Mitigating Risk with Security Entrances

BOON EDAM

your entry experts

Table of Contents

Section 1

Introduction

BOON EDAM

Introduction

Security entrances provide the most effective way to control the actual number and direction of people passing through an entrance.

Organizations face a wide range of risks, some of which can be addressed by controlling access to a building, an outside area, or an interior space. In the past – and even today – controlling access to such areas has been done by many firms simply by using locks on doors or gates. Larger and more sophisticated organizations use enhanced methods including access control systems to control electronic door locks, and even security guards posted at key locations. Some organizations employ security cameras at key locations to monitor access.

The trouble with each of these methods is that they have critical weaknesses. And because of these weaknesses, there are limitations on how well they can mitigate real-world risks for the organizations they serve. A door that swings or slides open does not control who enters, no matter how sophisticated the lock is. An access control system can manage who can open such a door, but once it is open, any number of people can freely enter or exit. It is not even possible to ensure that the person who was authorized to open the door actually entered. Adding cameras doesn't change the situation, other than to make it possible to replay what happened at a later time. Even adding guards may have limited impact – they can easily be distracted, misled or overwhelmed. These approaches are not enough to manage business risks related to access control.

Security entrances provide the most effective way to control the actual number and direction of people passing through an entrance. This paper will discuss security entrances and provide a baseline of understanding that will help managers, specifiers, and users understand what security entrances do, and how they relate to managing business risks.

Section 2

Risks to Businesses and Organizations

BOON EDAM

Risks to Businesses and Organizations

Every organization, no matter what size or type, faces a wide range of risks on a daily basis. Of all these various risks, there are five categories that are clearly related to, or directly affected by, access control. This is because in these five categories, the risks increase significantly when an unauthorized person has gained access into a controlled area, whether it is a building, a part of a building, or a restricted outdoor area. In every case, managing the risk involves either knowing that the unauthorized person has entered so that an appropriate response can be initiated, or better, preventing the unauthorized person from entering at all. As we've mentioned earlier, standard swinging doors alone, even when normally kept locked, cannot provide the kind of assurance needed to manage these risks. Here are the five risk categories that are related to controlling the physical access of people:

The **risks increase significantly** when an unauthorized person has gained access into a **controlled area**, whether it is a building, a part of a building, or a **restricted** outdoor area.

Safety: Some areas are dangerous to life and safety, and should only be accessed by authorized, and usually trained, people. This might include storage areas for dangerous materials such as acids or explosives, or it could involve potentially dangerous equipment or machinery. Only specifically trained personnel should enter.

Physical Security: Like "safety", this category is about protecting people, but in this case rather than keeping people safe by keeping them out, physical security keeps those that are already inside (staff, visitors, etc.) safe from attack by outsiders intent on assault, robbery, domestic violence, shootings, etc.

Loss Prevention: All organizations have assets worth protecting. They may be tangible, such as materials, equipment, or finished goods, or they may be intangible such as business plans and intelligence, customer billing information, personal information of the staff, and other data. It may seem obvious to control access to physical materials, but unauthorized physical access to internal networks, data servers, and physical records can potentially be even more damaging to the organization.

Liability: Some organizations are regulated in ways that require controlling physical access as a prerequisite for operation, including some energy facilities, healthcare records processing, and similar functions. Access control systems provide the proof of compliance these teams need for regulatory oversight and audit purposes. Other

Defending against **potential liability**, even in the case of accidents, often depends on being able to demonstrate that firms have taken steps to implement and **enforce policies consistently**.

organizations can help control their risk of liability by controlling access – for example, an exercise facility can be exposed to liability if someone who is not a member uses the equipment and gets hurt. Defending against potential liability, even in the case of accidents, often depends on being able to demonstrate that firms have taken steps to implement and enforce policies consistently.

Business Continuity / Loss of Productivity: Operations can be disrupted by the entrance of unauthorized people, causing a range of negative impacts from bad publicity to actually stopping work. In one example, a parkour enthusiast sneaked into the new World Trade Center Tower construction site and took 'selfies' from the building's spire, leading to several days of negative publicity about security management of the project after a spend of roughly 20 million dollars. Recently, at a major bank in an urban location, protestors pushed into the lobby area and blocked employees from going to work. And at a manufacturing plant, uncertainty whether a specific individual was in the building led to a work stoppage of several days while the police decided whether or not the plant was a crime scene. Any of these events introduced a loss of productivity from mild to severe and negative news from the incidents. Other potential costs for these sorts of incidents are unbudgeted sick days and the need for employee counseling due to fear or anxiety.

