RISK BASED SECURITY:

BALANCING SECURITY, VISITOR EXPERIENCE, OPERATIONAL EFFICIENCY, AND COST CONSIDERATIONS

BY JOHN PISTOLE AND MARK SULLIVAN

EXECUTIVE SUMMARY

All security systems are designed to keep people safe. The challenge is balance. Does the security present an undue burden, either to the provider or to the customer, does it evoke a sense of safety, and does it operate within the cultural bounds of the venue? And of course, how much does it cost? Security experts generally agree the use of a venue specific risk-based security (RBS) approach is preferable to "one-size fits all" solutions. Flexibility and adaptability are key factors in RBS solutions, allowing "tailored" systems designed to mitigate risk while maximizing customer movement or throughput with minimal disruption. Based on our experience, we believe that Evolv Technology's Edge platform provides the best RBS solution to detect metallic and non-metallic threats that cause mass casualties.

For optimal effectiveness and efficiency security providers must know and understand the type of threats being posed. Iconic landmarks obviously pose higher risks than other locations. The determination of what are called the Design Basis Threats (DBT) is often as much art as science, depending on outcomes sought by the security provider. Ideally, all security measures are informed by historic and current intelligence of the threats and vulnerabilities and are flexible enough to adapt to emerging trends.

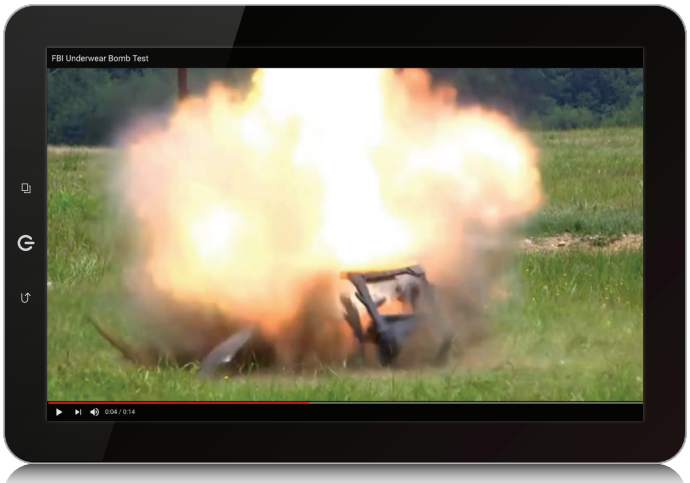
There are a number of threat scenarios RBS systems can address, including:

1. **Active Shooter**
2. **Person Borne Improvised Explosive Device (PBIED)**
3. **Vehicles as a Weapon**
4. **Vehicle Borne Improvised Explosive Device (VBIED)**
5. **Chem/Bio/Rad/Nuclear (CBRN)**

For purposes of this paper, we will focus on the first four. Once the venue is identified, threats and vulnerabilities can be assessed, and tailored security solutions can be implemented.

Traditional solutions usually involve security officers physically inspecting persons and property entering the venue. Reliance on a known and trusted security team is critical to the success of this solution and the recurrent vetting of these employees is a key ingredient in this formula. This approach generally employs an inefficient one-size fits all model and can be quite costly. Currently, it almost exclusively includes walk through metal detectors (WTMDs) and/or wands, as well as manual inspection of backpacks and bags to detect metallic threats such as guns and knives.

The vast majority of airports worldwide still use this approach even though the most significant threat is now from non-metallic IEDs such as that deployed by the "underwear bomber" on Christmas Day 2009. Some airports and mass transit venues use bomb sniffing K-9s, either in addition to X-rays or in lieu of X-ray. However, most security experts agree that traditional solutions such as X-ray are simply insufficient (and human resource intensive) to properly mitigate against the evolving threat from non-metallic IEDs. It is critical to stay ahead of adversaries who are developing the capability to execute attacks with catastrophic consequences using even a small amount of non-metallic explosives, as seen in this 15 second video that shows the FBI's testing of the Christmas Day underwear bomb.



https://www.youtube.com/watch?v=tumVKQKab-s

Tailored security solutions are needed for sports and entertainment venues as well as religious and cultural venues and schools. High profile sporting and entertainment venues are high-threat targets for terrorists and others, such as seen in Las Vegas on October 1, 2017 with a lone gunman who killed 58 people and wounded more than 500. Evolv's Edge platform could have detected the weapons the shooter brought into his hotel room. Because the Edge system is portable and adaptable, concert promoters and tourism officials, working with area hotels, can deploy the Edge using a RBS approach. Similarly, the Edge could have detected the weapons used in the Orlando nightclub massacre where the shooter killed 49 people in June 2016.

