLOGY

COVER STORY

FOCUS ON ACCESS CONTROL TECHNOLOGY

COLUMNS

Advertisers' Index

Advertiser Name	Page	WebSite URL
Alarm Lock Systems, Inc.	S7, S47	www.securityinfowatch.com/10212743
Altronix Corporation	S17	www.securityinfowatch.com/10212790
ASSA ABLOY - Electronic Security Hardware	S19	www.securityinfowatch.com/12381564
Banner Solutions	S43	www.securityinfowatch.com/12071932
Camden Door Controls	S27	www.securityinfowatch.com/10213140
Continental Access	S33	www.securityinfowatch.com/10213301
Deister Electronics USA Inc.	S23	www.securityinfowatch.com/10213427
DKS DoorKing Systems	S13	www.securityinfowatch.com/10213482
dormakaba Group	S25	www.securityinfowatch.com/12304402
Identiv	S9	www.securityinfowatch.com/10492079
Immix	S3	www.securityinfowatch.com/21152412
Lockey USA	S29	www.securityinfowatch.com/10215934
Marks USA	S37	www.securityinfowatch.com/10214311
Paxton Inc.	S35	www.securityinfowatch.com/10215750
SALTO Systems Inc	S39	www.securityinfowatch.com/10225529
Seclock	S2	www.securityinfowatch.com/10215009
STI-Safety Technology Int'l	S8	www.securityinfowatch.com/10214881
STid	S30-S31	www.securityinfowatch.com/12266353
Top Notch	S45	www.securityinfowatch.com/12129499
Townsteel Inc.	S46	www.securityinfowatch.com/12361123
Trine Access	S41	www.securityinfowatch.com/10215438
Vanderbilt Industries	S48	www.securityinfowatch.com/11514790
Viking Electronics	S4	www.securityinfowatch.com/10556843
WaveLynx Technologies	S5	www.securityinfowatch.com/12388450

ACCESS CONTROL 2021
TRENDS & TECHNOLOGY

PUBLISHED BY
ENDEAVOR BUSINESS MEDIA

1233 Janesville Ave
Fort Atkinson WI 53538
920-563-6388; 800-547-7377
Access Control – Trends & Technology 2021 is a supplement to *Locksmith Ledger, Security Business* and *Security Technology Executive* magazines.

EDITORIAL
Editorial director | Steve Lasky
Editor, *Locksmith Ledger* | Will Christensen
Editor, *Security Business* | Paul Rothman
Editor, *Security Technology Executive* | Steve Lasky
Editor, SecurityInfoWatch.com | Joel Griffin

SALES
Group Publisher | Nancy Levenson-Brokamp
(847) 454-2702
nancy@securityinfowatch.com

Northeast US & East Canada
SB, STE, SecurityInfoWatch | Janice Welch
(224) 324-8508
janice@securityinfowatch.com

Midwest
***Locksmith Ledger, SB, STE,* SecurityInfoWatch** | Brian Lowy
(847) 454-2724
brlowy@endeavorb2b.com

Western US & Western Canada
***SB, STE,* SecurityInfoWatch** | Bobbie Ferraro
310-800-5252
bobbie@securityinfowatch.com

Display/classified | Kristy Dziukala
(920) 568-8324
kdziukala@endeavorb2b.com

PRODUCTION
Production Manager | Jane Pothlanski
jpothlanski@endeavorb2b.com
Audience Development Manager | Courtney Wethal
cwethal@endeavorb2b.com
Art Director | Kayla Burger
kburger@endeavorb2b.com

ENDEAVOR BUSINESS MEDIA, LLC
Chief Executive Officer | Chris Ferrell
Chief Revenue Officer/CMO | June Griffin
Chief Financial Officer | William Nurthen
Chief Operations Officer | Patrick Raines
Chief Technology Officer | Eric Kammerzelt
Chief Administrative and Legal Officer | Tracy Kane
EVP/Group Publisher | Lester Craft
EVP Special Projects | Kristine Russell

Subscription Customer Service
Toll-Free 877-382-9187; Local 847-559-7598
Circ.SecDealer@omeda.com

Article Reprints • Brett Petillo
Wright's Media 877-652-5295, ext. 118
bpetillo@wrightsmedia.com

Now Available at a Distributor Near You

AirAccess®

Introducing the 1st New Revolutionarily-Easy, Cellular-Based, RMR-Generating Access Control System

The Fastest, Easiest Wireless Access Control System Today's Small/Medium Business Accounts Need & Will Pay More to Love

MAKE MORE MONEY

Build Business from SMB Accounts: 2X the RMR in a fraction of the time. Provide Hosted Access Control &/or Real-Time Monitoring from one simple, scalable, easy-to-bid system with unbeatable flat rate **as low as $19.95/month.**

EASIER & FASTER TO INSTALL

Cellular communications makes direct connections for you, outside your customers' network/IT Dept. Cloud-based software auto-learns system devices, i.e., Top-Rated wireless locks, panel & radio– **Minimal Training – it's purely plug and play.**

CUSTOMERS WANT 24/7 CONTROL FROM ANYWHERE

Easy Mobile App with built-in virtual, universal credential and customizable control of doors, locks, users and more. SMS notifications provide peace-of-mind, keeping accounts connected and in charge of system status or emergencies at their business or office, **with little hardware investment, for lowest TCO.**

Ask for a demo or training today
1.800.ALA.LOCK *or* www.AirAccess.com

AirAccess® by Alarm Lock

Ask for AirAccess Today at a Distributor Near You

Request information: www.SecurityInfoWatch.com/10212743

Time to Embrace Your Digital Self

By Steve Lasky

In the more than three decades that I've been a part of the security industry, an entire lexicon of buzzwords has zipped across my computer screen. From plug-and-play to convergence, interoperability and unified communications, and Cloud to AI. These terms have all been regarded as "disrupters" by industry folk when first crashing the scene. But nothing has approached the level of sheer transformation as the current digital evolution of security technology that is occurring at this moment.

The security industry is facing a huge digital disruption, and to be successful, it needs to embrace digital transformation. Maintaining the status quo will only increase this gap and prevent companies from capitalizing on a valuable opportunity. By challenging conventional thinking and reimagining how business is done, physical security can provide next-level insights, improving life safety and creating value across the organization beyond traditional risk management. This is the conclusion of a recent white paper released in a collaborative effort by Microsoft and Accenture Strategy.

The digital convergence of physical security for both access control and the integrated solutions that can help to amplify an organization's risk mitigation footprint is changing how end-users and systems integrators measure the traditional investment success of hardware and software. Digitization is driving a clearer picture of business paradigms such as return on investment (ROI),

Security professionals are discovering that by going beyond improved responsiveness to threats and more effective risk management, new physical security models that live in a digital platform can deliver faster response times at a lower cost, better security asset utilization, and improved lifecycle management. Additionally, more than 80% of security leaders believe that digital transformation will deliver significant non-financial benefits such as an enhanced employee experience; converged cyber and physical intelligence; and environments that are not only smart but aware.

We are already seeing this in new digitally robust access control solutions. As we enter a new post-pandemic security environment, digital transformation figures to be much more than a passing fad or a fading buzzword. It is the security industry's current course and future destination. AC

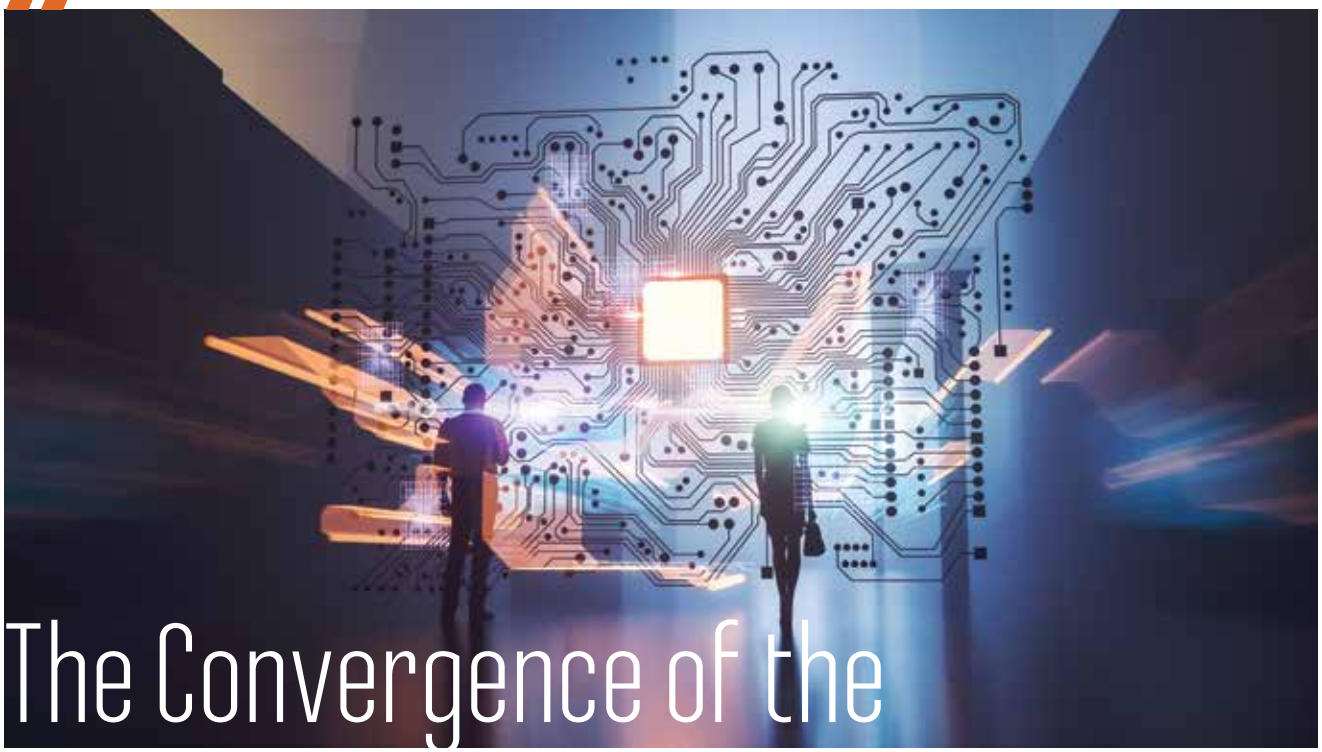
YOUR WORLD, **VERIFIED.**

When it comes to securing anywhere operations, you need the freedom of Access Control as a Service (ACaaS) and 24/7 cloud technology. Verify the right access to the right people at the right time on any device from anywhere in the world with subscription-based Freedom Cloud.

Request information: www.SecurityInfoWatch.com/10492079

go.identiv.com/freedomcloud // sales@identiv.com // +1 888.809.8880

IDENTIV



The Convergence of the Physical and Digital Security Worlds

Courtesy of Getty Images -- Credit: gremlin

Why identity management and access control are no longer separate issues in a post-COVID landscape

by Steve Van Till

In the corporate world, COVID-19 has seriously affected the security sector— both physical and cybersecurity. Traditionally, physical building security and cybersecurity have been viewed as separate disciplines with unique solutions. However, given the changing nature of security risk, organizations need to start taking a more holistic view of security and IT risk management (ITSRM). This means combining the previously disjointed approach to security dispersing ownership between business, security, and IT teams, the purview and guidance of the modern Chief Information Security Officer (CISO)

The corporate world experienced a significant uptick in physical and cybersecurity threats due to the pandemic sending millions of employees home to work. With office complexes and buildings vacated, the properties were ripe for exploitation by bad actors. Physical security breaches were up in 2020 as a result of business closures, contributing to an increase in commercial burglaries in major metropolitan areas. There was a 134% increase in Philadelphia during 2020, for example, and New York saw a 169% increase in the same year.

