CASE STUDY

2 FACTOR ACCESS WITH TOUCHLESS ENTRY FEATURE

Abstract

Two Factor Authentication (2FA) is becoming a powerful prevention protocol for thwarting unauthorized access, fraud, and cyberattacks. The physical security world is driving to protect sensitive information, and control staff and the public from accessing restricted areas. There is an increasing need to verify and authenticate user identity. Adding to the solution in a time of pandemic is a recognition to incorporate a touchless approach to the solution.

Paul Brauss

PBRAUSS@bluelinetechnology.com

In concert with the Intel IoT Solutions Alliance

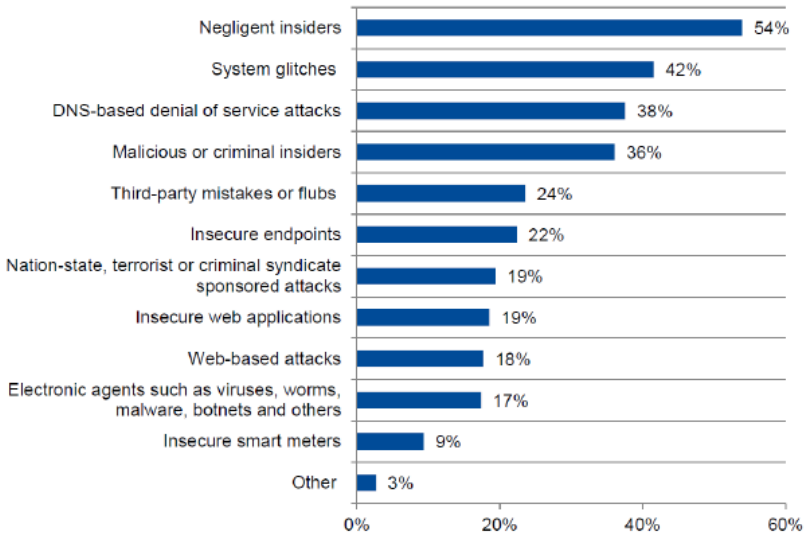
Table of Contents

Introduction:

A survey of critical infrastructure companies worldwide, including utility, oil and gas, alternate energy, and manufacturing organizations, found that 70 percent had suffered a security breach in the past year, according to the Ponemon Institute report commissioned by Unisys, Critical Infrastructure: Security Preparedness and Maturity. Many organizations are also not getting actionable real-time threat alerts about security exploits. According to 34 percent of the respondents in the Ponemon study, their companies do not get real-time alerts, threat analysis, and threat prioritization intelligence that can be used to stop or minimize the impact of a threat or cyberattack. Cloning cards to gain entry and access to critical points of a company is not uncommon and known to be easy. Any organization that understands risk management understands that an access control system must include a 2-factor protocol and a touchless, handoff approach is gaining a significant foothold.

The Challenges

Aside from video surveillance which is almost always forensic, critical infrastructure companies are relying on analytics for real-time feedback. This, however, does not stop someone who spoofs or swipes a card to enter authorized locations. As the critical infrastructure report recommended, deploying better authentication for applications and users is one way to combat remote attacks, with a call for "strictly enforced user credentials" to protect existing network segmentation. Bringing awareness of this issue provides transparency into potential risks which can only help strengthen the goal of providing an efficient protection method. Enforced security policies and procedures will aid in reducing card theft and nefarious card activity, but the human element poses the greatest risk. Relying on individuals to not "share" their cards, or inactivating or other maintenance for lost cards can be cumbersome. The turnover of employees and the temporary status of others only exacerbates the problem. A single line of defense when considering human behavior and access control alone cannot provide a fail-safe plan.



Top Security Threats - Critical Infrastructure: Security and Preparedness and Maturity Report. 2FA Facial Recognition can cover Negligent Insiders, Criminal Insiders which perpetuate to other types of attacks.

What is 2 Factor Authentication:

Access control systems control doors and locations. To prevent misuse, access control provides a way to monitor, control, and manage a door's "status." The access control software can allow or deny a user of the token based on door location, designated timeframe, and authorization privileges.

The inherent security risk in single token presentations is theft, loss, being loaned to another user, or the token cloned to gain access. Facial recognition as a biometric two-factor authentication assures the token matches the face and creates a much more secure environment.