The shootings in churches in Texas (2017) and Charleston (2015) demonstrate the vulnerability of Houses of Worship. Likewise, since 2000, there have been dozens upon dozens of school shootings resulting in multiple casualties, including at Virginia Tech, Sandy Hook Elementary School in Connecticut and most recently at Marjory Stoneman Douglas High School in Parkland, Florida. Parkland alone left 17 students and staff dead, and many others wounded. The examples we provide are helpful as they are illustrative, not exhaustive. All of these venues would have been good candidates for deploying Evolv Technology's Edge platform using a tailored RBS approach.

To be sure, no perfect security system exists. Utilizing the latest technology in a RBS manner enables event and venue operators to mitigate risk from known and unknown threats in the most effective and efficient way possible. RBS is highly flexible and can be easily implemented with sufficient training for all security personnel to ensure a coordinated approach that fully leverages human and technical resources while being adaptable to a changing environment or threat.

Evolv Technology's Edge was designed and built to aid an organization's move toward a risk-based security approach and provide balanced detection across a range of threats in a changing environment.

INTRODUCTION

The goal of every physical security system is to protect people and property. The challenging part is the development of an effective security program that operates within the cultural bounds of a venue, does not present an undue burden, and evokes a sense of safety for its users. In recognizing the natural tension between implementing security and creating an open inviting venue, a security system designer must define and quantify a trade space that accounts for customer experience, cost, and capabilities. This allows security providers to make informed decisions about which security approach works best for the expected risk of the facility, while also maintaining and even enhancing the environment the venue is trying to create.

One lesson that has been learned over the years is that the implementation of a Risk-Based Security (RBS) approach has a significantly higher acceptance and favorability by the public than those that do not provide any differentiation. The traditional screening systems now in place in many venues do not always balance the threat, are a source of frustration for patrons due to the lines and inconvenience, and many times have no way of evolving in response to a changing threat. Twenty years ago, few considered the need to screen people entering a place of worship, but it is now a serious consideration for many. While people want the safety that screening systems provide, they do not want to lose the culture, openness, and sense of welcome that makes their venue, stadium, or house of worship special and inviting.

While background information on traditional security solutions is provided below, it is done with an eye towards discussing Risk-Based Security (RBS) and the associated trade-offs security and operational executives must make in today's ever-changing threat environment. These principles are then applied to the security of sports and entertainment venues using state-of-the-art technology. Flexibility and adaptability are therefore key factors, allowing "tailored" systems designed to mitigate risk while maximizing customer movement with minimal disruption.

THREATS AND VULNERABILITIES

Any planned deployment of a security system must first take into consideration the highest probability threats and those it wishes to mitigate. Few venues are at the same level of risk as that of iconic buildings like the European Parliament, Buckingham Palace or the United States Capitol, and thus should not be expected to need or employ the level of security in place at those locations. The determination of what are called the Design Basis Threats (DBT), the primary threats that a security system is designed to mitigate, can be as much art as science and should be made in consultation with security professionals and local law enforcement support, hopefully all informed by current intelligence of the threats.

In general, though, the DBT for public venues and facilities such as stadiums, airports, houses of worship, and concert halls, for example, are relatively common unless there exist specific threats particular to local conditions. In today's environment the common DBTs that a facility's security system should be expected to mitigate, excluding every day crime, include:

Active Shooter Threats

The risk from this type of threat, especially in the United States, has steadily grown over the years from the Columbine shooting to the Orlando Pulse Nightclub to Las Vegas. In most instances, the highest risk to venues comes from weapons being brought into the facility and not from a stand-off sniper threat as experienced in Las Vegas. That said, security providers and promoters should coordinate with federal, state, and local law enforcement to understand the nature of current or emerging threats.