As can be quickly seen from this list, the risks in these five categories are not trivial. Managing them should be, and often has been, a management priority. However, as described in the introduction, the traditional tools for access management, including locks on doors, access control systems and guards, each have weaknesses that can reduce their effectiveness. At low effectiveness, they cease to be management tools and instead give the impression of security but without the reality. Fortunately, there is an additional tool that can be deployed alone or in conjunction with these traditional tools to boost their effectiveness and regain the intended benefits: security entrances.

Section 3

Characteristics of Pedestrian Security Entrances

BOON EDAM

Although there is a range of entrance styles, costs, and operational methods, all security entrances share a basic nature. This is because in general, the purpose of all security entrances is to create a general deterrent and an actual barrier to unauthorized infiltration, while allowing ready access to authorized people. The differences between the styles of security entrances are related to the level of security required and to aesthetic considerations. In all cases, appropriate provision must be preserved for emergency egress, as required by local and national codes including ANSI and NFPA, among others. Here are three other inherent characteristics of security entrances:

Staff Productivity: By their nature, security entrances are intended to reduce or eliminate staff workloads with regard to monitoring entrances, controlling authorized access, and preventing unauthorized access to a controlled area. Such monitoring personnel are often tasked with related activities that can take up their attention, such as maintaining visitor logs, answering questions, and screening for weapons. Using a security entrance alone, or in conjunction with metal detectors and other screening methods, can reduce the need for staffing and/or allow the staff at those entrances to focus their time and attention on important screening tasks.

Shell Chemical

Challenge: The Deer Park Shell facility is regulated under the Maritime Transportation Security Act of 2002. These security regulations focus on certain sectors of the maritime industry that would benefit from increased security, such as tank vessels, large passenger vessels, offshore oil and gas platforms, and port facilities for dangerous cargo. Under MTSA, Shell has to be able to account for who is in the production area at all times.

Solution: Swinglane 900 swinging optical turnstiles were installed between the administrative building and production plant, allowing Shell to account for everyone in the facility at any time. The high throughput supports the almost 3000 people that work in that area each day, and an audible alarm alerts staff to tailgating attempts for quick intervention by attending staff in an adjacent office.

The purpose of all **security entrances** is to create a general deterrent and an **actual barrier** to unauthorized infiltration, while allowing ready **access to authorized people**.

Characteristics of Pedestrian Security Entrances

Regulatory Compliance: Security entrances, by their nature, can also support regulatory compliance regarding infiltration into secure areas. This is because these entrances can be configured in a range of security layers, and at each level, can be used to create auditable logs. At the highest security levels, regulated organizations can demonstrate systematic mitigation of unauthorized access while allowing quick access to authorized staff.

Accurate Measurements: Perhaps the most powerful inherent characteristic of security entrances is that they enable the collection of accurate, definitive measurements. In conjunction with an access control system, they can provide an auditable trail of entrance and exit attempts, admissions, and denials for a range of possible business needs, including:

a. Mustering: "Who is in the facility right now?"
b. Investigations: "What time did Bob leave the building last Friday?"
c. Business Analysis: "How many customers come to the gym at each time of day, and how long do they stay?"
d. Security Planning: "What time of day do most of the access denials occur?"

At the very highest level of security, wherein security revolving doors and mantrap portals are implemented, (more on this in Section 4) there is at last the possibility of providing an accurate answer to the question, "What is the probability of an unauthorized infiltration tomorrow?" In the past, even with the use of full-time guards, there has been no accurate way to quantify that risk. Now, it is possible to provide specific metrics on this potential for a breach and demonstrate a quantifiable return on investment using these highly effective security entrances for business purposes.

At the **highest security levels**, regulated organizations can demonstrate systematic mitigation of unauthorized access while allowing **quick access** to authorized staff.

Section 4

Four Levels of Risk Mitigation Supported by Security Entrances

BOON EDAM

Four Levels of Risk Mitigation Supported by Security Entrances

As was described previously, all security entrances are designed to allow passage of authorized people while serving as a deterrent or actual blockage for unauthorized people. However, not all security entrances work the same way. This section will divide security entrances into four groupings, and describe how the characteristics of the four groupings result in a series of increasing risk mitigation levels. Organizations, knowing what other security methods will be deployed in tandem with the security entrance, can choose to implement the level of risk mitigation they need to serve their objectives.