Two-factor authenticators are classified as:

- something you know (Password)
- or something you have (Card, fob, a cryptographic key)
- and something you are (Face, fingerprint, iris scans).

Two-factor authentication assures the user is a valid subscriber. For example, a PIN and access card are not a true and secure two factor unless it is tied to a biometric authenticator. (Roger Grimes KnowB4, Inc podcast)

Facial recognition, like the solution introduced by Blue Line Technology, deployed with access control makes it very difficult to steal and use the entry tokens.

Parallel Biometrics versus Integrated Biometrics Benefits

In the market loaded with Access control products, the market is changing at a rapid pace with new technologies for an enhanced security platform. Companies are playing catch up to add new solutions for a growing legacy issue. How do you add 2-factor capabilities to the system without major integration changes? It is difficult to navigate through the decisions of access control suppliers for readers that integrate into their systems for visitor management, employee attendance, and

door access. The logical choice is biometrics.

The typical biometric capabilities provide the opportunity to add a 2nd factor to the existing access system. Access control manufactures are quick to point out that a biometric solution can be integrated into their platform. There is a cost associated with this integration and a cost to maintain the integration. Access control manufacturers constantly upgrade their software with patches and new capabilities. This constant change poses a challenge with integrated biometrics.

The deterrence and behavior modification security experts are looking to achieve include:

1. Combat the cloning devices which have made it very easy and a minimum cost for devices that engineers understand make it simple to duplicate cards.
2. Stop employees that work together from passing cards back and forth to avoid the reporting of a lost or stolen card. In some cases, the expense of replacement is passed onto the employee. With the lost or stolen card, there is always the chance that the card is used in a malicious manner. We've all heard of lost or stolen access cards in an office environment. Just consider a lost or stolen card in a much more secure location. For example, Schools, Military bases, Airports, and Hospitals. These are just a few examples but are very critical to a secure environment.
3. Eliminate archaic pin code as an additional security measure. Pin codes have their own challenges, most often the pin codes must be changed or as we have seen in countless applications there is one pin number assigned for all employees.
4. 36 percent of security breach issues originate from insiders
5. Single-factor "time and attendance theft" is equal to 4 percent of overall employee costs due to misuse of cards and employees signing in for each other
6. Can the administration of a 2-factor be made easier? That's what we at Blue Line Technology asked as part of their VOC (voice of the customer) design process.

Blue Line's design is simple. It is not dependent on the legacy access system to make the product work. By running a parallel system, the biometrics is much more reliable. The read range, accuracy, and speed of entry are first and foremost. Also, another benefit is you do not have to change the readers that you have in place. The 2nd factor is added in parallel with little to no impact on your existing system. The Blue Line solution is also not bound to any new software updates or patches that may impact your legacy system. One question is what about administering the new parallel system? The initial enrollment is the only time that you should have any major data entry. This can be accomplished in 15 to 30 seconds per person and will need no other changes after that. Once you have the picture you are good. There is an additional benefit by not being integrated into the access system. If you have a legacy issue and your system is inoperative, you can switch to single factor biometrics and continue business as usual until the legacy system is repaired.

Blue Line believes it is much better to interface into all access control products than to integrate into a few!

The Solutions:

Location 1 Solution: Avenue of America, New York

Blue Line Technology in concert with Gunnebo and Schneider Electric, a Blue Line Technology certified integrator, configured a multi-factor access management solution used in a unique building management solution. Building management companies have to address the different access

control needs of their tenants. Supplier partners Schneider Electric, Gunnebo, and Blue Line Technology addressed the needs. The team also wanted to address recent industry reports highlighting the need to bring together a multi-factor entrance solution with the elements of "something you have" plus "who you are" biometrics from the separate database that minimize threats of hacking and breaching. In this particular office location, the tenants may have Bluetooth devices, access cards, or bar codes scanner as a single factor. To complete the requirements the solution needed to be able to adapt to the different technologies plus add the second requirement of a biometric element facial recognition.

In this application, the customer selected a 3-lane suite of turnstiles using the Gunnebo OptiStile 220 swinging barriers model with a rich powder coated Cardinal Black finish. They coupled this with card reader capability and finalized the approach with the Blue Line Technology patented First Line facial recognition software. By addressing all the tenant's needs there is a minimal invasion with the access control experience and the installation proved to meet the best in class solution requirement. "Blue Line Technology working with the Gunnebo and Schneider Electric, was able to configure a flexible integrated solution that is most resistant to hacking or breaching yet remain comfortable for the users," said Gabe Keithley, Director of Customer Service for Blue Line Technology.