Person Borne Improvised Explosive Device (PBIED)

This threat has evolved from the dedicated terrorist focused on suicide bombings and now also includes the threat from an explosive device that is carried in and left behind. The explosive attack that occurred in London, where a backpack was dropped, and the failed attack in the New York City subway, where the perpetrator strapped the device to his back, reflect this growing trend.

Vehicles as a Weapon

The threat of this type of ISIS-inspired attack has also increased due to the ease of execution and ability to hide in plain sight until the moment of attack. These attacks have been executed in London, Paris, Berlin, New York, and Charlottesville in recent times. Unfortunately, most venues are vulnerable to this type of attack, either on the sidewalks and streets approaching the venue, or where entry queues may extend beyond the perimeter of a facility, creating an attractive secondary target.

Vehicle Borne Improvised Explosive Device (VBIED)

The vehicle borne explosive threat, while still of concern, has not been as prevalent as the first three threats and been limited primarily to the Middle East North Africa (MENA) and the South Asia region since the Oklahoma City bombing in 1995, with the exception of the failed attack by Faisal Shahzad in Times Square in 2010. Depending on the risk level of a venue and its configuration, especially access to underground parking such as was exploited in the 1993 World Trade Center bombing, this type of threat should be assessed as part of a cost/benefit analysis of employing mitigation measures.

Other Threats

For high risk iconic facilities there are myriad other risks that should be considered, from chemical, biological, or radiological attacks to stand-off explosive attacks to using aircraft as weapons. For the vast majority of venues though, active shooter, PBIED, and vehicles as weapons are the primary threats of concern and likely should be the primary focus of a security system.

Once the threats have been identified, those threats should help inform a vulnerability analysis of the facility. For public gathering venues the most likely vulnerabilities derive from the large numbers of people that enter for an event, either through turnstiles, gates, or into parking areas. These people present vulnerability both because they generally arrive unscreened and unknown to a facility, and the large numbers of people inside a facility and the queues they form outside present an attractive target. An attack on a crowd trying to get into a sports venue would be viewed as an attack on the venue/team even though it did not occur inside the facility. Identification of these key vulnerabilities allows the development of a mitigation strategy, such as ensuring the screening system is able to process people as quickly as possible to eliminate large queues and the target they present.

TRADITIONAL SECURITY SOLUTIONS

There are fundamental aspects to a safety and security program that are essential to any good program, including well supervised and trained staff, well thought out written emergency action plans, exercises to test plans, policies, procedures and staff response, partnership with first responders, command and control and surveillance systems, physical security systems, and personnel screening procedures for guests, vendors and staff. All of these elements are needed at one level or another depending on the threat environment, risk acceptance and vulnerabilities of a site to implement a strong security program.

In addition to an effective perimeter security system to ensure no one can enter surreptitiously, a key component of the overall system is effective screening of people entering the facility. Screening is one of the most critical strategies of a security system and, if done properly, will ensure that weapons or explosives are not smuggled into a facility. An equally important goal of the screening system should be to ensure that people queuing to enter the facility are processed as quickly as possible.

The traditional practice for screening individuals entering a facility is to use security officers to conduct bag checks while other security officers implement metal detection screening using walk through metal detectors or handheld metal detectors. All people screened are treated the same, whether it's an executive of the sports team who owns the facility or a patron visiting a venue for their first game or event. While this approach is widely utilized, it represents a huge investment in equipment and staff to check every single person entering, when logically the risk posed to a facility by a senior level employee or even a longtime season ticket holder is significantly less than that posed by an unknown person visiting a venue for the first time.

PURPOSE OF PHYSICAL SECURITY SCREENING

The primary focus of physical security screening should be to identify the presence of dangerous items, such as firearms and explosive devices. A secondary purpose should be to serve as a deterrent to a potential terrorist or adversary. Magnetometers (either walk-through metal detectors or hand-held metal detectors) are the traditional devices used to identify metallic objects/weapons. In general, walkthrough devices are preferred by law enforcement and security experts as they provide a more consistent and usually more comprehensive screening capability than hand-held metal detectors, which require a screener to physically move the hand-held detector over the entire body of the person being screened. While some may argue that hand-held metal detectors can be as effective as walk-through metal detectors, their effectiveness is dependent on the skill and endurance of the operator, who must take the time to ensure the screening covers the entire body. Since walk-through metal detectors screen the entire person at once they offer the advantage of higher throughput rates and more thoroughness than can be attained screening patrons with handheld metal detectors or through "pat down" searches.