Before describing the four risk mitigation levels, there are two other concepts that are important to understand. The first of these is that all security and risk mitigation efforts related to access control depend on credentials for establishing and confirming the identities of authorized people. The credentials process is outside the scope of this paper; suffice it to say that the selected credentials should be of the same security level as the rest of the system or they will become the weak link.

The second concept is that of "tailgating and piggybacking". Often these words are used interchangeably, probably because when many people think of a swinging door, there isn't much difference. However, with security entrances the two words are slightly different in meaning.

Tailgating describes a situation when a second person follows an authorized user through an entrance without using credentials, and assumed to be an intruder. For example, with an optical turnstile, the tailgater rushes through the open barriers before they close behind the authorized user. With a security revolving door, the authorized user presents their credentials and steps into a compartment alone to proceed into the secure area while the tailgater attempts to ride in the trailing compartment.

Piggybacking is about two people working together to enter on a single authorization. The situation could be "friendly collusion" (two coworkers when one forgot their credentials) or "coerced collusion" (intruder and employee under duress). The term applies specifically to security revolving doors or mantrap portals where two people could enter a compartment together and attempt to pass through.

From a risk management viewpoint, every entering person must be authorized to meet the objectives of the security entrance, so tailgating or piggybacking is always considered an intrusion. This concept is so important that to a great degree, the difference between the security levels described below for security entrances is the extent to which they can be defeated by attempts at tailgating and piggybacking.

As the four security levels are described, keep in mind that multiple levels can be deployed as "layers" on large campuses or even in the same building to meet the varied needs of different areas.

From a **risk management viewpoint**, every entering person must be authorized to meet the objectives of the security entrance, so tailgating or piggybacking is **always considered an intrusion**.

Level 1: Crowd Control

Nature

Security Level 1 entrances help staffed entrances cope with large numbers of authorized people who have to enter or leave a secured area in a short timeframe. Level 1 systems are designed to slow down and organize entry and "keep honest people honest"; they present visual deterrents to potential infiltrators while preserving a relatively open appearance for authorized people. Typical applications include sports stadium entries, factory shift changes, transit terminals, and high-occupancy, high rise buildings. Level 1 employs simple mechanical or electro-mechanical technology to achieve the goal of high throughput while counting each authorized person, and offers the lowest capital cost. There are normally no detection sensors of any kind, and so defeat is possible by jumping over or crawling under barriers. Therefore, manned security is needed to deter attempts to defeat and/or to respond quickly after an infiltration incident, increasing the operating costs. By slowing down high volume traffic, and forcing an orderly flow of passing people, Level 1 enables supervisory staff to more effectively monitor the process.

Organizationally, there must be a structure and provision for the **ongoing training of guard staff**, as well as scheduling shifts, ensuring break coverage, and **enforcing procedures and policies**.

Type

For applications where controlled entry is the security goal, tripod turnstiles have proven to be the ideal solution, as they effectively direct users through specific, guarded entry points. Entertainment venues, transit stations, and public buildings, among many types of applications, choose tripod turnstiles for their ability to withstand a large volume of users while maintaining their integrity.

Throughput

Waist-high tripod turnstiles can process up to 30 people/minute in one direction at a time, including access control processing time. If there is a lot of two-way traffic, such as during shift changes or lunch, then the max throughput per direction falls to 12-15. Adding more turnstiles to accommodate this traffic pattern raises space requirements and capital cost.

User Education

Waist high turnstiles do not typically require user orientation training.

Metrics Capability

Waist high turnstiles can count the number of people entering or exiting. The access control system can track all presented credentials. Due to lack of detection sensors or alarms on turnstiles, these systems cannot detect or track jumping or crawling infractions.

Strategy Implications

Organizationally, there must be a structure and provision for the ongoing training of guard staff, as well as scheduling shifts, ensuring break coverage, and enforcing procedures and policies. With the limited metrics available, there is a complete reliance on the supervision of the manned security to verify authorized identities, process visitors, create infraction reports, and any other related tasks. Tracking and measurements are only as accurate as what is reported or observed by the staff. This strategy is vulnerable to distractions, favoritism, and absenteeism, which all create opportunities for infiltration.