But the physical world wasn't the only one under fire. A July 2020 study completed by Tanium of 1,000 executives in the U.S., UK, France, and Germany found that 90% of executives surveyed said they experienced an increase in cyberattacks due to the exponential expansion of the threat surface due to a remote workforce.

These statistics showcase the significant increase in risk that corporations are facing from all angles. Combating threats in a pandemic, and in a post-pandemic world requires a broader view of security risk and security management.

While the numbers can make the situation look dire, it's not all bad news. The technology available today makes linking the physical and cybersecurity realms easier than it ever has been before, and the changing role of today's CISO provides a more comprehensive view of keeping all forms of security cohesive, and up to date.

But what are the barriers to bridging these two elements of security?

Identity is the core of security, both cyber and physical, but managing it is very complex

CISOs and their supporting departments struggle with providing the right people with the appropriate level of access to the right technology A 2018 study from Okta found that companies have an average of 129 software applications, with 10% of businesses having more than 200 apps. And that number only increased during 2020, as companies required more technology solutions to support remote work.

Making the situation increasingly difficult is that within each of the 129 applications, employees can have access to various levels of entitlements within the application as a whole. The process of managing this level of provisioning for identity and credential management for all employees that join, leave, or move within the organization is already a high-volume task. Additionally, the expansion of the gig economy has forced corporations to have to factor in additional users that need access to corporate data, tools, content, and access to physical spaces from third parties and contractors, only adding to the overall risk for the organization.

Due to the level of detail that is required to ensure accurate provisions, mistakes are bound to happen. Unfortunately, the mistake that happens most often is leaving users over-entitled due to access that has mounted over time (physical or virtual) for tasks that then never get removed.

Managing that amount of change requires technology to support the process. Identity and access management tools have been heavily invested in by organizations to create central control over access to their virtual networks, applications, and data such as Okta, Microsoft AzureAD, G-Suite and many more. These solutions become the gateway to propagate identities and the correct level of control across the entire environment. These systems are also usually automatically connected to HR solutions to ensure up-to-date and authoritative information is being utilized and is connected to the rest of the organization. Having a link to employee directories allows technology to rapidly identify authorized users and de-provision users to remove facility access quickly and easily.

Unfortunately, that same approach has not necessarily been applied in the physical security world. Much of physical security has been legacy systems that have not necessarily kept up with the evolving nature of identity management and access controls to ensure that the user really is who they claim to be.

Forward-thinking CISOs and CSOs are now looking more broadly at security and how to not only mitigate risk but also how they can make their departments more efficient. These leaders are looking at how they connect the IAM solution to other parts of the organization such as physical access control as a more centralized process as well as ensuring that there is a single record of truth on individual access. These CISOs expect access control solutions to integrate their IAM solutions with their physical credentialing and access control. Ultimately, by doing this, their teams save time and effort, by utilizing a single source of truth for access (physical and virtual), automatically eliminating access upon offboarding.

> CISOs expect access control solutions to integrate their IAM solutions with their physical credentialing and access control.

From a data and risk management perspective, with these systems connected, CISOs and threat analysts in the Security Operations Center (SOC) have more data and visibility as they investigate threats and understand the level of risk or exposure from a cyber and physical event.

Applying cybersecurity practices to the physical world

Centralizing employee information in the company system including credentials, level of access, and privileges ensures all points of vulnerability have been identified, and prevents "privilege creep", where an employee accumulates more access rights than necessary to perform his or her job. The same should be done on the physical access side, to ensure employees only have access to spaces they need to do their job to protect data, privacy, assets and information from possible over-exposure and insider threats.

However, many organizations haven't managed the level of access that they provide to their physical security administrators and users with the same rigor as they do cyber access. Controls need to be put in place to manage what a physical security team can see, do, and act within the security platform itself. The 'guards' put in charge of security need to be provisioned in a granular way to the access control system. It is important to not over-provision users of the security system itself to have more access than is necessary in order to do their job.

For example, let's look at insider threats. Insider threats aren't a new phenomenon, they've been a high priority to detect and deter for years. However, now not only are insiders attempting to steal and disrupt operations in the cyber realm through advanced attacks, but they are now also targeting the physical world through inappropriate access to sensitive areas.

This means that no longer are attacks either cyber or a physical security problem, they are one and the same.

To you help you ensure that you are applying the best practices from IAM to your physical access control solution here are a few tips:

- CISOs — check that your physical security solution has enabled multi-factor authentication (MFA). There are more than 15 billion logins are available for sale on the dark web and your security admins, front desk clerks, guards are all vulnerable to bad password management and hygiene. MFA is the easiest, quickest, and widely supported way to protect from unauthorized access from compromised login credentials. And while the digital world has rapidly adopted this best practice, the physical world is lagging behind.

- Implement a least-privileged approach for admins, security teams and guard access to the physical security system. Why? As shared above, entitlement creep is abundant, and the more access your guards have than is required for their position, the greater the exposure could be from an insider threat or compromised credential to grant excessive access to sensitive spaces across the corporate footprint.

> Combining physical data and cyber analytics creates a powerful, unified view of users and access.

What's the impact? Imagine a bad actor who purchases a security guard's username and password online. Without a second means of authentication, that intruder can slide right into a company's online system. Furthermore, if that security guard has been over-provisioned, the intruder can now grant themselves physical access to whatever they would like, including data centers and server rooms with key confidential information.

Applying the systems of checks and balances that have been proven to be successful in the cyber world to the physical world will not only improve access control to a company's building but ultimately will result in stronger security overall by preventing access to all points of entry.

The changing role of CISOs offer opportunities to make cyber and physical security management cohesive

As threats to cybersecurity are manifesting more and more as gaps in access control, whether that be of the building itself or the data and security centers, it is clear that a cohesive solution is an answer to the problem.

Fortunately, organizations are catching on to the extremely detrimental effects of a security breach and are making structural changes to support the mitigation of cyber and physical security threats. Today's CISO is more important than ever before, with the responsibility of cultivating enterprise-wide security strategy. Having a more comprehensive view of security for the entire organization, rather than disjointed teams handling cyber and physical security needs, dovetails well with the changing need of technology and process solutions to address threats. Additionally, with the greater visibility by the CISO into all aspects of security, he or she can now ensure consistent practices are being implemented to protect the tools that are meant to protect their employees.

Viewing identity management and access control data together can identify new security risks

A June 2020 study by McKinsey & Company found that the pandemic has accelerated the digital economy by seven years. The digital adoption of applications for corporate work, in conjunction with tech solutions for physical security, is not just a temporary fix; these solutions are here to stay.

You've heard it said, 'data is the new oil.' This means that in the age of technology, data is the new commodity that businesses must manage as a rich resource. Managing users' and administrators' identity and access control data in virtual and physical environments with a single framework provides central visibility into individuals' access to all systems and spaces as well as aggregate data on who is utilizing them.

Combining physical data and cyber analytics creates a powerful, unified view of users and access. Advanced analytics can then utilize the combined power of identity data in real and virtual worlds to better detect anomalous activity, identify potential threats to security leaders and support faster, more effective, incident investigations. By integrating identity management and access control together organizations gain a 360-degree view of their facilities to monitor and track access events alongside cyber incidents. Having the ability to manage users and administrators from one framework provides insight into who has access to internal applications and data, as well as which physical location and facility are they accessing it from. Furthermore, integrating video into your access control allows for verification and visual proof in investigations and remediation activities.

This is the true value of connecting IAM with access control platforms — central visibility to control access across the physical and virtual environments. And the further integrated your systems are, the more easily you are able to manage access rights across services, provide centralized compliance reports, and, if needed, provision and de-provision users and administrators quickly. AC

About the author:

Steven Van Till is Co-Founder, President & CEO of Brivo, Inc. a cloud services provider of access control, video surveillance, mobile, and identity solutions delivered as a SaaS offering. He also serves as Chairman of the SIA Standards Committee and is a frequent author and speaker for numerous security publications and forums, and the inventor of several patents in the field of physical security. Van Till was previously Director of Internet Consulting for Sapient Corporation, where he led client strategy engagements for the first wave of the dot.com era. At the healthcare informatics company HCIA, he was responsible for Internet strategy for data analytics services. Steve is the author of "The Five Technological Forces Transforming Physical Security." In his first book, he shares his journey through the surprising ways that the biggest disruptors of our time--cloud, mobile, IoT, social, and big data--are impacting the physical security industry.

BUILD A TOTAL SOLUTION WITH DKS

DKS engineers each product line for seamless integration, providing you with the level of perimeter security, access control and flexibility your property demands.

Whether your location is urban or remote, residential or commercial, maximum security or public access, DKS delivers a complete, full range of safe and secure Access Control, Telephone Entry, Gate Operator, and Traffic Control products to suit your needs.

MADE IN USA

DKS DOORKING®

Traffic Control | Access Control | Telephone Entry | Gate Operators

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

FIND YOUR SOLUTION AT:
doorking.com/TotalSolution
800-673-3299 • info@doorking.com

Request information: www.SecurityInfoWatch.com/10213482

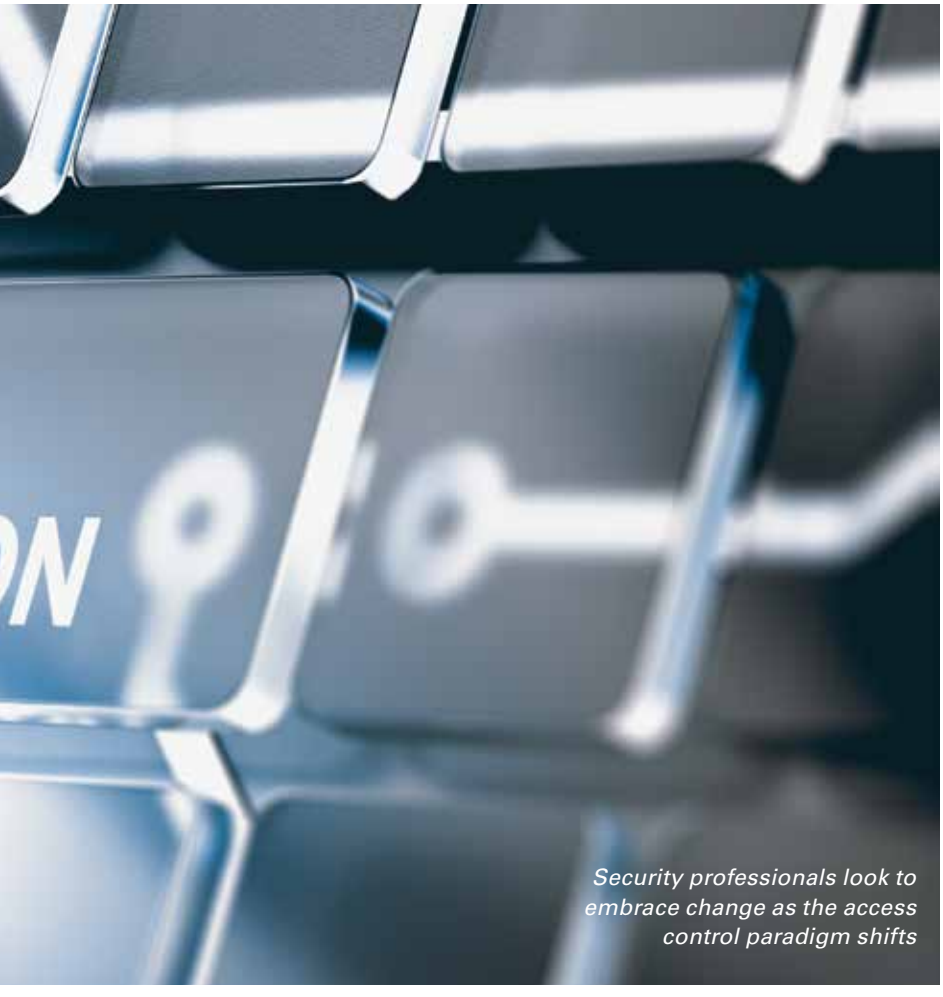
The TRUTHS About Access Control Systems Digitization

What digital transformation means to the physical access control industry and its future impacts

by Lee Odess

The mainstream conversation around digital transformation has been in play for more than three decades. Digital transformation for businesses began with the computerization of processes and, more recently, includes the Internet of Things (IoT), social media, mobility, cloud, augmented reality, big data, blockchain, cryptocurrency, and NFTs. Most industries have felt the massive impacts of digital transformation. For those that were at the beginning of this transformation, the pandemic has accelerated the impacts.