This solution focused on building management services gives each company/tenant a choice…they can use a single factor card, phone, or face and can enhance access with 2-factor capability. The option of having the ability to switch over to 2 factors, quickly is beneficial in cities and apartment buildings due to situational needs. The building management company in this instance is using the turnstiles just in the lobby but plans and offers access control options to each tenant on each floor. The first access control point is located in the lobby through turnstiles. Secondary access control including facial recognition is offered to tenants on each floor specific to their needs. The tenants on the upper-level floors are using facial recognition in this instance. This capability makes it ideal for multitenant applications and provides managed service configurations.

The benefit to the overall design is that it can be retrofitted onto existing floors without a need to tear out existing card readers. This addresses the cost impact of a completely new process while bringing forward best in class solutions. The organizations worked seamlessly to minimize installation time and maximize the value proposition.

Specific quotes from:

- George Gonzalez – Schneider Electric: The team at Blue Line Technology is a responsive group that understands the needs of the integrator and helps bring forward a great solution. The product performs exactly as the description.

- Nasheer Abdul – Schneider Electric: Projects like these have a lot of input from customers that must be considered. Blue Line helped us address every concern and commission a great solution.

- Tom Lally – Gunnebo: The suite of turnstiles is equipped with a lit bit of everything. They are aesthetically pleasing and provide the controls needed for the application. Bringing together multiple-factor authentication can be achieved while maintaining good looks and a streamlined finish.

(Frictionless (Touchless) entry Avenue of America New York)

Location 2: SPIRE (Utility Market Segment) St. Louis

Blue Line's 1:1 matching 2FA (two-factor authentication) factor provides an extremely accurate validation process for 2FA authentication, threat detection, and an enterprise approach to protect employees, visitors, and customers. Blue Line Technology, aware of Spire's emphasis on security for employees and facilities, approached Spire. Spire representatives hearing about the potential security enhancement opportunity brought the information forward to their security director. Spire's Director of Security, Al Moore, was receptive to exploring the concept of facial recognition and requested an on-site demonstration of our product. Blue Line installed a one-camera, Axis Q3505 MKII, system to be integrated into the current access control management system for two-factor authentications for his security staff around their SOC and security locations. Installation took less than 8 hours and another few hours of training multiple guards who would be interacting with the system.

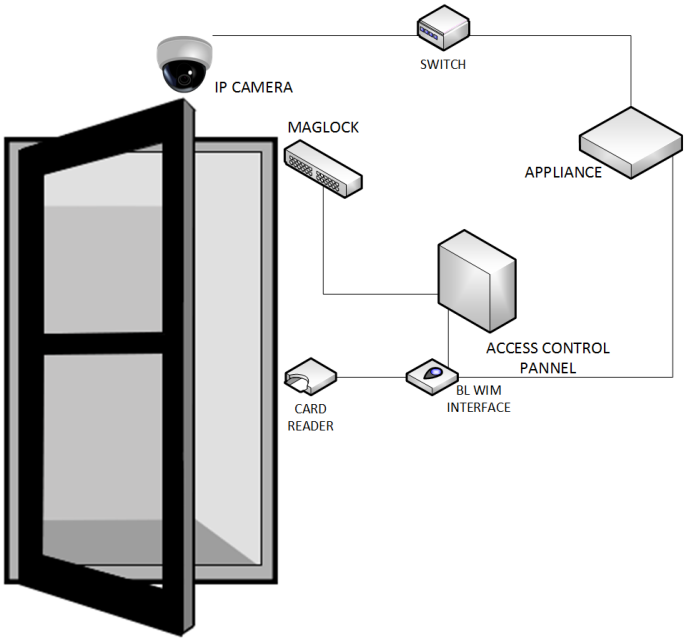
1. **Dual Authentication** – in certain vulnerable or sensitive areas, they want to add an extra layer of protection of security to protect from stolen or hacked credentials.
2. **Access Control**- desire to allow employees to pass through access control points "on the fly" without reaching for a card or fob with 2FA (face and the card read though the access control panel)

Results
After 30 days, Mr. Moore agreed facial recognition used for the two-factor was an effective and innovative method to enhance his organization's security. Spire identified several objectives that the facial recognition 2FA may be the solution for:

1. **Dual Authentication** – in certain vulnerable or sensitive areas, they want to add an extra

layer of protection of security to protect from stolen or hacked credentials.