A comprehensive security strategy screens not only the individual, but also performs a close examination of any bags the individual is carrying. It is essential that staff are well-trained to visually inspect the contents and structure of the bag to be able to recognize and identify explosive devices and their components (explosive material, batteries, wires, etc.) as well as weapons. The employment of screening systems coupled with inspection of personal items/bags form part of a comprehensive security strategy to reduce harm and save lives, but also can contribute to limiting the potential liability of a venue operator in the event of an incident.

EXPLOSIVE DETECTION TECHNOLOGIES

The use of metal detectors to screen people, coupled with bag screening, provides a robust security screening strategy with a high likelihood of detecting any weapons that may be brought to a venue, and provides a sense of safety to the patron that security is being addressed. With a rise in the use of improvised explosive devices, some venues may choose to also consider explosive detection technologies. A cost benefit analysis should be completed to determine whether the extra costs for deployment and the additional time it takes for traditional methods during the screening process are worthwhile. Traditional explosive detection technologies include:

Explosive Trace Detection

Commonly used in airport screening where a person or item is swabbed, and that swab is then scanned for trace amounts of explosives. It is a reasonable approach, but the equipment is relatively expensive to procure and maintain, the process significantly slows down the screening process, and if the explosive device is thoroughly cleaned and carefully handled the swab may not collect any trace explosive.

Explosive Detection Dogs (K-9)

For many experts, K-9s are considered the gold standard of explosive detection and the province of the military, law enforcement and homeland security. In recent years there has been significant growth in the availability and use of private K-9 teams, especially around sports stadiums. K-9s are best used to ensure an area is clear of explosives or to screen a line of people relatively quickly. While K-9s provide a good capability, well-trained certified teams are relatively expensive, there are significant constraints regarding how long they can screen at a time, and their stamina and effectiveness can degrade as ambient temperatures increase. They are best in mobile applications versus standing at a checkpoint trying to screen everyone who arrives. When used properly, K-9s provide an excellent capability to screen people, their packages, and vehicles, as well as provide a sense of safety for most patrons. It is important to note, however, that K-9s are not permissible in some cultures.

X-ray Machines

X-ray machines have long been used to screen packages and baggage at airports for explosives. They are relatively expensive to operate, require well-trained operators who can identify the presence of explosives in an x-ray image of a package, and can significantly slow the screening process. They are useful in that they can detect both explosive devices (with metallic components) and weapons and can be a useful addition to the security system for high-risk facilities that have highly trained staff and do not need high throughput.

The type of explosive detection technology used should be focused on the primary threat to the facility. In airport screening operations, X-ray machines are used where it's necessary that the threat has metallic components to be detected, even though the most significant threat is now from non-metallic IEDs. For example, see the results of the FBI's testing of the Christmas Day 2009 "underwear bomb" in the following 15 second video.
https://www.youtube.com/watch?v=tumVKQKab-s

An X-ray machine with a well-trained operator has the potential to detect a threat as small as that in the video, assuming it has metallic components. For public venues, the explosive threat is likely to be much larger in size, with the intention of causing a mass casualty event from the explosion. This larger threat increases the number of viable detection options.

Integrating explosive detection into primary screening for all patrons is typically an expensive endeavor. Detection technology and/or K-9s are expensive to procure and maintain and can significantly slow throughput of a screening system. That said, explosive detection systems can be useful and relatively cost-effective if deployed as part of a random screening program that is implemented as part of regular operations or when intelligence indicates a heightened risk to the venue.