Many experts, such as Chris Barbin, founder of Tercera.io, believe we have entered a part of digital transformation that is the third stage of cloud computing. Chris breaks down the waves in his recent eBook, "What It Takes to Be a Services Leader in the Cloud's Third Wave," The first wave, sparked by the Dot.com era and 9/11, was focused on SaaS applications with the main benefit being about productivity. The second wave, stimulated by the financial crisis, spurred an increased adoption across all business sectors and was all about platforms focused on profitability and production. This brings us to the third wave, accelerated by the pandemic, and it is all about the different cloud architectures (hybrid and multi-cloud) delivering a heightened connectedness and engagement. The main differences between the third wave versus the prior waves are a much more sophisticated customer base, a vast adoption of cloud systems and tools across all business sectors, and a deep understanding of the value created that has moved from nice to have to need to have.



Security professionals look to embrace change as the access control paradigm shifts

Courtesy of Getty Images -- Credit: Olivier Le Moal

Following the Digital Footprints

As per Wikipedia, the definition of digital transformation is "the adoption of digital technology to transform services or businesses through replacing non-digital or manual processes with digital processes or replacing older digital technology with newer digital technology."

While researching this topic, I came across a robust report, "72 Vital Digital Transformation Statistics: 2021/2022 Spending, Adoption, Analysis & Data" where FinancesOnline summarized statistics that relate to this third stage of cloud computing:

- 67% of companies said they were more advanced in using technology than their peers before the crisis, and 56% said they were the first movers to experiment with digital technologies (McKinsey)
- In 2019, 51% of digital transformation efforts stem from growth opportunities. (Altimeter)
- In 2018, 60% of executives say the Internet of Things will play a critical role in their digital business strategy. (IDC)
- the leading technologies already implemented include big data/analytics (58%), mobile technology (59%), and APIs, and embeddable tech (40%).
- In 2018, executives said that digital

Courtesy of Getty Images/By hqrloveq

transformation's top benefits include improvement of operational efficiency (40%), faster time to market (36%), and meeting customer expectations (35%). (PTC)

- less than 30% of technology vendors are active partners in organizations' digital transformation initiatives (PTC).

The good news? There is an enormous amount of opportunity in this third wave of cloud computing. The bad news? It was going time yesterday. If you believe you can't, or won't, or you take a "seen it and done it" approach to this transformation based on legacy mindsets, the changes will drastically impact you and your business negatively.

The security industry is not immune to the impacts of digital transformation, advancements in technology, or customer demands. We are amid this digital transformation, and the decisions organizations make right now centered around change and action will bring immediate results and set the company up for long-term success.

We have been somewhat, not shockingly, late to the game within the physical security industry when embracing and discussing its long and short-term impacts. We have had the luxury of keeping these conversations at a high level, with a macro point of view; but that has all changed. The fact that I am writing this article is a glaring example of how we have been asleep at the switch.

To be clear, it is my point of view that the security industry has been in the midst of a digital transformation for years and it is starting to feel, see, and deal with its actual impacts right now.

"But Lee, my business is growing, my customers are not asking for it, and when I read my favorite blog, I am not hearing about it. Seems like more of the same."

I hear you and you are not wrong. What you are hearing and doing is true, but so is the point of view that it is happening. And here is why:

The Truths About Digital Transformation

Due to the specific period of transformation that we are in, market confusion is prevalent because two truths exist. This period is the definition of a phase change. Our two truths, the phase change, can be categorized as "the old" and "the new." It creates confusion because both truths exist and are genuine. You have old ways continuing (e.g., high security selling prox cards and hearing from their dealers and end-users that mobile is a fad) and new truths introducing themselves (e.g., independent software vendors, also known as ISVs, entering into the high-security market and being a viable channel for our industry. For instance, companies managing identity for enterprises).

The benefit of having two truths is that we as an industry get to work out this new normal being exercised. The bad news of having two truths is that it can create a false sense of confirmation bias where you start to believe your truths and even worse, have an echo chamber also confirm these for you (you hear this when people use the words won't and can't).

Before I get a finger pointed at me as someone who is trying to divide our industry, let me address a couple of things:

- When I say "old," I do not mean "bad." When I say "old," I speak to the historical and traditional ways we've done things as an industry.
- When I say "new," I do not mean "always good" or "better than." When I say "new," I speak about how we will do things as an industry.

I believe the most significant impact of these changes on our industry, both now and tomorrow, is the transmutation of our industry with a mix of old and new, called the "new normal." You hear the term "new normal" used a lot right now when people discuss what work and society will look like when we get on the other side of the pandemic. There are many similarities here. The pandemic has done many things, mostly terrible, but one of the most influential byproducts of the pandemic has been the acceleration in the adoption of new ways of doing things – especially in the security sector. At the same time, there has been the confirmation of some of the old ways - things that will either stay the same or have become augmented to be even better than they were prior to the pandemic. A good example is the movie industry - I believe that being able to watch newly released movies in my home at the same time as the movie is in theatres is an excellent blend of the old and new - ultimately giving the end-user, in this case, me, more choices to craft my experience.

The security industry is not immune to the impacts of digital transformation, advancements in technology, or customer demands.

POWERFUL WAYS TO OPEN NEW DOORS

Altronix®

Designing and deploying access control has never been easier with Altronix power integration solutions. Create more ROI and leave the heavy lifting to us.

YOUR AMERICAN BRAND FOR **ACCESS POWER & CONTROL**

Request information: www.SecurityInfoWatch.com/10212790

Reality Will Drive "New" Truths

With all of that said, I do not believe we will throw out all the old and shepherd in only new. What I think more likely will happen is this:

- Some old truths will die and make way for new truths. For example, our only mission to keep bad people out by being restrictive and binary has forever been changed to also "letting the right people in." This fundamental shift in what we do as an industry challenges how we approach the market, the tools and systems being used, and the mindset needed to deliver for our customers.
- Some old truths will be augmented and made better by new truths. For example, visitor management was a sleepy technical add-on to most access control systems. Post pandemic, it has turned into a dynamic interface and is now more about workflow automation and an identity management solution. Another example is how the definition of safety has changed to include wellness. The changes described result in the increased dependency to apply new technology to old truths to deliver a satisfying solution. In short, most old technology cannot deliver on these new use cases, so you either need to iterate off of the old or innovate new.
- Some new ways are introduced as mainstream solutions, go-to-market strategies, or ways to do business—for example, account-based marketing and selling and access control as a feature of a more significant value proposition. These two new ways of doing business have yielded mainstream investments of more than $500 million, making this no longer a cottage industry focused only on high security. If you believe "it" won't, "it" can't, or that you've seen this before, I recommend revisiting that mindset. This fundamental shift is different.
- Some new ways are introduced but either need more time to marinate or may not come to be realized. A good example here is robotics, touchless solutions, and artificial intelligence at the edge are still being worked out. We are 100% better than yesterday, but there is still work that needs to get done.

For end-users and integrators, I recommend you do the following:

- Challenge yourself to use this pandemic as an opportunity to change your approach, conversations, expectations, partnerships, talent, and technology solutions. Don't fall victim to the belief that you've seen this before and it too shall pass. Chances are, what you selected, installed, and set up five years ago is outdated and not going to meet the new use-cases you have. If your partners or sources of expertise are telling you all the ways you can't, are using yesterday or even today feedback as the compass to where the market is going, and you feel as though you are getting bad advice, trust your instincts.

> The benefit of having two truths is that we as an industry get to work out this new normal being exercised.

- Look forward to where the market is going. While the security industry is doing its best to catch up to cloud computing, the rest of the enterprise technology world has already shifted to a multi-tech architecture that includes onsite, at the edge, and in the cloud computing and is focused on the value creation part of the business. Our industry will follow suit here. We have reached a point where it is no longer about architecture. It is about what the architectures do to support the use cases and needs you have as well as the value they create.

I would stop having architecture conversations and start having conversations about what you want your systems to do. Then match the architecture that makes sense to support it. But do not stop there. Look for hardware solutions that support software and choose more dynamic solutions that go beyond the single note for yesterday's needs. It is a lot easier to change your software and adjust support to a changing environment if your key features are not reliant on the hardware type.

- Consider resetting the expectations of the type of work you do as a security integrator and as an end-user the work you are looking for your security integrator to do. The scope of work a security integrator is being asked to deliver is changing along with the digital transformation. Gartner predicts that 85% of large organizations will engage external service providers to migrate applications to the cloud (up from 43% in 2019). As Chris Barbin states in his eBook, "[those that will lead the third wave] will also need to possess different skill sets, go-to-market strategies and labor and delivery models that fit this new digital era."

Summing It All Up

I personally feel it is impossible to argue that things are not changing. The more productive conversation is around what impacts are the changes having and a discussion around the timing of changes. Then we can talk about what to do about it. The pandemic only accelerated what was happening up to 2019, why not also accelerate our conversations?

What side of this transformation are you going to be on? The one where it happens to you or the one where you help make it happen? I am choosing to embrace the change and am doing my best to help make it happen. I feel that when the dust settles that will be the right side of history. AC

About the author:

Lee Odess is the Founder and CEO of consulting firm Group337 and author of the book, "The 6 Phase Changes Shaping Access Control. He is an industry veteran, having held sales and technology positions with companies like Allegion, UniKey Technologies, Brivo and Lutron Electronics.

Touch-free solutions for high security applications.

ASSA ABLOY
Opening Solutions

Reduce potential touchpoints on highly trafficked openings with HES and Securitron hands-free products:

- Durable Securitron Magnalocks® with patented, instant release circuit – no residual magnetism
- Securitron XMS motion detectors designed to reliably release magnetic locks
- Push buttons from Securitron for secondary egress can be activated with an elbow
- Securitron Touch Sense egress bars to enable hands-free movement through virtually any door
- Intelligent power supplies from Securitron allow remote monitoring of the opening
- HES electric strikes provide automated lock control

Learn more at **assaabloyesh.com/handsfree**

Request information: www.SecurityInfoWatch.com/12381564

Experience a safer and more open world

TOUCHLESS Access Control Continues to Expand its Mission

From a security standpoint, touchless access control remedies common risks caused by human error.

How to create healthy, secure and connected building environments through touchless technologies

by Tony McGraw

As the world begins to reopen amid rapid vaccine distribution, business and organization leaders are tasked with earning back public trust and confidence by delivering safe, healthy and connected building environments. To keep up with the changes, businesses are rapidly adopting and integrating new, data-driven technologies into their existing facility infrastructures to meet evolving expectations and regulations. One of the most impactful solutions leading the way in this adoption wave is touchless access control.