2. **Access Control**- desire to allow employees to pass through access control points "on the fly" without reaching for a card or fob with 2FA (face and the card read though the access control panel)
3. **Remote Monitoring and Detection** – with Spire's rapid expansion into other markets outside their region, they wanted to upgrade security in certain remote facilities that can be monitored from their head office in St. Louis SOC (security operations command).
4. **Threat Detection** – that is parallel in all applications, they are provided with immediate notification of fired employee or unauthorized person trying to gain entry.



(Card and Face) entry Spire Security Operations Center)

Location 2 Summary

The physical security world is driving to protect sensitive information and control staff and the public from accessing restricted areas. Blue Line's 2FA solution provides a cost-effective, immediate verification and threat notification all within one camera placed at the door. This method of authentication provides the "who is carrying the credential" and ensures they have access to the door. Plans for Spire's turnstiles will be drawn up to include 2FA facial recognition authentication in their main lobby of Spire's headquarters. Employees will gain entry to the facility and then be provided with "on the fly" two-factor authentications in secure and restricted areas without the inconvenience of reaching for their card. Blue Line Technology's First Line Facial Recognition system with 2FA was designed to create a safer and more secure environment, allowing multiple client locations to work seamlessly.

Specific Quotes from:

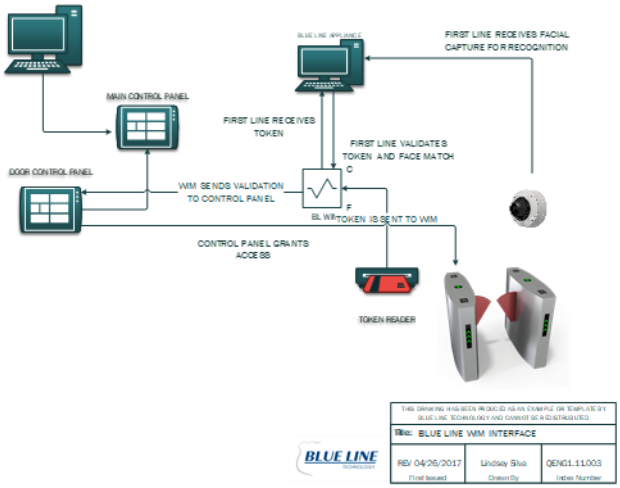
- Mr. Al Moore- Spire: We purchased the initial system and deployed the first camera at our SOC then added a camera at a second location. The results exceeded expectations for ease

of access for security personnel to enter the SOC and keep unauthorized individuals from entry. The security officers, now familiar with the 2FA solution have planned future deployment within their campus.

- John Frank – Spire: The Blue Line access control solution has provided selected areas within Spire Energy an added layer of security while providing a contact-free validation process to gain entry into restricted areas.

Location 3: Johnson Controls Birmingham

Identifying clients or specific individuals of interest gives the user situational awareness needed to successfully secure their environment. Johnson Controls took an advanced approach to the use of facial recognition capabilities with Blue Line's First Line software. Located on a higher floor of a multipurpose office building, the management team of JCI was looking for a solution that provided flexibility to their employees in concert with a new turnstile system being installed. The overall objective was to examine a market loaded with Access control products, and determine the advantages of new technologies for an enhanced security platform. They believe companies are playing catch up to add new solutions for a growing legacy issue. Their goal, to add 2-factor capabilities to the system without major integration changes? It is difficult to navigate through the decisions of access control suppliers for readers that integrate into their systems for visitor management, employee attendance, and door access. The operations team recognizes the logical choice is biometrics. But they wanted to understand more.
All biometric capabilities provide the opportunity to add a 2nd factor to the existing access system. The access control manufactures are quick to point out that a biometric solution can be integrated into their platform. The problem is that there is a cost associated with this integration and a cost to maintain the integration. Access control manufacturers constantly upgrade their software with patches and new capabilities. This constant change poses a challenge with integrated biometrics. The question then becomes is it worth the cost to add a 2nd factor to a door?