SCREENING CHECKPOINT DESIGN CONSIDERATIONS

The primary considerations when designing a security checkpoint include ensuring that effective security screening can take place and that patrons, once screened, cannot acquire banned objects or materials and carry them into the venue. After provisions of effective security, an important consideration for any screening operation is throughput. A number of variables affect throughput, with some able to be controlled by a venue and some beyond a venue's control. Variables include but are not limited to:

- Number of screening stations and layout of screening stations
- Number and experience of staff
- Experience of patrons with screening operations
- Number of patrons and time of arrival for entry
- Number and type of items patrons carry with them
- Effectiveness of patron outreach communications
- Sensitivity of screening systems
- Process to resolve screening alarms
- Divestiture procedures

Generally, screening of bags will take longer than people moving through a walk-through screening system such as a metal detector or an Evolv Edge multi-threat screening system, so the checkpoint should be sized to support at least one bag screening table for peak operations. Furthermore, it is important to have positive control of patrons and their bags during the screening process to ensure that prohibited items cannot be passed to another patron after the screening is conducted.

As the screening system is being designed, the threats that the system targets for detection play a critical role in determining which human resources, equipment, and procedures are deployed. Metal detectors only detect metallic weapons. To reliably detect a non-metallic explosive device, use of an advanced system like the Evolv Edge or deployment of a separate explosive detection capability such as an Explosive Trace Detection system or K-9 team provides the most reliable results.

The other consideration is determining the required screening throughput each station should achieve to efficiently handle the expected crowds. The equipment used, the threats to be detected, the sensitivity levels of the equipment, and the divestiture procedures all have significant impact on the throughput levels. As advanced capabilities like those found in the Evolv Edge—which integrates both metallic and non-metallic weapon and explosive detection in a walk-through system—become more prevalent, major event and sports venues should consider migrating to this approach. This integrated approach addresses multiple threats, enhances security, improves patron experience, potentially decreases human resources, and maintains or increases throughput.

SECURITY SCREENING LAYOUT DESIGN CONSIDERATIONS

When developing an implementation plan for security screening the key factors that must be considered are required throughput, space available for screening, and budget. It is essential that each venue has accurate data to determine the expected throughput of each entrance so that security checkpoints can be adequately sized and staffed to efficiently screen patrons as well as avoid long queues.

As staff and patrons will become more experienced and comfortable with screening procedures over time, venue operators should re-evaluate the screening layout and staffing requirements to ensure each entrance's staff and equipment are being used optimally and to assess whether any efficiencies can be gained.

Several additional considerations need to be taken into account when implementing a physical screening system:

- Location (indoor versus outdoor, power source)
- Available space to use for screening
- Crowd flow
- Budget
- Weather

If given the option, physical screening should be conducted in an area protected from the elements. This will provide maximum performance of the equipment from an operational standpoint and the lifespan of the equipment will be significantly longer. A protected screening location will also reduce patrons' anxiety if they are outside in inclement weather.

A best practice when establishing a screening station is to use visual cues such as signs and tape or other markers on the flooring to passively guide people to the appropriate stations and queuing areas without having to be instructed by staff. This guidance can help minimize confusion and maximize throughput.

RISK-BASED SECURITY

One lesson that has been learned over the years is that those security systems that implement a risk-based approach to screening have significantly higher acceptance and favorability by the public than those that don't provide any differentiation. A prominent example of this approach is the TSA PreCheck program. TSA PreCheck leverages a preliminary vetting process that separates "low risk" passengers from those who are unknown or may require additional screening. By extending the screening process beyond the airport, TSA has significantly increased the throughput of its PreCheck screening lines for passengers while mitigating risks and saving more than $500M per year in reduced staffing and equipment costs.

A risk-based approach involves trade-offs among security, access, usability, and cost in a way that provides several advantages. These include:

A balanced security system drawing on complementary and layered capabilities

Perfect security does not exist and the cost curve becomes quite steep if you struggle to achieve it. A methodological approach to using a risk-based security will evaluate system trade-offs in a way that optimizes the variables at any given time.

"Life cycle" focused

Comprehensive security requires a dynamic and adaptive approach to a diverse set of activities that take place across the system life cycle. It is important to take into account changes in the environment over time, and changes in the risk profile of different groups of people over time (employees, visitors, dignitaries).

Capability and competency based

While software- and hardware-based capabilities play an essential role in effective security solutions, there is an equal emphasis on organizational, managerial, and operational capabilities to provide the full spectrum of mitigations needed to minimize risk.