Leveraging touchless technologies, facility touchpoints and occupant interactions can be optimized with powerful artificial intelligence (AI) and machine learning capabilities to deliver a streamlined building experience with minimal touchpoints. With these solutions visibly in place, occupants have peace of mind knowing that their health and wellbeing are protected, allowing them to remain productive and engaged. Connected, data-driven access control solutions create a modern, enhanced healthy building environment that will continue to exceed expectations and pay dividends long after the pandemic has passed.

The Evolution of Touchless Technologies in a Pre-Pandemic World

Despite their sudden rise in adoption, touchless technologies aren't an overnight sensation; in the years leading up to the pandemic, demand for touchless technologies was already gaining steady momentum across many industries. Before the COVID-19 virus turned the world upside down, touchless access control existed as an easy way to improve and streamline security and the occupant experience, alleviating headaches attributed to traditional methods of access control.

From a security standpoint, touchless access control remedies common risks caused by human error. Employee identification badges can be easily lost, while keycodes in the wrong hands pose a dangerous cybersecurity risk. These physical methods of access control can also create opportunities for tailgating, allowing unauthorized personnel to enter buildings undetected. In addition, traditional access control forces individuals to stop at entryways or doorways to swipe their badge or input their keycode, creating traffic bottlenecks and a disjointed occupant experience that can be detrimental to customer and employee well-being.

Certain industries were ahead of the curve and had already led the way

Courtesy of Getty Images -- Credit: martin-dm

in touchless technology adoption pre-pandemic, particularly those that had to manage and track large volumes of ticketed individuals, such as airports and sports and entertainment venues quickly and efficiently. Hospitals had also adopted touchless access to minimize the spread of disease long before COVID-19 was on anyone's radar, and the advanced degree of access control helped safeguard dangerous or vulnerable medical resources and medications like narcotics. Touchless technologies were clearly already positioned to become an industry-wide trend, but the COVID-19 pandemic and the resulting mindset accelerated that demand, turning a trend into a potentially life-saving necessity.

Touchless Access Control Continues to Gain Momentum as COVID-19 Wanes

The COVID-19 pandemic elevated touchless access as the gold standard for health and security. Suddenly, hospitals weren't the only institutions concerned about touch contamination and occupant wellness. From banks to schools, every industry now faces a critical need for clean, healthy and safe building environments. Keypads and access badges became a hotspot for touch contamination, potentially leading to the spread of disease throughout any facility. At the same time, the bottlenecks caused by individuals stopping to swipe their ID or input their keycode was no longer just an annoying nuisance to busy employees and customers, but also an impediment to social distancing efforts. As a result, touchless access control rapidly evolved to keep up with demand, becoming a keystone technology for any facility's security management and pandemic response strategy.

Utilizing the latest in AI-powered facial recognition technology, organizations can completely do away with access badges or keypads, greatly reducing the potential for touch contamination between individuals. By keeping occupants moving even when entering high-security areas, bottlenecks are mitigated, and security personnel can better monitor suspicious behavior as crowds are dispersed. Because every individual is automatically screened by facial recognition technology, security managers and occupants can rest easy knowing only authorized individuals are accessing the building.

In the COVID-19 era, touchless technologies have also grown to include health screening solutions that empower businesses to create and maintain healthy spaces to protect occupants. Elevated skin temperature screening solutions use thermal imaging software to identify individuals quickly and automatically with high temperatures, potentially indicative of fever or illness. Because the solution can screen large volumes of moving people at once, it removes the need for a manned temperature screening checkpoint, alleviating staffing burdens and allowing occupants to quickly and safely get where they need to go. To further prioritize occupant health, social distancing monitoring, contact tracing and mask detection technologies can be integrated to automatically monitor building occupants to ensure all individuals are adhering to safety guidelines.

These health screening and monitoring solutions can be integrated onto a single, cloud-based interface to provide security managers with comprehensive, data-driven and real-time insight into their buildings' overall health status, even when offsite. Should an individual enter the facility with an elevated temperature, remove their mask or break social distancing rules, an alert is automatically sent to a security manager for swift remediation. This cloud-based remote monitoring capability empowers businesses to maintain a healthy, safe and connected environment at all times.

Delivering Optimal Outcomes in Myriad Vertical Markets

While touchless technologies were once considered an industry-specific tool, they are now considered an essential solution for any organization.

They can optimize any building's security strategy to provide data-driven protection, regardless of industry. By integrating these solutions into their existing network of building technologies, businesses and organizations can be empowered to drive the outcomes that matter most for their stakeholders, both during the pandemic and beyond.

- In a healthcare setting, patient arrival areas that can easily become crowded are particularly vulnerable to the spread of disease, and often require an individual to manually screen incoming patients and visitors for symptoms. Implementing elevated skin temperature screening solutions within lobbies or emergency areas streamlines the check-in process and removes the need for manual symptom screening, protecting doctors, nurses and staff in the process. An individual with a high temperature can be quickly navigated to a protected area, minimizing their time spent with healthy fellow patients or staff members without proper personal protective equipment (PPE).
- When airline tickets are replaced with facial recognition and retina scanning, airport security processes will be streamlined, allowing travelers to get where they need to go faster. This will have a positive effect on airports' bottom lines: the quicker travelers get through security, the faster they are able to explore the airport's dining and shopping opportunities, ultimately generating critical nonaeronautical revenue. By keeping security lines moving, airports will also ensure travelers are able to maintain social distancing guidelines to create a safe and healthy passenger experience without letting anything slip through the cracks at a security level.
- Within an office building, touchless access control allows employees to move throughout without worrying about the risk of infection found in traditional access control, allowing them to remain healthy and productive. Social distance monitoring tools can send employees real-time alerts through their mobile devices with mass notification systems if they violate social distancing protocol. Building administrators can also leverage mass notification tools to aid in contact tracing and redirecting foot traffic in case of a positive diagnosis. The investment in employees' health, wellness and comfort can also improve employee satisfaction, enhancing workforce development and retainment efforts.
- In a school or college campus, traditional access control can place students and faculty at risk. Campus facilities like dormitories are particularly vulnerable to tailgating, and K-12 schools, unfortunately, face an increased threat of violent incidents. As a result, administrators need to know who is entering their facilities at all times, especially during the pandemic when social distancing and contact tracing are common practices. Facial recognition technology used in touchless access control gives them that real-time insight into their buildings' comings and goings, providing an extra degree of protection at all times.

Across industries, organizations found their need for healthy, safe and connected building environments fiercely intensified by the pandemic. Through the strategic implementation of touchless technologies, any building can deliver streamlined occupant experiences that mitigate risk and surpass expectations.

> Despite their sudden rise in adoption, touchless technologies aren't an overnight sensation. It's up to business owners and security managers to rise to this challenge and reinstate confidence by leveraging intelligent and connected touchless solutions.

Touchless Technologies Redefine the Modern, Healthy Building

As the world adapted to the pandemic over the last year, occupants' expectations have rapidly evolved; whether they are an employee, patient, customer or visitor, they expect the spaces and places they spend time in to demonstrably invest in their health and wellbeing while maintaining an enjoyable experience. Even with vaccines being distributed around the world, the public's new, heightened awareness of health and safety risks means this desire for an optimized building environment is unlikely to fade.

It's up to business owners and security managers to rise to this challenge and reinstate confidence by leveraging intelligent and connected touchless solutions. By integrating touchless technologies like biometric access control, elevated skin temperature screening solutions, face mask detection and social distance monitoring solutions, organizations can not only navigate today's challenges and meet consumer demand but future-proof their facilities as well. The resulting facility connects every data touchpoint to create a modern environment that is healthy, safe and ready for anything. AC

About the author:

Tony McGraw serves as vice president and general manager of security solutions at Johnson Controls, a global leader for smart, healthy and sustainable buildings. He brings more than two decades of leadership in security and operations to his current role in helping realize safer and healthier buildings to improve customer and occupant experience.

Electronic Key Control & Asset Management Solutions

deister electronic

Securely Store, Manage and Account for Keys and Assets Instantly

- Quick and Efficiently issue keys and assets to users
- Audit Trail of all Transactions
- Secure access with use of Pincode, Card or Biometrics
- Scalable solution that manages up to 384 keys in a single cabinet
- Ask about our near touchless options
- Integrates with many of the leading Access Control Systems

The Future of Reader Technology

The new Infinity Reader™ series

- Multi-Technology Reader (125 kHz, 13.56 MHz, NFC & Bluetooth®)
- OSDP/Wiegand Auto-Detect
- Supports OSDP File Transfer - configuration and firmware reflash
- 3 separate LEDs helps those who are visually impaired
- UL Listed for both Indoor & Outdoor Installation
- Reader Configuration and Firmware are field upgradeable

UL LISTED · OSDP · HID Prox · EM 4102 · MIFARE DESFire EV1 / EV2 · (PIV) · CASI-RUSCO PROXLITE · HID iCLASS · ISO 14443 A/B · KANTECH · ISO 15693 · AWID · MIFARE Classic

Deister Electronics USA, Inc., 8576 Wellington Road, Manassas, VA 20109 USA 703.368.2739 www.us.deister.com

Request information: www.SecurityInfoWatch.com/10213427

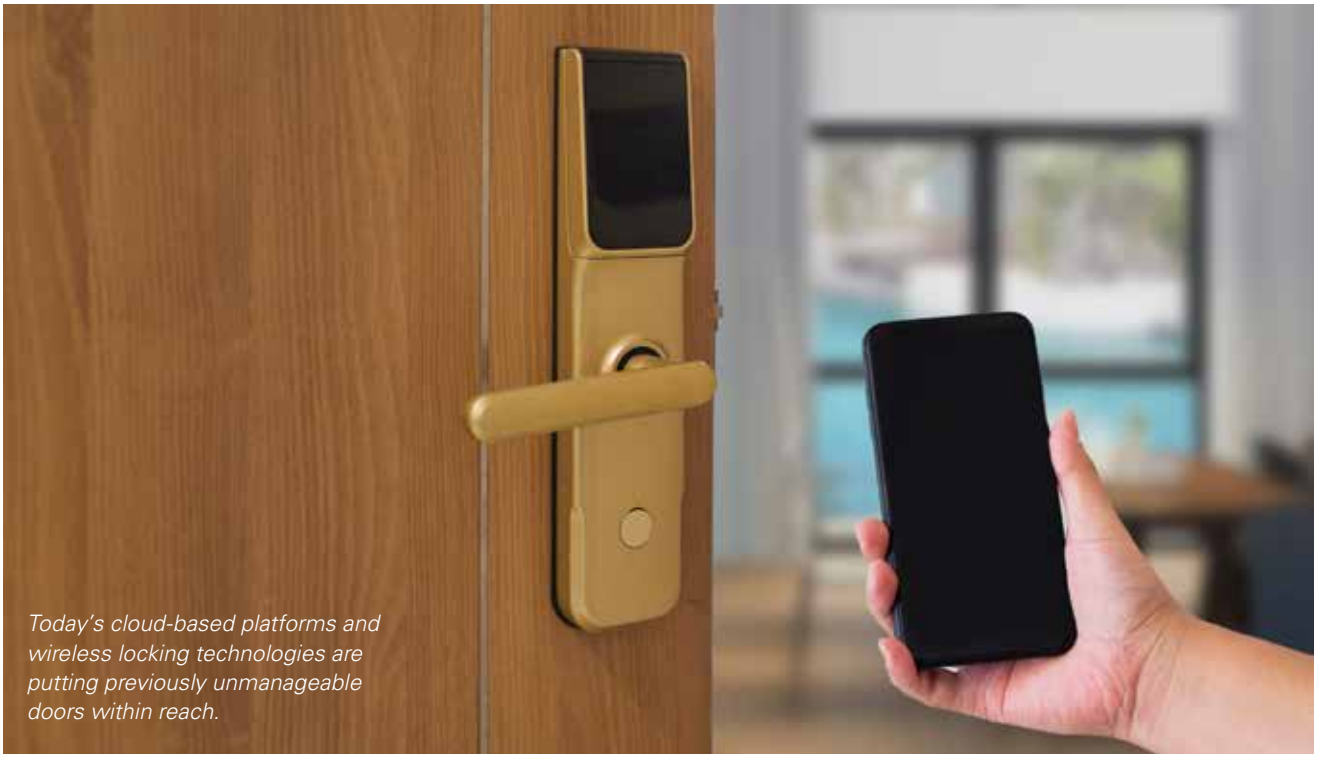
Universal Access Control Puts Unmanaged Doors Within Reach

Better technology and lower costs have made it possible to install access control equipment at places not thought of previously

by Daniel Bailin, Kim Garcia

In recent years, the access control market has been the benefactor of many technological advancements. At the same time, there has been an increased demand to expand the scope of access control systems beyond just the primary building entrances and high-traffic areas to include "secondary" doors.