Martin's Famous Pastry Shoppe

The Challenge: Expansion created the opportunity to upgrade access to the bakery facilities, reinforcing a cultural commitment that Martin's employees are working together to bake the best products and provide the best sales distribution support in a safe environment. The safety and security of the bakery premises is also required by strict food production regulations.

Solution: Installation of an unmanned security revolving door at the entrance to the building prevents tailgating or piggybacking incidents and ensures only authorized employees can enter the premises. Management knows exactly who is on the production floor at any time, and the high quality entrance reinforces a perception that Martin's bread products is a premium brand to employees and visitors.

Payback/ROI
Level 1 minimizes up-front costs to provide a basic level of entry control. Payback is primarily its value as a visual deterrent and as a mechanism for controlling the entry rate of large groups. Business information is limited to metrics and incident responses provided by security staff. Ongoing operational costs are high relative to other capability levels because staffing is required to ensure compliance.

Level 2: Deter

Nature
Security Level 2 increases the deterrent factor of Level 1 by presenting a full height barrier that deters casual attempts to defeat by climbing or crawling. Similar to Level 1, there are no presence detection sensors or alarms and simple, mechanical or electro-mechanical technology is used. The full height barrier of Level 2 is often deployed at a perimeter fence line as a first layer of physical security, and in such cases may not be directly supervised by a guard. Another use is for "exit only" to allow

Therefore, **with limited metrics** and no piggybacking alarm, unmanned full height turnstiles are often **part of a multi-tiered security plan**, where other types of security entrances are relied upon to enter and move deeper inside buildings and other secure areas.

people to leave but deter them from entering, similar to the exits used at the New York Metro subway system.

Type
Full height turnstiles fulfill the description of Level 2 with their full height barrier that eliminates crawling under. Climb-over attempts are deterred when used with suitable fencing or wall systems. For applications where the security goal is to deter or deny all casual infiltration attempts, full height turnstiles are a proven cost-effective solution. They only allow travel in one direction at a time, and provide a rugged, high-visibility entrance for both indoor and outdoor installations. Parking areas, equipment or supply yards, construction sites, heavy industry, manufacturing and energy facilities, and facility and campus perimeters are all ideal locations for the application of Level 2 entrances.

Throughput
Full height turnstiles handle up to 18 people/minute in one direction, including access control processing time. As is the case with Level 1 turnstiles, Level 2 turnstiles are most efficient during one-way rush periods such as shift changes or lunch periods. During periods of two-way traffic, the maximum throughput drops to 7-9 per direction. Planning the optimum number of turnstiles for a particular installation requires knowing the expected traffic patterns to prevent unnecessary bottlenecks.

User Education
Full height turnstiles typically do not require special user education.

Metrics Capability
Full height turnstiles can generally count the number of inbound and/or outbound people with greater accuracy than waist high turnstiles because of their greater resistance to climb-overs and crawl-unders, but they are vulnerable to piggybacking, which can remain undetected without sensors or guards present. When integrated with an access control system, submitted credentials can also be tracked.

Strategy Implications
With collusion or coercion, two small people could physically piggyback in a single compartment of a full height turnstile. Therefore, with limited metrics and no piggybacking alarm, unmanned full height turnstiles are often part of a multi-tiered security plan, where other types of security entrances are relied upon to enter and move deeper inside buildings and other secure areas. One exception to this is when the budget is restricted and they are deployed indoors; in this case, the turnstiles should be supervised. In summary, the impact of the overall strategy depends on the capability level deployed for the building entrance and interior areas.

Payback/ROI
Level 2 entrances provide a higher level of entry control security than Level 1, with a modest increase in capital cost and, when used outdoors, the elimination of most direct guard supervision costs. The payback of full height turnstiles is the strong visual deterrent and denial of casual infiltration, making it ideal for more distributed or isolated entrances on perimeters, and as an initial layer in a multi-tiered security plan. Operating costs are very low (including ongoing maintenance) relative to other capability levels because there is typically no direct guard supervision, or they are remotely monitored.

Full height turnstiles can generally count the number of inbound and/or outbound people with **greater accuracy** than waist high turnstiles because of their greater resistance to climb-overs and crawl-unders.