The design of a risk-based security system relies primarily on these components:

Threats

Understanding of what must be detected to protect people and facilities.

Vulnerabilities

Understanding the vectors that an attacker may exploit.

Vetting

To what extent is the "user" base of the system known or unknown, and able to communicate risk?

Identity Management

Assessing system confidence of a user's identity and then attaching a risk assessment to the user and his or her belongings.

Routing

The ability to move high risk, low risk, and unknown risk users through the appropriate security channels, which will differ based on type and level of risk.

Physical Screening

The process of using equipment to screen personnel and belongings.

A successful risk-based security approach is reliant on an enterprise approach that not only provides excellent technology to perform physical screening but also ensures that the personnel performing the screening are using the technology appropriately, that people presenting themselves for screening have already been vetted, and that the screening process is not unduly burdensome. There is no "silver bullet" or "cookie cutter" enterprise approach. What might work particularly well in office buildings and places of worship, where it is possible to learn more about the regular user, will be different than in public venues where the majority of people presenting themselves may be unknown, and thus may present a different threat.

Advanced screening technology not only provides superior screening capabilities but also improves the user experience. Biometric capabilities enable fast stand-off identification of known persons and a dynamic risk-based screening approach can tailor the screening system response to the risk of the person presented for screening. This approach ensures that effort and time isn't wasted on screening trusted persons who pose no risk, while also ensuring that the screening systems in place are on highest alert when unknown or high-risk individuals present themselves.

Evolv Edge has made advances possible in the field of personnel screening that provide high resolution and high refresh rate that meet or surpass the capability of the best screening machines deployed in today's sports, entertainment, and commercial venues.

Recognizing the natural tension between implementing security and creating an open, inviting user experience, it is necessary to develop scalable and flexible security approaches to: a) define and quantify a trade space that accounts for the employee and visitor experience; and b) compare and contrast cost and capability so the customer can make informed decisions about which security approach works best for the expected risk of the facility.

The challenge commercial entities have in implementing a risk-based program is two-fold. First, a "known patron" program must be established along with a quick way to validate membership in that program at the entry to the screening system of a facility. Second, a program must tailor the screening process to account for the different risk levels of different people going through the process. While these challenges need to be overcome, the benefits to implementing a risk-based screening program could be significant for a facility and create a much better experience for the most valuable repeat customers. A risk-based screening program can also improve overall brand perception of a facility by implementing "smart" security solutions. These solutions help make life easier while maintaining a level of safety, allowing faster throughput into a facility, and thereby mitigating the risk of long queues outside a facility. Overall security costs can potentially be decreased since people can be screened at a faster rate, requiring less security staff. Properly implemented, a risk-based approach accomplishes the following:

- Improved security effectiveness
- Increased operational efficiency
- Enhanced customer/patron experience
- Lower overall operational cost
- Better adaptability to evolving threats

TAILORED SECURITY SOLUTIONS — SPORTS AND ENTERTAINMENT

In today's world, the risks and threats to high-profile enterprises can shift rapidly, and an effective security system must evolve in real-time to counter shifts in adversary behaviors. Therefore, as a security program is developed, it is important to couple leading edge security approaches, technologies, policies, and procedures with customer expectations. This will enable an enterprise to maintain its culture and character. The goal is to create a secure complex with multiple layers of protection that:

- continuously reduce risk in a manner transparent to the user;
- adapt in real-time to a changing threat environment;
- create a frictionless entry process enhancing the customer experience; and
- result in a world-class facility and security capability.

The culture of a sports or entertainment complex and the environment the venue owners wish to project is in almost all instances one of openness and welcome. The focus as fans arrive should be on the game or the concert and not on the security process. At the same time, the process must be visible and visibly effective, so people feel welcome and safe, while serving as a deterrent to a bad actor. This dynamic is a constant challenge for a security system and is why many organizations are moving to a risk-based security approach that focuses screening where it's needed most, maintaining effectiveness of the system while significantly improving throughput and the experience of its customers.