Perimeter locations such as garages, entry gates, elevators and doors to executive offices, supply closets and IT rooms, historically have been beyond reach for access control, typically because of the cost and installation complexities. But



Today's cloud-based platforms and wireless locking technologies are putting previously unmanageable doors within reach.

Courtesy of Getty Images -- undefined undefined

Easiest Digital Upgrade

Switch™ TECH

It's Time to Make the Switch

Switch will transform mechanical SFIC lock-sets into digital access control devices for a fraction of the cost of traditional access control devices. And with a range of finishes available to match your current door hardware, it's the easiest digital upgrade you will make.


Spun


Spun Gold


Polished Chrome


Polished Gold

Mechanical Made Digital
timeforaswitch.com

BEST
dormakaba Group

today's cloud-based platforms and wireless locking technologies are putting these previously unmanageable doors within reach.

In this article, we want to look at how this can be accomplished and what security pros have to know when recommending expanded access control.

Yale Assure YRL226- CBA Lever Smart Lockx

Protecting Uncommon Doors

The first step in securing so-called secondary doors is to take a look at the hardware requirements and consider the tradeoffs of hardwired solutions versus smart locks.

Entry gates -- Entry gates typically serve as a barrier to an outdoor space, such as a courtyard or a pool, without allowing access to the interior of the building. Entry gates are unique doors to secure because of their location (often outside), their use frequency (often considered high traffic) and their requirement of supporting a mix of user types, including one-time access for visitors or deliveries and primary users, such as employees or building residents.

Because they often are a distance from the main building, entry gates typically aren't in an area that has reliable Wi-Fi signal strength to support wireless lock options. In instances where signal strength is strong enough, security pros can evaluate the anticipated traffic flow to decide whether a smart lock could support it. An area that has high traffic could exhaust the battery life of a smart lock too quickly. So, hard-wired locking hardware is recommended if the Wi-Fi signal is unreliable or the traffic flow is expected to be high.

Elevators -- Elevators are a critical point of entry to many areas of a building, so they have to have security protection like any other door on a property. The right access control solution tied to an elevator system can restrict access to specific individuals to only the necessary floors. This is an important requirement often seen in hotels, where high-floor suites are restricted to specific guests.

But it also is an important function in today's mixed-use high-rise buildings that have shared spaces and different tenant types. Buildings, where multifamily apartment units might be located on certain floors and businesses or coworking spaces, are located on other floors require a security solution to ensure that each tenant feels safe.

Although location- and user-specific access rights might seem complex at first, good access control software manages these situations with ease. Because elevators require a constant power supply to be operational all the time, hard-wired access control hardware is the only choice for this application.

Service doors -- Storage closets, maintenance rooms and even IT rooms are spaces to which many end users would like to control access, but these locations frequently don't make the cut because of budget constraints. Primary entrances and other perimeter doors are justifiably the higher priority for costly hard-wired solutions, but smart locks are excellent, cost-effective options for service doors.

With smart locks, customers can protect these rooms, which often contain high-value materials, while getting rid of the hassle of keys. Because service doors are almost always located inside a building, they can connect easily to the Wi-Fi network, typically have a specific set of users who should be granted access and are low-traffic doors that see openings a few times per day.

Shared-use rooms -- More frequently, commercial buildings have shared-use spaces for business tenants. Much like multifamily properties have communal pools, gyms and rooftop patios, commercial buildings now provide shared conference rooms, training facilities, huddle rooms and gyms to clients. The prevalence of this model is expected to increase in light of the trend toward remote work, which has led businesses to downsize from stand-alone office buildings to spaces where employees rotate in and out of shared workstations.

Shared-use rooms are great for smart locks because they connect with a building's Wi-Fi easily and they typically see low to medium traffic, so battery life isn't a major concern. The right access control system is particularly important for shared-use spaces because integration with scheduling tools that business tenants might use to book such spaces is important. Access schedules and credential management provide a seamless experience to business tenants who ultimately want to feel that the shared spaces are an extension of their own office space.

Putting It Together with Software

When adding access control to doors not typically covered by a system, selecting the hardware is only half the challenge. The lock features only come to life through the right access control software.

If a security pro installs a hard-wired access control system at primary entrances and smart locks at other doors on a site, some access management platforms require that they be managed in separate applications. This can be a real headache to those managing the day-to-day access requirements of a site.

Fortunately, today's universal access control systems allow users to combine hardwired and smart-lock solutions into the same platform for complete management and control, which allows for future growth and a feature-rich experience for the end-user. When looking for a universal access control platform, there are four primary things that security pros should seek:

1) Cloud-Based System

Many end-users insist on remote management capabilities as the world emerges from the COVID experience. Being able to give or revoke access at a moment's notice in light of personnel

CAMDEN DOOR CONTROLS

NEW FOR 2021

ACTIVATION

CM-222 Series
Touchless Switches

ValueWave™ economy switches now include blue/green illuminated models.

These are a preferred color illumination in some ADA compliant automatic door installations.

CM-700U Series
'Universal' Pull Stations

Camden's Blue Pull Stations now include a 'Universal' English, Bilingual and Spanish label set.

Ideal for use with mag locks in access control applications.

CONTROL

CV-603 Series
Access Control System

An app-based wireless Bluetooth® access control system that is designed to provide 'best in class' security of doors and gates, with up to 2,000 users.

CV-WR Series
Wiegand Receiver

Designed to interface with existing access control systems for both long and short applications.

The CV-WRX4 is a 4 channel receiver with in/out parking gate control. Use with CV-WTX2 2 channel key fob + HID prox.

LOCKING

CX-ED1309
Electric Strike

Now available with ANSI round faceplates in brushed aluminum or dark bronze finish.

Designed for narrow stile aluminum door frames, maximizing latch protection in store front retail commercial applications.

Magnetic Locks
UL1034 & UL294 Listed

Camden's 600 lbs. and 1,200 lbs. magnetic locks are now UL1034 & UL294 listed.

Weather and vandal resistant construction with the best performance and value.

FASTEST

SHIPPING: 85% Next Day!
DELIVERY: Standard 2 Days!

CAMDEN DOOR CONTROLS

Opening New Doors to Innovation, Quality and Support!

Call: **1.877.226.3369 / 905.366.3377** Visit: **camdencontrols.com**

Request information: www.SecurityInfoWatch.com/10213140

OpenEdge 620 Smart Lock

changes is critical to business continuity. Along with the necessity to provide real-time system updates, this makes having a cloud-based solution the only choice to manage today's access control client.

2) Easy to Use

Every access control system on the market will tout ease of use as a key feature, but many don't deliver on that promise. The software interface and application should be easy to use for anyone, security pro or end-user, who might interact with the system regularly. It should be intuitive to add or change hardware as well as manage access schedules that are critical to the daily management of a site.

3) Futureproof and Scalable

Cloud-based access control platforms are by their nature infinitely scalable. Adding wireless locks should be easy, and any system constraints only are those imposed by the limitations of the hard-wired components of a system. A universal access control platform can grow over time as the client's system requirements change, and it can integrate and manage new hardware technology within the same platform. This is in contrast with proprietary systems that work only with select brands of hardware and can be restrictive to end-users in the long run.

4) Integration with Other Systems

Access control is not the stand-alone system it once was. Today, these systems even help to drive business processes. For instance, a company using an IT contractor might require that the access control system integrate with its ticketing software to generate access codes automatically for contractors who visit various office locations. The right universal access control platform can add value by streamlining workflows that extend beyond just managing door access on a property.

Getting Started

A little bit of advance work can go a long way in making sure that the solution you specify can meet the demands of your customers today and into the future. These checkpoints should be part of every pre-installation site audit to help you to identify the best technology options for every door.

1) Understand your users.

Make sure you understand who will interact with each door and at what frequency. That can drive decisions about the type of credentials your locks have to support. Frequent users, such as employees, might prefer prox cards or key fobs as their credentials to save time accessing the door. Temporary or less frequent users, such as delivery drivers or custodial workers, might prefer PIN codes.

2) Consider traffic areas.

Consider how frequently users might come and go through each entry point on a typical day. High-traffic areas, such as main entrances, likely aren't suitable for smart locks because of battery-life considerations, while low-to-medium-traffic areas, such as maintenance closets or huddle rooms, are suited to wireless smart locks.

3) Check signal strength.

Wireless smart locks have to have reliable network connectivity, and network strength can vary greatly around a site. Know what's possible in terms of connectivity to each of the doors you want to secure. For instance, it might not be possible to secure a maintenance door in a parking structure by using a wireless lock if it's too far away from the Wi-Fi network. Making sure to examine the signal strength in advance will help to ensure the right lock is used.

4) Understand your existing system.

If access control hardware (smart or electronic locks) is on-site already, understand how it all plays into the total solution. Are the existing locks part of a system, or are they stand-alone devices? Are they cloud-based, or are they controlled by an on-premise software solution? Understanding the existing system, its infrastructure and its gaps will help you to determine how best to move, add or change it to bring total access coverage to your customers.

Also, if an access control solution already is installed, it can be useful to match the credential type on any installation to the credential type already employed. If users already use a prox card to enter a parking garage, for example, best practice would be to make sure they can use that same card to gain access to the elevator and the huddle rooms. It also can be useful to look for smart locks that provide more than one credential type. The right access control software will allow you to build on the existing system on-site and still deliver seamless credential management.

With the combination of wireless smart locks, hard-wired devices and cloud-based universal platforms available, bringing affordable access control to every door is a reality. End users recognize the necessity to eliminate keys from their entire property, from an operational perspective and because users want the simplest way to carry out daily activities. Adding access control to doors that typically aren't included can help security pros to expand their offerings while helping end-users to save time and avoid headaches. AC

About the authors:

Daniel Bailin is the chief product officer for RemoteLock. He's responsible for developing and driving the technology roadmap and product innovation strategy to propel the company's future growth. He has more than 20 years of experience in the access control, biometrics and semiconductor industries, where he has held product innovation and business development leadership roles.

Kim Garcia is the director of marketing for RemoteLock. She has more than 15 years of marketing and sales experience in the security industry.