Level 3: Detect

Nature

Level 3 security entrances employ sensor technology to accurately detect objects moving through the opening, and can determine whether one or two people are passing. In this way, they can detect when tailgating or piggybacking occurs, and sound an alarm when it is detected. The detection technologies can be sophisticated enough to tell the difference between a tailgating person (raising an alarm) or a rolling bag or umbrella (which should not raise an alarm). Like Level 1 and Level 2 security entrances, they present a visual deterrent to casual infiltration, and provide a mechanism for integrating with access control systems and credentials. They are not expected to completely eliminate infiltration, but they are equipped to reliably detect attempts and successful infiltrations. They strongly differ from Level 1 and Level 2 entrances because any infiltration is immediately detected and raises an alarm so that staff can react during, or after, the event. Thus, Level 3 security entrances provide an increased measure of security regarding infiltration while improving aesthetics in terms of appearance and openness.

Type

Optical turnstiles fall into this category, and due to their sensor technology and materials, they have a moderately expensive capital cost. Optical turnstiles are usually equipped with a physical barrier such as a gate or swinging doors (sometimes as high as 6 feet) that retract or open when access credentials are accepted, providing both a barrier to people approaching the entrance, and a visual cue when the credentials are accepted and someone is approved to proceed. Level 3 entrances cannot prevent tailgating attempts because the barriers remain open long enough for a second person to rush through. They could also be violated by climbing over or crawling under the barriers, but these cases can also be detected and generate an alarm automatically. Optical turnstiles are particularly popular in corporate lobbies, and other interior applications such as separating portions of shared workspaces, where their appearance adds prestige and an attractive aesthetic for the organization.

Level 3 security entrances employ **sensor technology** to accurately detect objects moving through the opening, and can determine whether one or two people are passing.

Throughput
Optical turnstiles with barriers can process up to 30 people per minute going in one direction, including processing time for integrated access control. As with Level 1 and Level 2 turnstiles, the capacity for optical turnstiles drops when traffic moves in both directions; in that case the max throughput per direction falls to 12-15. Adding more turnstiles to accommodate this traffic pattern increases space requirements and capital cost, so planners need to understand the expected usage patterns and plan the number of needed lanes accordingly.

User Education
To ensure user safety, all users require some minimal training to be familiar with the procedure for providing their credentials and proper conduct related to negotiating moving barriers and "taking turns" during two-way traffic periods. This will also ensure the highest degree of throughput and minimize erroneous alarms, such as, for example, loitering inside a lane without presenting credentials. Note that many models have extra sensors near moving barriers to help prevent accidental contact with users.

Metrics Capability
Optical turnstiles are equipped with presence detection sensors, and therefore can provide accurate metrics including the number of authorized personnel inbound and outbound, and the number of tailgating incidents or alarms. Certain models equipped with dense sensor arrays can be set up to alarm and count jumping or crawling attempts. Access control can track all credentials submitted.

Strategy Implications
As mentioned, some minimal orientation or training is required for all users. The metrics are similar to non-optical turnstiles but with an added bonus: a far more accurate detection and count of tailgating incidents that can be used to guide improvements and strive towards elimination through user training and policy enforcement. However, if a quick response to alarms or additional deterrence is required, manned security must also be at the site, which brings with it the need for similar ongoing management and costs as with non-optical turnstiles. Finally, because optical turnstiles can have a very sleek, attractive appearance compared with other entrance options, they are usually readily accepted by building and organizational management.

Payback/ROI
The payback of optical turnstiles is in their value as a strong visual deterrent, particularly those with visible barriers, and in their ability to accurately detect piggybacking and tailgating intrusion attempts and raise alarms in real time. Due to reliance on security staff to monitor and respond quickly to infractions, ongoing operational costs can be relatively high when these costs are included. One reason optical turnstiles are so popular in corporate lobbies, beyond the visual prestige they add, is that security staff are often already stationed there to assist visitors and contractors. Thus, the high effectiveness of optical turnstiles to detect infiltration attempts can be deployed without significantly raising operational costs at such entrances.

One reason **optical turnstiles** are so popular in corporate lobbies, beyond the visual prestige they add, is that **security staff** are often already stationed there to assist visitors and contractors.

These **security entrances** not only serve as a visual deterrent, but **physically deny** all forms of unauthorized entry – including tailgating and piggybacking.

