nyrej EST 1989

The four elements used to control a visitor's access to a facility

October 09, 2009 - Owners Developers & Managers

Most entry control processes are designed primarily to identify and control access to those who normally inhabit a building - trusted tenant employees and building staff - who are issued credentials (a building pass or access control card) by the facility. Visitors to the facility don't have building-issued credential but building security needs assurance that it is acceptable to allow entry.

The term "acceptable" is subjective and depends greatly on the security level of the facility being visited but, although some may be omitted, let's discuss all of the four elements used to control a visitor's access to our facility: Verification of identity, validation of purpose, contraband screening, and access control.

Verification

"What is your name and do you have a government-issued credential with picture identification?" A driver's license is a commonly accepted identification credential; most states in the U.S. provide a machine-readable license that facilitates extracting the holder's data and some systems can verify that the document is not counterfeit and check watch-lists of undesirables. However, procedures need to address the individual who does not have a driver's license or even a picture identification. One facility's policy might be complete denial of access; anothers might be a requirement for the visitor's host come to the lobby and vouch for the person's identity.

Validation

The second task is to validate that the visitor has a legitimate need to be in the building. Typically this requires contact with the host company - someone who has the authority and responsibility to admit visitors. This may be as simple as phoning the visitor's host to verify an appointment or checking a list of pre-authorized visitors. A list is most useful where there are multiple visitors for a conference or for a training course, particularly if the host may not be locatable at a regular phone number - nothing is more frustrating than arriving a few minutes late for a meeting and knowing that the reason security cannot reach your host is because he/she is chairing the meeting in some unknown conference room!

Screening

Before 9/11 it was rare to see personnel or package screening in a commercial environment but, since then, many facilities have implemented some level of visitor checking - from a cursory look into hand-carried bags and briefcases to a full airport-style screening.

Access Control

Once the visitor has been verified, validated and/or screened they have earned a reasonable level of trust and can receive a building-issued credential - a visitor badge - which can double as an access control card permitting the visitor access to allowable areas or, for higher security levels, the badge can be used in concert with an authorized employee's card - modified two-man rule. The benefits include the maintenance of an audit-able record of visitor access - and the authorizing host. For simple applications a bar code can be printed on the visitor badge; for higher security environments, more sophisticated technology can be used: passive infrared (PIR) and radio-frequency identification (RFID) systems allow a visitor's tag/badge to be tracked within a building on a graphic display and can be paired with the host escort.

The Systems Approach

Most visitors, 99.99%, arrive for legitimate purposes and should be welcomed at the facility. Active participation of smartly presented security officers who are well trained in both equipment operation and people skills, and who show a keen interest in ensuring that any delay or inconvenience to the visitor is minimal, are the attributes that make the visitor feel at home and are most effective in detecting off-normal conditions and denial of access to the 0.01% of visitors who are intent on harm.

Automated Visitor Management Systems (VMS) are being implemented at corporate facilities, commercial office buildings (at both entry lobbies and loading docks) and gated residential communities. Modified versions are also applicable for visitors to school buildings.

Pre-Approval

The validation phase can start before the visitor arrives: the (authorized) host of the visitor uses a web browser to access the VMS web server (password controlled) and supplies information such as the visitor's name, affiliation, date, time and duration of visit, where in the facility the visitor will be permitted and if a host is needed. Pre-approval of visitors greatly reduces processing time and reduces the number of processing stations required. Typical processing time varies between 15 seconds and a minute, or more, depending on complexity and pre-approved status.

The Visitor Arrives

A standard government-issued credential, such as a driver license, is presented for verification of identity and its data automatically can be extracted by a driver license reader. Alternative data entry methods are keyboard entry (slow and error prone), business card scanner/reader or a passport scanner. The VMS software can validate the visit by checking that the individual is not on a "black list" and is expected (pre-authorized) at that date and time. If not pre-authorized, the processing staff can phone the host for validation or can require the visitor to phone the host and obtain pre-authorization. In a busy entry lobby, the latter procedure is becoming more prevalent since the responsibility for authorization is transferred from the administrative staff to the trusted host.

Taking and storing a photograph of each visitor is valuable as a deterrent and can be used to identify a visitor who becomes a suspect in a security incident. Printing the photo on a disposable badge to be worn by the visitor is of less value: given the quality of the camera and typical lobby lighting conditions, the print quality is, typically, poor and the photo of questionable use unless employees and security staff in the facility are trained to check the photo against the holder.

The Visitor's Badge

The system can automatically print the visitor's badge as soon as the identity is verified and the purpose for the visit validated. The design of the badge should include: visitor's name, affiliation, host's name, meeting location (e.g., floor/room number) and expiration date. A self-expiring sticker may be of added security and, if the badge is to be used in an automated access control system, a bar code can be printed on the badge.

Any process that requires peeling off a backing or peeling off on old label from a plastic badge is time consuming and creates waste. Card stock, pre-printed with standard building information, is probably best if longevity and bar code reading are issues.

The period of validity of a badge may be set at a single visit, multiple visits in one day, of multiple days for, say, a visitor who is attending a week-long training course. The quality of the badge should reflect its expected duration. Another factor to plan for is disposal: a badge dropped in a garbage can outside the building should not permit entry by a dumpster diver.

Access Control

As soon as the visitor badge is produced, the badge identification number (e.g., bar code) and the expiration data can be transmitted to the access control system so that elevator bank turnstile readers, or other control devices, can accept the visitor's badge and control passage within the facility.

Kiosks

The VMS process is ideal for automation, if the visitor is pre-authorized and has a machine-readable government-issued credential. ATMs and boarding pass kiosks have trained us well. The self-processing procedure is very quick and cost payback period for a kiosk, compared to the cost of staff, can be short; however, most complex situations - e.g., a group of visitors, a visitor who has not been pre-authorized, or one without uniform credential - still requires staff assistance.

David Aggleton, CPP, CSC, is the president and principal consultant at Aggleton & Associates, Inc., New York, N.Y.