(Frictionless (Touchless) Schematic JCI Office)

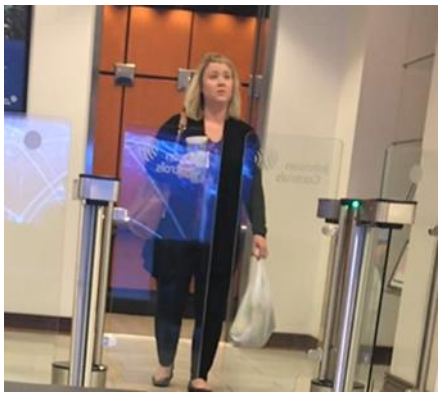
Anthony Richards (Product Specialist) is quick to answer yes and believes it is well worth the cost. The alternative parallel approach has strong advantages. The reason for 2- factor solution is obvious. Ask a security/access administrator about the challenges of managing employee access to

any employer. A common issue you have is the lost or stolen card. With recent advancements in cloning devices, the security engineers understand that card duplication is getting much easier all the time. Employees that work together often pass cards back and forth to avoid the reporting of a lost or stolen card. In some cases, the expense of replacement is passed onto the employee. With the lost or stolen card, there is always the chance that the card is used maliciously. We've all heard of lost or stolen access cards in an office environment. Just consider a lost or stolen card in a much more secure location. For example, Schools, Military bases, Airports, and Hospitals. These are just a few examples but are very critical to a secure environment. Johnson Controls was looking to make the administration of a 2-factor solution easier. The operations group in Birmingham validated the Blue Line solution achieved its desired outcome.

Specific Quotes from:

- Anthony Richards – Formerly, JCI: The Blue Line solution has demonstrated an ideal way for current security systems to be enhanced without the need for costly tear out projects. The solution is advantaged for companies facing the need for enhanced security with a comprehensive low-cost solution that can be managed without constantly upgrading software.
- David Haynes – JCI: We installed the system on the 6th floor off the elevator. It is wired for either face or card and our employees find the hands-free benefit very useful. The installation was simple and we mounted cameras to the wall to minimize installation costs. The facial recognition solution has met every expectation.
- Jeff Oswalt - Regional Sales JCI – Our applications team tested the system with an option of face/fob to provide easy frictionless access. The system has operated flawlessly for 2 years and we see this as an important part of an access strategy.

Location 3 Summary:
Engineers report Blue line's design is simple. The solution is not dependent on the legacy access system to make the product work. By running a parallel system, the biometrics is much more reliable. The read range, accuracy, and speed of entry are first and foremost. Also, another benefit is that current readers do not have to be changed significantly reducing the cost of the enhanced security solution. The 2nd factor is added in parallel with little to no impact on your existing system. The Blue Line solution is also not bond to any new software updates or patches that may impact your legacy system. One question is what about administering the new parallel system? The initial enrollment is the only time that you should have any major data entry. This can be accomplished in 15 to 30 seconds per person and will need no other changes after that. Once you have the picture you are good. There is an additional benefit by not being integrated into the access system. If you have a legacy issue and your system is inoperative, you can switch to single factor biometrics and continue business as usual until the legacy system is repaired. Key application engineers responded it is much better to interface into all access control products than to integrate into a few!



(Frictionless (Touchless) entry at Johnson Controls Birmingham)

Summary

Each building scenario was looking for a solution that provided a deterrence effect without a caustic approach to security enhancement. The Blue Line Technology solution with a focus on Biometric Interface instead of integration drove the cost of the solution to the lowest possible rate. The IT leadership along with Security leadership agree that the enhancements are substantial and address the common needs:

1. The enhancement interfaced with existing access control.
2. The installation as an addition to existing security proved cost beneficial.
3. The touchless entry capability was seen as a significant improvement.
4. The message of security improvement resonated throughout the company.
5. Registration is a simple process.
6. The desired outcomes were achieved.

A 2 Factor solution is not necessary for every door. In many situations, once inside the building the desire is a validation. The goal is to provide the access control point without the hassle that many systems offer. These locations represent floor controls, data room controls, Security Operation Center controls with a surveillance record. As we move into less intrusive solutions the Blue Line 2 Factor application has addressed the need and made the access control process hassle-free.