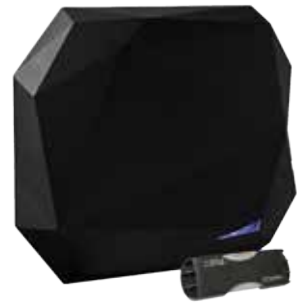
SECURE THE OUTSIDE. PROTECT WHAT'S INSIDE.

When it comes to security, LockeyUSA has you covered. With a broad portfolio of products, including keyless locks, hydraulic gate closers, and panic exit devices, we are committed to securing your assets outside and protecting what is inside. LockeyUSA is your partner for perimeter security and gate hardware products.

lockeyusa.com

Vehicle Access Control with STid SPECTRE

Company's sales and operations manager outlines the product's features and benefits



Contactless technologies (RFID, Bluetooth®, IoT, etc.) offer new possibilities to simplify the driver's experience. STid's SPECTRE reader accepts the challenge of fast-track security for vehicles access, making it both secure and extremely smooth.

Here's more from Frederick Trujillo, Sales & Operations Manager in USA.

Combining intuitiveness and vehicle access control

Seven out of 10 employees drive their car to work each day – a situation likely to be intensified with the current health crisis. Employees will select their own vehicle rather than use public transport; however, a motorist's daily commute can quickly turn into a nightmare because of traffic-jams.

At the car-park entrance, the situation is no better: they need to stop their vehicle, open the window and present their card until almost touching the reader to gain access.

This lack of fluidity raises anxiety. That's why we need new solutions such as contactless technologies to simplify the driver's experience.

The new advantages of contactless technologies

Contactless technologies such as RFID, NFC and Bluetooth® offer new alternatives to allow continuous flow car-park secure access by automatically identifying the vehicle and/or driver.

When a driver approaches the car park entrance, the vehicle is automatically detected thanks to a Teletag positioned inside the car and a STid SPECTRE long-range UHF reader installed nearby.

SPECTRE ensures a calm and consistent read over an impressive range of up to 13 meters. The car park owners can also opt for multi-antenna access management. Up to four antennas can be connected to just one SPECTRE reader to tackle all security challenges and fulfill all configurations: managing a diverse fleet of vehicles (cars, vans, motorbikes...), encompassing wide access points and even smooth access control for four separate vehicle lanes.

Ensure both vehicle and driver are authorized for entry

The driver's "access rights" can also be controlled thanks to STid Mobile ID®. Their identity is also verified before allowing both cars and drivers access.

This is a level of security that many companies or offices need to ensure. For example, motorcycles in car parks are challenging. The motorcyclist doesn't have a front number plate for identification, hindering access control for their vehicle. The rider is required to remove a glove to either use a card or a smartphone.

With STid Mobile ID®, by simply tapping the smartphone inside their fastened jacket pocket, the motorcyclist can gain successful access.

This growing need for intuitiveness must never impact on security and data protection. STid ensures security between the Teletag and the reader and between the reader and the system using the Secure & Smart Communication Protocol (SSCP), which helps to provide uniformed end-to-end security. This protocol protects the communications of physical and digital access control equipment. It provides a secure connection between the readers (inspection devices) and the management system (concentrator) to guarantee a level of security in line with government requirements.

An answer that is not just technological

Analyze current procedures and conduct a full risk assessment to identify the potential added values of employing new technologies. The same applies for a true Return on Investment (ROI). Our ultimate success is based on attentiveness to market needs and to always propose improved, instinctive and highly secure solutions.

To learn more about STid's products and solutions, please contact Frederick Trujillo at f.trujillo@stid.com or visit https://stid-security.com

STid

STid

ENHANCED DRIVER EXPERIENCE

SPECTRE

Stress-free access to your Car Park Barriers

No more traffic queues or bottlenecks at peak times (...), the new SPECTRE's UHF delivers both speed and security at your Car Park Barriers and enhances your daily experience.

Connect up to four antennas to just one SPECTRE Reader to tackle your toughest security challenges and your diverse fleet of vehicles. Simply and easily control access for four separate vehicle lanes...

SPECTRE is the markets most robust reader and intuitively easy to use. It's discreet by design, flexible in its configuration, secure and encrypted in its communication.

Welcome to enhanced speed and security - in one single solution.

WE'VE GOT YOUR BACK

OSDP™ Supported by SIA

SSCP Supported by SPAC

www.stid-security.com

Request information: www.SecurityInfoWatch.com/12266353

Your Access Control System Is At Risk

There are intelligent and cost-effective solutions available to ensure the security of almost any system

by Sarah Bowling

There are probably thousands of opportunities to threaten the security of an existing access control system.
Courtesy of Getty Images -- Credit: Gangis_Khan

Free Virtual Campus Safety Classes & Demo

Contactless Solution in Hand – Access Control App Works with Any Brand Access Readers & Leading Wireless Locks

COVID-19 has created a host of security & safety challenges. Uncomfortable new-norms have changed our lifestyles, but our smartphones are still front and center. That's why the powerful Continental Access CA4KApp with Built-in Mobile Credential is the ideal easy contactless solution for access control. It works on any smartphone and provides contactless authorized access through any type of door – and it works with any brand reader and most wireless locks.

Ideal for campuses, schools, hospitals & buildings, the CA4K Access Mgr App, simply provides smartphone-based access privileges for a few to large numbers of users; and Campus Security Managers with smart, comprehensive enterprise control of users, threat-levels and a few, to thousands of doors – right in the palm of their hand.

- **Easy Intuitive Mobile App** provides Contactless Access for All Readers & Door Types from any smartphone
- **No Buttons, keys, keyfobs to touch** – For quick controlled access thru doors, wireless locks & elevators
- **Fast powerful processing** ensures fast, smooth access for simultaneous users even at peak times
- **Integrated with CA4K Enterprise Security /Video/Access** Platform for Comprehensive Control of All Doors (1-32,000), wireless PIN/Prox locks, readers, elevators & entryways
- **Generous Tradeup Incentive** for Retrofitting Existing Systems

For Free Demo or Free Campus Safety Class
call 1.800.645.9445 or email CIMktg@cicaccess.com

Also see our full schedule of trainings & solution-based hot-topics www.cicaccess.com/seminars

CA4K ACCESS MGR APP

Download on the App Store | GET IT ON Google Play

Continental Access

Request information: www.SecurityInfoWatch.com/10213301

Let's face it. There are probably thousands of opportunities to threaten the security of an existing access control system. It's an inherent dynamic of the technology–hacker relationship. We make it, they break it. Unfortunately, when technology is compromised it often means an upgrade is in order; not only for the technology itself but for the hardware that supports it.

Certainly, we are seeing impressive efforts made by hardware manufacturers to minimize footprints, maximize interoperability, and future-proof installations. However, before you design your solution, you need to understand and prioritize the risks you are facing. This article outlines the three most imminent threats to legacy systems and proposes a general risk-mitigation solution for each. With careful product deployment and thoughtful transition strategies, these threats can be easily, efficiently, and affordably resolved.

1. Your legacy card technology can be cloned.

The majority of access control credentials in deployment today still use 125kHz low-frequency proximity technology. This read-only technology is over 25 years old and though certainly reliable and economical, it is known to be extremely vulnerable when it comes to securing your proprietary data. Prox cards can be easily cloned.

The fastest way to duplicate an LF Prox credential is to pop down to your local big-box pharmacy or hardware store. Oftentimes you'll see a "Key Me" kiosk somewhere near the store entrance. For as low as $9.99, you can easily copy your company card, your student ID, or even your gym pass! Another popular method of duplicating your prox credential is with a handheld cloning device which can be purchased online for just a few dollars more. Within 20 seconds, a user is able to read unsecured data off the original prox card and write that same data to a blank card. Access granted!

What You Can Do About It:

Get off prox. Depending on the number of cardholders you have, the process and the price of replacing already-issued cards can be painful. However, the cost associated with a breach can be much higher. More often than not, "getting off prox" falls into the "how can we afford not to?" category. Upgrading to a new secure credential technology such as encrypted smart cards or mobile credentials is highly recommended. Your primary goal must be to secure the communication/authentication between the credential and the reader so that proprietary user data is protected.

> The majority of access control credentials in deployment today still use 125kHz low-frequency proximity technology. Just because you've upgraded to a more secure credential technology doesn't mean you're out of the risk zone.

2. Your existing wiring can be skimmed.

Even if no one copies your card, that doesn't mean your card data is safe. Once your card is authenticated by the reader, your data still needs to be communicated to the panel for access to actually take place. Traditional wiring protocol, known as Wiegand, has been the industry standard since the 1980s. Wiegand consists of uni-directional, unencrypted wires that run between the reader and the panel. It's these wires that can be easily compromised. By simply removing the reader cover, a hacker can slip a skimming device on the Wiegand wires. Every time a card is presented to the reader, the skimming device can capture the unencrypted data as it travels along the Wiegand wires. This is a surreptitious and incredibly effective method of capturing entire databases of cardholder information!

What You Can Do About It:

Upgrade to ODSP. Open Supervised Device Protocol (OSDP) was developed by Security Industry Association (SIA) and approved as an international standard by the International Electrotechnical Commission (IEC) in 2020. It offers more functionality, interoperability, and most importantly, higher security than Wiegand. Instead of communicating unencrypted data between the reader and the panel, OSDP supports bi-directional, encrypted communication via RS-485 thus protecting that proprietary card data traveling to the panel for access command. Essentially, upgrading to OSDP requires installing a panel converter of some sort or, more popularly, a complete panel replacement. This transition also affects your reader, as it too needs to be capable of supporting the new protocol.

Essentially, you're asking your hardware to speak a new language. Most access control manufacturers now offer "intelligent panels" which communicate OSDP and offer a wide range of features and functionality not offered in legacy panel technology (e.g., ability to do remote firmware updates to the reader via file transfer). Reader manufacturers have varying approaches to supporting OSDP. Replacing hardware with hardware is not only infuriating, but it can also be very expensive. If you are planning to transition your legacy system to OSDP, it is important to select the right hardware that will set you up for future success.

SIA launched a certification program called OSDP Verified. Defined by SIA, this is a "comprehensive testing program that validates that a device conforms to the SIA Open Supervised Device Protocol (OSDP) standard and the related performance profiles".

Key Features To Look For When Evaluating OSDP Reader Hardware

- OSDP Verified

Paxton

Paxton10

Access Control | Video Management | One System

Paxton's most powerful system

- 1000 doors
- 1000 cameras
- Bluetooth® smart credentials
- Compatible with PaxLock & Entry ranges
- Security & Fire Alarm Integration
- Multiple sites
- Perfectly simple

Find out more and sign up for Paxton10 training at **paxton.info/5228**

"I'll definitely recommend Paxton10. Like all Paxton products, the user interface is simple, it's plug and play and it looks good."

Courtesy of Getty Images / By kukhunthod

- Readers can handle the transfer of structured data units required for smart card operations (File Transfer)
- Readers can automatically detect OSDP when connected to the new panel without needing new wires or field firmware updates
- Readers with a certified EAL6+ crypto engine to protect your keys
- Reader manufacturers who allow you to own and access your keys, unfettered, for true credential interoperability
- Readers are configured for maximum security, that prevents badge ID duplications, and that works well with dual-tech cards with no security compromise

3. You're locked into proprietary technology.

Just because you've upgraded to a more secure credential technology doesn't mean you're out of the risk zone. In fact, there's a very good chance you've locked yourself into a proprietary relationship with a vendor without realizing it. Most manufacturers have set up their business models to support a proprietary solution due to the method of encryption most commonly used to secure your data. In the commercial market, the most popular method of securing data on a card is called symmetric encryption.