Until recently, there have been limited commercially viable solutions that provide an integrated risk-based screening solution for commercial venues. The Evolv Edge is one such system with the technical capabilities to identify both non-metallic explosives and metallic weapons. The Edge system also has the capability to use a dynamic risk-based screening algorithm that tailors the screening process to the risk-level of an individual person. This personalized approach

creates a frictionless screening process for "known" patrons, significantly improving the speed and feel of their screening experience without sacrificing any of the protective feel a security system should provide. This capability holds the potential to change the expectations of the screening experience for the general public, similar to how TSA's PreCheck program changed the expectations of the frequent traveler.

An integrated approach that uses Edge to implement a risk-based screening approach could also be leveraged beyond physical screening to access control. Using the biometric recognition capabilities of the platform and leveraging the "known fan" database it could be expanded to not only contain information about the risk level of a person but also be integrated with the access control systems of a facility.

EDGE SCREENING PROCEDURES

When developing an implementation plan, it is important to recognize that each venue is different, with its own unique environment, whether physical or cultural, which will greatly impact how effective screening can be accomplished. As is said in the aviation industry, if you've seen one airport, you've seen one airport. The procedures presented here are meant to be a guide for implementing security and represent a best-case scenario where there is enough equipment to perform the screening, room to install the equipment, and staff to operate it. They should be viewed as a starting point for planning.

Operational procedures should be standardized at a venue allowing screeners to work at any screening station without the need to learn different pieces of equipment. The implementation and screening procedures for an Edge system will be relatively straightforward for any experienced security staff since the Edge footprint and procedures are similar to a standard walk-through metal detector.

There are some specific, tactical recommendations that will help improve the Edge screening experience. These include ensuring there is sufficient signage and instruction for the visitors being screened, sufficient tables if divestment of personal items is required, and protocols for ensuring visitors move through the system appropriately with visibility to their personal items, proper metering, and positive control if there is an alarm.

CONCLUSION

As the threats against our safety and security continue to evolve and become increasingly unpredictable, security systems must evolve with them. The traditional screening systems now in place are not always informed by the current threat, are a source of frustration for patrons due to long lines and inconvenience, and usually have no way of being quickly updated to account for a changing threat. Further, threats against our safety continue to grow, as does the variety of places where screening is desired.

While people want the safety that screening systems provide, they do not want to lose the culture, openness, and sense of welcome that make their venue, stadium, or house of worship special. Implementing a risk-based security program provides the best option and allows an organization to tailor a program that fits their culture, so they do not have to sacrifice what they represent for safety.

The Evolv Edge was designed and built to aid an organization's move toward a risk-based security approach and provide balanced detection across a range of threats. Its ability to dynamically tailor its screening algorithms to the risk level of the person, operate in an environment where limited divestment is required, and integrate seamlessly into existing checkpoint operations will increase security and enhance both screening throughput and overall customer experience.

ABOUT THE AUTHORS:

John S. Pistole

Former Director, United States Secret Service

John Pistole is the former administrator of the United States Transportation Security Administration (TSA) and a former deputy director of the Federal Bureau of Investigation. Since the World Trade Center and Pentagon attacks, Mr. Pistole has been involved in the formation of terrorism policies during the Bush and Obama administrations.

Under his leadership, the TSA was transformed into a risk-based, intelligence driven counterterrorism agency dedicated to protecting our transportation systems. Among Mr. Pistole's many accomplishments were design and delivery of TSA's Pre-Check program, which provides pre-screened trusted travelers with expedited passage through security at participating U.S. airports.

Today, Mr. Pistole is the fifth president of his alma mater, Anderson University in Anderson, Indiana.

Mark J. Sullivan

Former Director, United States Secret Service

Mark J. Sullivan was a federal law enforcement agent for nearly 35 years. Mr. Sullivan concluded his federal service as the Director of the United States Secret Service (USSS), beginning as an entry level field agent and ultimately serving in a variety of leadership roles in the organization for nearly 30 years.

Mr. Sullivan led high impact initiatives in criminal investigations and protective operations, strategic planning, threat assessment and risk management, human capital management, technology deployment, IT modernization and budget development and execution.

Today, Mr. Sullivan works with clients on a variety of domestic and international security issues including financial and intellectual property investigations, business due diligence, major event planning, security vulnerability assessments for sports venues, buildings and critical infrastructure, risk management consultation, and security training and executive protection.