Level 4: Prevent

Nature

Level 4 introduces true tailgating and piggybacking prevention for higher-security facilities and for locations where security staffing is impractical. As this statement implies, these security entrances not only serve as a visual deterrent, but physically deny all forms of unauthorized entry – including tailgating and piggybacking. To achieve this objective, they must incorporate full height barriers to prevent crawling under and climbing over, as well as sensors to ensure that only one person passes through at a time. Properly designed and integrated with a strong access control system, Level 4 security entrances provide the highest level of security protection, allowing only authorized people to enter, without the need for security staff supervision.

Type

There are only two types of entrances that are able to support Level 4: security revolving doors and mantrap portals. These can be implemented to detect and prevent tailgating because they both make use of full height barriers that cannot be defeated by crawling under or climbing over, and because both can be equipped with sophisticated sensors that can ensure that only one person is passing through the entrance. If one person attempts to tailgate in the trailing compartment of a security revolving door, they are rebuffed while the authorized user can enter the secure area. If two people attempt to piggyback in either a security revolving door or mantrap portal, both users are rebuffed to the non-secure side. Level 4 security entrances are the solution of choice for employee-only entrances to commercial buildings of all types, high security facilities, and critical or regulated data centers and records facilities (such as medical and financial records and processing).

Throughput

A security revolving door can handle a maximum of 20 people per minute, per direction simultaneously, for a total of 40 people passing through each minute (half in each direction). A mantrap portal can process up to 6 people per minute, but only one at a time in either direction. There are some factors that will slow down throughput: the use of optional, and heavier, bullet-resistant glass or the use of dual authentication. Capital costs are impacted by how many entrances you need during peak one way and two-way traffic flow periods.

User Education

Because of the relative complexity of the sensors, alarms and moving parts, an orientation program is a must for Level 4 entrances, so users can be trained on how to use the entrance properly and safely. Trained users also keep the number of false rejections, due to user errors, down to a minimum.

Metrics Capability

Due to the integration of sophisticated near-infrared sensors and optic technologies, Level 4 entrances can provide a rich assortment of metrics, including: authorization received, passage

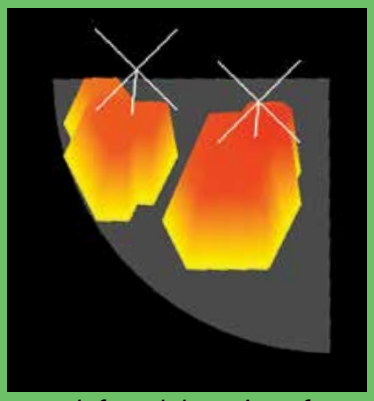
Level 4 Security Entrance Sensors and Predictive Metrics

A critical element of a Level 4 security entrance is the ability to use sensors to confirm that only one person is attempting passage. When a Level 4 entrance is used, whether it is a security revolving door or a mantrap portal, there is a point where the person attempting passage is temporarily "trapped" inside a compartment. It is at this point that the system must confirm that only one person is in the compartment.

In the past, sensitive floor mats were used to detect more than two feet pressing on the floor of the chamber, but people quickly found that if one person literally was "riding piggyback" on the other, this test would be defeated. Setting a weight range could exclude some piggybacking attempts, but that approach raised other complications. Weight mats are not in common use any more.

Instead, leading suppliers have improved other types of sensors to achieve this task. For example, Boon Edam employs a sophisticated overhead sensor technology called StereoVision 2® which scans the entire compartment using near-infrared scanners and "time of flight" technology. By measuring the time it takes for beams to bounce off objects in the chamber, it forms a 3D image of the contents of the compartment; by analyzing this image, the system can determine with a very high accuracy whether one or more than one person is in the compartment.

Managers can adjust several parameters in StereoVision2® that will affect the sensitivity of the assessment to meet the needs of a facility; this exercise results in access to predictive analysis of the risk of a potential breach by piggybacking. As a manager adjusts the sensitivity higher, it is more likely that individuals will be rejected erroneously for wearing a lumpy backpack or fidgeting, for example. Lowering the sensitivity will decrease rejections (be more forgiving) but increase the risk of potential piggybacking breach. Calibration therefore involves finding the balance between convenience and risk. As the sensitivity is adjusted, StereoVision 2® displays the chance of a successful piggybacking breach as a percentage per 100 attempts using highly accurate sampling data. Considering that piggybacking attempts are rare to begin with, many managers have calibrated their doors to a risk of piggybacking to 5% or lower, while still keeping unintended false rejections at a reasonable level. This is an example of the predictive probability metric regarding potential breach that can be obtained for a given entrance, which is something that other types of security entrances or guards cannot provide.