This type of encryption uses a single, secret keyset to encrypt and decrypt your user data when it is shared between two authenticating devices (e.g., the card and the reader). This method allows for a fast, easy, and affordable secure credential solution. The problem, however, is that those encryption keys are often owned and managed by the vendor. Furthermore, vendors often utilize a "common key" or "universal keyset" so that every credential and reader/device deployed in the entire marketplace uses the same "secret key".

The risks here are twofold:

- A vendor-owned encryption key means if you want your credential to work on any device in your ecosystem (card reader, lock, secure printing device, etc.) you are forced to purchase those products through that very same vendor. Or, at a minimum, pay a module fee in order to have that vendor manage the keys and establish compatibility with the various devices and applications in your ecosystem. Buying proprietary encrypted credentials means you've instantly limited your ability to freely source products at a competitive price. You've also limited your own ability to freely integrate your credentials to work on all of the devices in your ecosystem.
- If a vendor programs a "common key" or "universal keyset" in all of the credentials and devices they sell into the marketplace, the entire deployment is at risk should that universal keyset somehow become compromised? Even if individual customers have been assigned a unique format (Facility Code, bit format, badge ID range), if the encryption keyset that protects their data gets hacked, then every single customer using products with the same keyset becomes compromised. Owning your cards, but not your own encryption keys – is like owning a house in a gated community but the HOA uses the exact same locks and keys on every front door in your neighborhood. If someone picks your lock, they essentially pick everyone's lock.

What You Can Do About It:

Own your keys. Believe it or not, there are solutions that allow an end-user to abolish these vendor handcuffs, and this involves taking ownership of a unique encryption keyset.

For example, LEAF is an industry initiative devised by product manufacturers who evangelize open standards for credentials. These LEAF partners have defined a credential that is highly secure, openly sourced, and totally interoperable with unlimited devices or applications which may reside in a project ecosystem. Some of these manufacturers also offer Key Management Services, which make owning your keys and provisioning them to the devices of your choice an easy process to deploy. Owning your keys means you now have the power to support any device or application in your ecosystem with just one credential. The purpose of a LEAF solution is to break the chains otherwise established by credential manufacturers with proprietary business models.

I encourage you to research your options when faced with designing your transition strategies, so as to capitalize on the most intelligent and economical solutions available in the industry today.

AC

About the author:

Sarah Bowling is the VP of Marketing and Communications at WaveLynx Technologies

Free! LocDown Lock for Schools

LocDown® Any Door from Safely Inside with Budget-Friendly Classroom Locks by Marks

Keep teachers, staff and students safer in the classroom with **Marks LocDown® Locks.** In the old days, with a standard lock, someone would have to go outside into the hall to lock up a classroom, but **LocDown Locks** uniquely lock from the inside, so no one has to potentially face an external threat. **Created in conjunction with, and spec'd by, one of the largest school districts in the country (LAUSD) and used by many more nationwide, Marks LocDown Locks have an inner door key and lock-down indicator, and easily & super-affordably replace any standard door lock.**

- **Lock Down in seconds, with a simple key, safely from inside** the classroom, without having to step foot into the hall or danger
- **Lockdown indicator** gives visual peace of mind
- **Retrofits any standard lock** easily & very economically
- **Classroom Locks in cylindrical or mortise lock styles,** with unique double cylinder locking mechanism
- **Ultra Durable for Life -** Lifetime warranty; exceeds ANSI/BHMA Grade 1 standard

LIFETIME WARRANTY MARKSUSA

Request information: www.SecurityInfoWatch.com/10214311

Get a Free LocDown Lock with Free SAVI™ Onsite Security Check:

Find out how safe your school is with a free professional onsite survey & get a Free LocDown Lock** Sign up online at https://bit.ly/2IdzS1O

MARKSUSA

1.800.645.9445 • salesinfo@marksusa.com • **www.marksusa.com**

SAVI® (School Access-Control Vulnerability Index) and LocDown are trademarks of Marks USA/ Napco Security Technologies, Inc. **Free Lock, model 195DB/26D, with completed onsite S.A.V.I. survey by security professional, no obligation, no charge. (Offer limited to one free lock per school.) For full warranty details, consult manual or see terms online.

How to Use EAC to Secure a Cannabis Facility

by Bryan Sanderford

Getty Images/

Cannabis business operations face a unique set of challenges that are both public-facing and anchored in strict government and banking compliance mandates. The one common denominator with these challenges is the need for tight physical security to better protect people, property, and assets with two predominant areas of interest focusing on entry/egress points, and back areas where cash is handled.

Given all of the sophisticated security solutions available today, the most pervasive and effective physical security solution for cannabis businesses is to keep facilities, products and cash locked down. Door control technology continues to be a proven first line of defense to help prevent incidents from occurring, effectively keeping both customers and employees safe.

People usually think of doors as a means of keeping someone out, or alternately, keeping someone in. Doors provide privacy and, when locked, a level of security that is both simple and effective. Perhaps you never thought about it at length, but there are many ways that doors can be opened and/or closed. They can be manually operated with a handle or push bar, revolve, swing or even slid into a pocket in the wall – and they can be operated automatically with the push of a button, the swipe of a card or a proximity device, or be programmed to lock if another door is open or unsecure. All of these solutions are appropriate for

SAY GOODBYE TO MECHANICAL KEYS

SALTO's easy to install products make it simple for locksmiths and security professionals to upgrade and replace mechanical-key-operated locks with the latest in electronic access control.

Learn more at **salto.us**

Request information: www.SecurityInfoWatch.com/10225529

SALTO
inspiredaccess

specific applications in today's cannabis facilities.

Controlling Physical Access

Perhaps the most essential aspect of cannabis business operations is also the most precarious – customer interaction and access to retail areas. This earmarks entry/egress control as a primary priority when implementing physical security measures. Fortunately, there is more door technology on the market today than ever before, including advanced programmable door interlock systems (often called mantraps), which provide very high levels of security. Door interlock systems provide cannabis facilities with a unique form of protection for both customers and employees that is not afforded by conventional access control systems.

Interlock systems have different names based on their functionality, and are commonly referred to as one of the following:

- Interlocks
- Mantraps
- Sally Ports (for vehicles)
- Secured Vestibules
- Air Locks

In its simplest form, a door interlock system commonly referred to as a "mantrap" is composed of two doors electronically connected so one cannot open until the other has closed. For cannabis facilities, an interlock door system can provide unrestricted access to an interior vestibule, where customers and/or employees can be screened automatically or by a security guard before entering your facility. Access to the interior of your operation is only allowed when the exterior door is closed, preventing tailgating of unauthorized individuals.

For retail locations, a secure vestibule may be employed. When an individual(s) in the interlocked area is approved, the outer door remains locked, and the individuals are allowed to proceed through the inner door. Conversely, if an individual is deemed suspicious, an alert can be sounded. The inner door will remain locked and the outer door will unlock allowing the potential threat to exit the building. This effectively prevents potential problems from escalating inside your facility.

For employee entrances, a secure-entry vestibule configuration provides a fast method of entry and egress through a combination of locked and unlocked doors. Exterior doors are normally secured and interior doors are normally unlocked. An electronic access system controls entry from the outside and a Request-to-exit (REX) device is used on the interior of exit doors. Unlocking the entry door will lock the interior door of the Secure Entry Vestibule. Once the exterior door is re-secured, the interior door is unlocked to allow access to the facility.

Courtesy of Dortronics

For cannabis facilities, an interlock door system can provide unrestricted access to an interior vestibule, where customers and/or employees can be screened automatically or by a security guard before entering your facility.

The highest level of security is provided with a restricted entry and exit system, whereby a door is unlocked by a request for access only if no other related doors are unsecured. Opening any one door keeps all other related doors locked. Restricted entry and exit systems will buffer simultaneous requests for access to prevent two or more doors from being unlocked at the same time. This door interlock system configuration is most appropriate for back areas of cannabis facilities where inventory is stored and cash areas are located.

For cannabis distribution facilities, sally ports can be deployed to control vehicular entry/egress using any combination of overhead doors, gates or bollards.

Door interlocks are also available with different modes of functionality. Cannabis facilities with a high amount of pedestrian traffic in the morning and late afternoon may want two doors operating during these time periods with the ability to switch to a single door during midday or evening hours. Intercom systems can also be added to door interlock systems to allow communications between the individuals inside the "mantrap" and a facility greeter or security guard controlling the system.

For employee access to highly secure areas within cannabis facilities, advanced interlock systems can be deployed with biometrics that read faces, eyes, and/or fingerprints to provide highly accurate identity authentication and verification, adding a much higher level of sophistication and security. This prevents lost, stolen, or replicated physical access control credentials or even simple key locks to be compromised by unauthorized personnel.

While security is the core priority, a door interlock system deployed at cannabis facilities must also be user friendly and safe, or it can become a logjam for customer traffic as well as a potential source of liability. In an emergency, the door interlock system must enable people to evacuate the facility. For example, if the power fails, an emergency override would ensure that the door can be opened manually. Moreover, safety codes may require that the door interlock systems be integrated with the facility's fire alarm control panel to allow emergency door release. A local emergency pull station may also be required to allow doors to be unlocked in non-fire alarm emergencies or to interface the system with NFPA 101 delayed egress controls. In every case, local compliance mandates must be carefully adhered to when designing a door interlock system for your facility. Working with a reputable manufacturer and system installer ensures you will get the ease of operation and specific door interlock capabilities and compliance you need, along with high-quality customer support and service.

Door control solutions like interlock systems are highly cost-effective while delivering an effective means of securing your facility. Dortronics is a leading supplier of door control solutions and electronic locking solutions ideal for cannabis facilities. Our experienced team of door control experts are here to help assist with your specific needs with personalized support and products that are made in the U.S.A. We look forward to hearing from you. AC

About the author:

Bryan Sanderford is the National Sales Manager at Dortronics. Please visit www.Dortronics.com for more information.

INNOVATIVE DESIGNS SUPERIOR PRODUCTS

THE RIM PANIC SOLUTIONS

THE NEW ENHANCED 4850

PoE Friendly

NOW EVERYDAY LOW CURRENT DRAW

UP TO 48% LOWER THAN THE COMPETITION

THE SUPERIOR 4800F

FIRE RATED LIKE A 9500, PRICED LIKE A 9600.

SEARCH "NEW TRINE 4850" TO LEARN MORE

Request information: www.SecurityInfoWatch.com/10215438

AVAILABLE JULY

TRINE ACCESS TECHNOLOGY.

Smart locks made simple

Simplicity can take many forms in a smart lock. But each of these simplicity-enhancing features and benefits can be a key factor in selling these devices and growing the connected side of a dealer's security business.

(Image courtesy Kwikset)

Once seen as difficult to install, connected locks are now making the lives of homeowners easier while simultaneously boosting integrators' bottom lines

by Nick English

When considering why homeowners purchase technology products for their home, one must consider the principal drivers behind the purchase. These days, simplicity and convenience are paramount – particularly at a time when the pandemic has already complicated so much. Today, while stuck at home, many homeowners are working on projects that will make life less stressful and make their homes more secure. And many of these projects involve connected devices like smart locks.

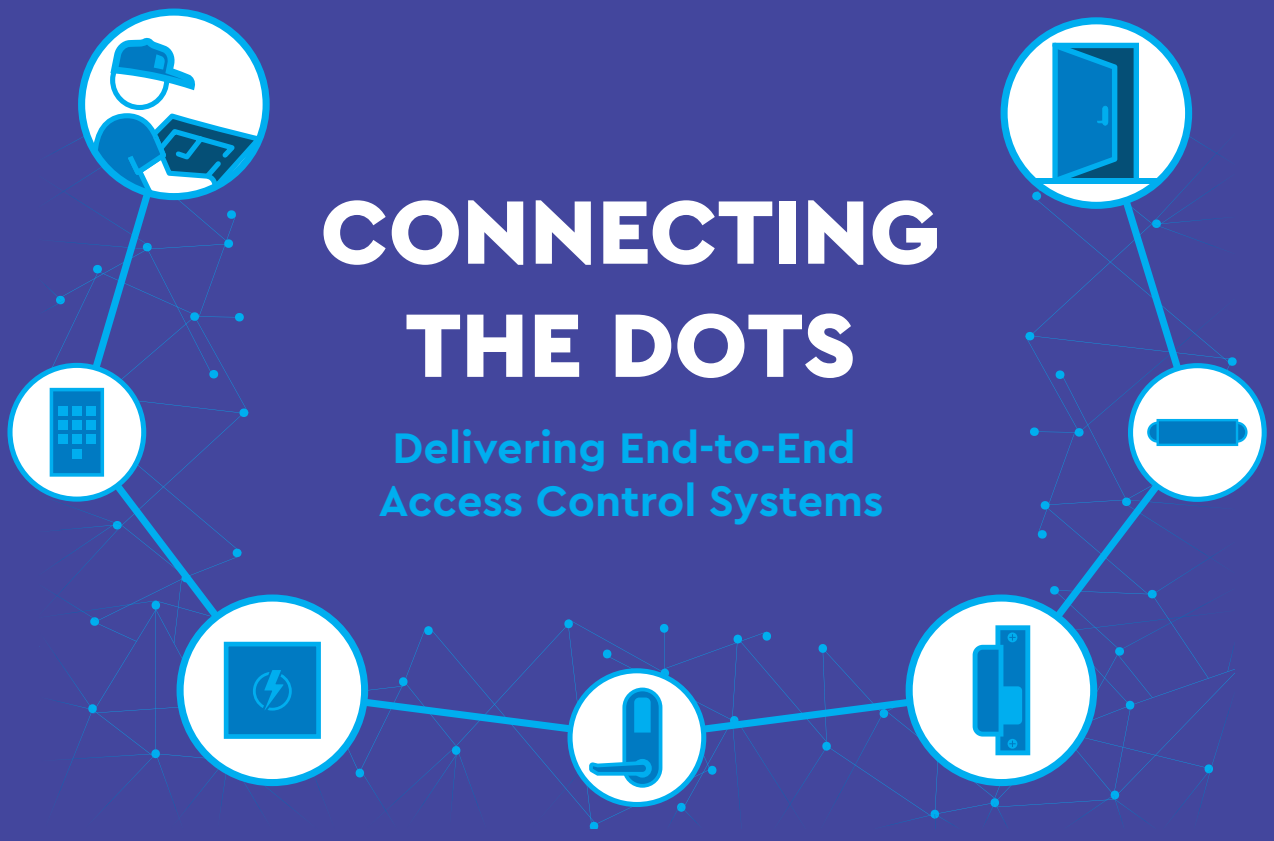
Even the most tech-savvy customer wants technology that is going to improve their day-to-day living today and in the future. A 2019 smart lock audience segmentation study conducted by Kwikset found that even "tech enthusiasts" were looking for "durable, tech-savvy locks to make life more connected." They wanted "long-lasting, durable" locks" that "bring convenience to life, so they should be easy to install, too."

Not surprisingly, the same study found that "everyday fixers" (who are described as suburban homeowners who take care of their home their way) were also interested in "durable, functional locks" and "convenience."

Simplicity can take many forms in a smart lock. But each of these simplicity-enhancing features and benefits can be a key factor in selling these devices and growing the connected side of a dealer's security business.

Simplicity of Design

According to a 2020 Smart Door Lock study conducted by Parks Associates, "Strong product design instantly communicates the added value of a connected product. Design differentiates, validates value, and contributes heavily to the user experience."



CONNECTING THE DOTS

Delivering End-to-End Access Control Systems

From the latest ASSA ABLOY products, to complete system design, to comprehensive, personalized training, Banner Solutions electronic access control experts connect the dots to deliver the right solution for any job.

Redefine your expectations at: BannerSolutions.com/eac

banner SOLUTIONS

ASSA ABLOY

ELECTRONIC SECURITY HARDWARE

HES | Securitron

888.362.0750 eac@bannersolutions.com bannersolutions.com

Courtesy Getty Images / By mikkelwilliam

Most people don't want to bring the latest technological device into their home if it's going to detract from the home's décor – if it is unattractive or calls attention to itself in a negative way. They might begrudgingly put up with a tangled mess of wires in order to get that perfect sound from their home theater, but they'd prefer if the wires were invisible, and the devices themselves attractive and sleek, but unobtrusive.

When it comes to the look of the lock itself, we find that buyers of smart locks fit into two main categories. Some, particularly those with a more traditional-looking home, want a smart lock that conveys a similar aesthetic to a traditional lock. These smart lock options can somewhat disguise the technological advances and are not overly disruptive in terms of design "language."

Others buyers do prefer a more forward-looking design, albeit a lock that is unobtrusive as well as sleek and modern. The Parks Associates study makes the point succinctly: "A simpler design can make the device appear less daunting to consumers unfamiliar with smart door locks, attracting more customers and enhancing the value of the product."

Simplicity of Installation

Sometimes what is thought to be the complexity of smart locks by the dealers and technicians themselves can slow the growth of a smart lock business. For example, one of the reasons I've heard from those hesitant to grow their smart lock business is a perceived difficulty of installation. This perception couldn't be further from reality. If you've ever installed a traditional deadbolt, or even if you haven't, installing a smart lock is remarkable easy.

> Most people don't want to bring the latest technological device into their home if it's going to detract from the home's décor.

If you're replacing a traditional mechanical deadbolt with a smart lock, then the hole you need for the smart lock already exists, the door is already chiseled, and the frame is already cut out. Installing a smart lock is just as easy as swapping in a new deadbolt. And if it is a new door, it has arrived to you with a hole already in place, pre-cut.

The hole for the mechanical deadbolt works just as well for a smart lock. In fact, in some cases, the smart lock might be a better fit. Today's smart locks increasingly feature smaller footprints and tapered parts, to help ensure that everything fits, and the door closes correctly.

If the door doesn't fit after installing a smart lock, odds are that there are issues with the door frame or jamb – not the lock. To address this potential issue, before the old/original deadbolt is removed the technician should ensure the bolt is free to move and does not bind up or have any issues closing freely. It is important to address any issues with the door frame or warping -- before the electronic deadbolt is installed.

And as for complicated electrical work, or wiring, there is none. Smart locks are battery operated. Popping in

TOP NOTCH DISTRIBUTORS™

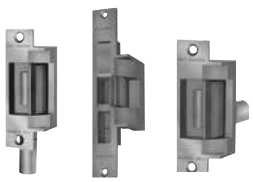
We Know Service

www.topnotchinc.com | 800.233.4210

YOUR SOURCE FOR ALLEGION ACCESS CONTROL PRODUCTS

Automate your opening.

Top Notch stocks all the products your customers need to secure and electrify their openings; from maglocks to electric strikes, push buttons and much more. Most orders ship same day! Need assistance with your next project? The experts in Top Notch's EAC department are available to help you select the right products for the right application.
Contact **eac@topnotchinc.com** or call 800.233.4210 today, and experience the difference.



Electric Strikes
Von Duprin 6200 Series

Electromagnetic Locks
Schlage M490/492

Heavy-Duty Pushbuttons
Schlage 620/631 Series

Top Notch is a proud partner of: ALLEGION SCHLAGE VON DUPRIN

Contact Top Notch Distributors for all your door hardware needs!

www.topnotchinc.com | PH 800.233.4210 | FAX 800.854.4146 | sales@topnotchinc.com

Request information: www.SecurityInfoWatch.com/12129499

the battery is as easy as, well, popping in a battery.

After the smart lock is physically in place, the device can be ready to use without a lot of complex programming. This is especially true if the smart lock features one-touch programming, an advantage that serves to speed the installation process. This means that customers that expect the installation of their smart lock to be a time-consuming process can be relieved to learn just how quickly they can get their new device up and running.

Additional Benefits

Here are some additional benefits to zero in on when it comes to selling smart locks:

- **Uncluttered keyrings.** Simplifying lives can mean eliminating clutter, including reducing the number of keys in the homeowner's pocket. Smart lock users can store their key in a safe, out-of-the-way place because they can use a personal user code to enter the home. They can also assign a time-sensitive user code to whoever might need one and delete it when they see fit. In this way they are not passing out copies of keys to friends, relatives, caregivers and contractors – keys that can be lost or stolen.
- **Easy information.** Smart locks connected to a home automation system can be empowered to maintain important information about their use and deliver it to a controlling device. In this way, they can provide homeowners with an audit trail of who has been granted access to their homes, and when. Homeowners can even receive notification via text message of when their loved ones have arrived home safely, or when the painters came and when they left.
- **Converting customers.** Converting customers to smart lock customers has never been easier than with the addition of the latest smart lock conversion kits. These products turn mechanical locks into smart, electronic locks by replacing the interior half of the existing lock without changing the exterior. These products appeal to design-focused homeowners who want the convenience of keyless entry and home automation while maintaining the style of the front door and/or matching an existing handleset. AC

About the Author:

As North American Sales Manager for Kwikset Residential Access Solutions, Nick English is responsible for management of all sales and distribution through Pro Security channels, including sales and performance management of Territory Sales Managers and Key Account Managers.

Easier Wireless Access Locking, *Their Style, Their Way*

- **Class-leading wireless access locks for every application** - Lowest-maintenance, longest battery life, keyless access, multi-credentials, matching models inside & out
- **ArchiTech Networx: Same proven Trilogy® electronics, but designer minimalist look, customizable** with hundreds of architectural finishes & Grade 1 Lock styles and various colors/shapes of multi-tech ID reader + Smart Mobile iLock® App
- **Cost-saving, easily networked - No Panels, No PIMs** - Choose Networx® Ethernet, WiFi &/or POE Gateways & Extenders, each controlling over 60 locks
- **Wireless keyless access solutions for all doors,** from mortise, to narrow stile, to exit devices. Cylindricals simply retrofit standard locksets in about an hour.
- **Global or Local Management & Lockdown -** Networked to save staff labor from door-to-door operations & provide emergency solutions, via lock, keyfob or server, including free Alarm Lock Software or Enterprise Integration in realtime, with top platforms, Continental, Lenel®, Software House®
- **Smart Apps for lock users or security managers**

MORE AFFORDABLE
Lowest labor & equipment costs without sacrificing top conventional access features

EASY INSTALL
Replaces any door lock, on any door type, neatly, quickly

EASY NETWORK
No wires to run to doors. Uses customers' existing network or Ethernet & multi-lock (63 locks/gateway) gateways & opt'l repeaters

CENTRALLY MANAGED
Auto-Schedule program updates, queries, or free access by time, by door & more

GLOBAL LOCKDOWN
or unlock in seconds from the server or any lock

USERS
Supports thousands of PIN, ID or iLock App users. Easily local/remotely

networx
by ALARM LOCK

From the Makers of #1 Trilogy Locks

1.800.ALA.LOCK • www.alarmlock.com

Request information: www.SecurityInfoWatch.com/10212743

an ACRE brand

vanderbiltindustries.com @VanderbiltInd Vanderbilt Industries

VANDERBILT

Request information: www.SecurityInfoWatch.com/11514790