Infrared detection of piggybacking attempt

Managers can also set every employee entrance to the same settings across many facilities, or tailor each door differently to meet unique needs. Once a manager determines a set of preferred settings, all the doors set the same way will work in the same way, regardless of where they are located, time of day, or any other variable. This way, management can have a clear understanding of the risk at these entrances and be certain that any infraction is not an accident.

For mantrap portals, there is one additional assurance that can be employed. To ensure that the person that presented the accepted credentials at the start of the process is the same person that is passing through the portal, a biometric sensor can be located in the transit compartment to confirm the identity of the person as they are passing through the portal. If they cannot confirm their identity with the biometric sensor, they are denied entry.

completed, tailgating/piggybacking rejections inbound or outbound, biometric access control rejections, safety rejections, and emergency button rejections. Security managers can use the access control system to count rejections and then investigate the optic records to discover why those rejections occurred. Most importantly, today it is possible to obtain predictive metrics that can provide a probability of piggybacking infiltration in terms of a percentage (see "Sidebar: Level 4 Security Entrance Sensors and Predictive Metrics" for more information).

Strategy Implications

Detailed and predictive metrics without the need for security staff makes Level 4 the most reliable strategy to eliminate tailgating and piggybacking. In addition, installing security revolving doors and portals provides a consistent, verifiable and auditable "standard operating procedure" for inbound and outbound traffic that can be tailored to automatically support organizational policies. By understanding and determining false acceptance and rejection ratios through sensitivity calibration, and by verifying a door's performance over time, management can develop an objective, predictable and quantifiable risk of intrusion that can be proactively managed.

Payback/ROI

The primary payback for Level 4 security entrances is a combination of the visual deterrent, the highly secure working principle that will only admit authorized personnel while denying tailgating and piggybacking, and the detailed metrics that can be used to monitor and improve the security programs. These entrances are the most expensive per unit in terms of capital costs due to the sophisticated technologies within. However, since no security guards are needed to monitor these entrances, they can be reduced in number or reallocated to higher value activities to provide a tangible, ongoing financial payback on the investment. Many organizations find that the capital cost of installing Level 4 entrances can be recouped in as little as one year. Ongoing operational costs involve only routine maintenance, making Level 4 entrances an increasingly desirable option for many organizations.

Detailed and **predictive metrics** without the need for security staff makes Level 4 the most reliable strategy to **eliminate tailgating and piggybacking**.

Section 5

Summary and Conclusion

BOON EDAM

Summary and Conclusion

With numerous different types of **security entrances** available, organizations can work with an expert to design a customized plan for their facilities that capitalizes on the **varying levels of security** to provide **optimal protection** at the most **efficient cost**.

Organizations today face a wide range of risks regarding safety, loss prevention, liability, business continuity, and more. Traditional methods of controlling access, particularly those with swinging or sliding doors, have critical weaknesses, no matter how strong the locks are or how carefully credentials are prepared.

Answering these three questions will provide a basis for prioritization and planning:

1. What is the current vulnerability of your organization to a tailgating intrusion?
2. What are the potential costs of the wrong person getting into your building?
3. If these costs are not acceptable,what commitment in terms of budget and process is your organization willing to make to limit your vulnerability to tailgating and intrusion?

Security entrances are the best tool to manage business risks related to access control. With numerous different types of security entrances available, organizations can work with an expert to design a customized plan for their facilities that capitalizes on the varying levels of security to provide optimal protection at the most efficient cost. And because certain types of entrances eliminate the need for personnel to man the access point, even the most advanced and sophisticated type of security entrance can provide a surprisingly high ROI by eliminating the cost of security guards. Ultimately, security entrances are a good investment for any organization that needs to control access to any points in their facilities.

About Boon Edam

Our World Revolves Around Yours

Boon Edam is a global market leader in security entrances that go beyond detection to prevention of tailgating. With 140 years of experience, we have proven expertise in managing the entry, egress and transit of people within facilities. Our turnstiles, security revolving doors and mantrap portals provide a first line of defense for facilities while our customer focus takes individual needs into account to determine the best approach to maximize ROI and security requirements.

Contact Us

402 McKinney Parkway
Lillington, North Carolina 27546
United States of America

T +1 910 814 3800
www.boonedam.us

BOON EDAM

your entry experts