Best Practices to Manage Access for Temporary and Contract Workers

By Cindy H. Dubin, Contributing Editor

Against all odds, a pair of White House party crashers in November 2009 made their way effortlessly into a state dinner hosted by the President. By all accounts, this breach in security came down to negligence on the part of the Secret Service, the Social Office and security guards. When questioned by reporters, Valerie Jarrett, senior adviser and assistant to the President on Intergovernmental Affairs and Public Engagement, said the event "exposed significant security gaps" and that "the security system should have been more diligent." But, just two weeks later, a couple expecting to take a White House tour was mistakenly ushered into a Veterans breakfast with the Obama's. Questions arose following the event as to whether security personnel did their job screening the couple before granting them access.

"If you can get into the White House, you can breach access anywhere," says John Sileo, corporate director of security for Freeman, about the situation.

Controlling breaches in security by outsiders can be a risky business. In August 2009, International Data Corporation (IDC) revealed the results of its survey of 400 high-level managers in the United States, United Kingdom, France and Germany. The surveyed organizations said contractors and temporary staff represented the greatest risk to their companies. "Any time you bring in someone from the outside, you have risks," notes Kevin Newcomer, corporate loss prevention manager for Ace Hardware Corp., which usually has 150 to 200 outside employees at its Oak Brook, Ill. site at any given time.

The economic downturn has played a role in the number of temporary and contract workers companies are using today. After several months of decline in the number of temporary employees in the U.S. workforce, the figure hit a yearly low in July 2009 at 1.7 million. Since then, the number has risen, hitting an estimated 1.9 million in December on a seasonally adjusted basis, according to the U.S. Bureau of Labor Statistics.

There are signs that employers are reconsidering their hiring strategy as the economy turns around. According to the *Employment Dynamics and Growth Expectations Report*, compiled by Robert Half and CareerBuilder, 40 percent of companies say they plan to hire contract, temporary or project workers in the next year.

SECURITY POLICIES THAT WORK

No matter how many outside employees a company hires, security managers agree that access control is vital. For some, restricting access has always been part of their corporate culture. For others, current world events dictate tighter restrictions. Here, three companies share their security policies for managing how much access is given to temporary and contract personnel.

1. Establish a dedicated vetting process for outside employees. According to a 2009 report from Forrester Research, *Identity And Access Management Mitigates Risks During Economic Uncertainty–Using Identity And Access Management To Protect Your Business*, many enterprises do not have dedicated controls in place for temporary workers because of the misguided belief that short-term workers "don't have enough time" to be dangerous.

At Ace Hardware, all employees are vetted and their backgrounds screened before they even enter the front door, explains Newcomer. "We perform the same level of screening for full-time employers that we do for contractors. It doesn't make sense not to take that preemptive step."

Eric D. Zuck, chief of security for Sand Expo Convention Center in Las Vegas, says he wishes he and his team had more control over the vetting process. "We have had felons sent to us who were wanted by the police."

2. Educate outside help about the corporate security culture. The IDC report points out that security training for contractors is often limited, and company security policy is not always clearly communicated to temporary workers. At Freeman, a Dallas/Fort Worth provider of services for exhibits and meetings, all employees – full time and contractors – must participate in a security training program, which outlines the company's policies for physical access management, explains Sileo. This is an essential to Freeman because it hires outside personnel to work on site at its warehouse facility as well as off site at various convention centers. "Anyone working for Freeman clearly understands our security culture once they go through the training program."

3. Clearly define access points. Temporary employees should only have access to those systems that are required to perform their job function. Supplying blanket access based on full time employees' roles can introduce unnecessary risk, states the Forrester report.

On the first day of work, Newcomer and his team help all employees understand the Ace corporate security culture by defining access policies and how much access is required to perform various jobs. "At Ace, no one has access to everything," says Newcomer. He explains that a temporary or contract worker and a full-time employee performing the same job function will enjoy the same access privileges. "If the job doesn't require 24-hour access to the building for their specific job function, then don't give it to them."

And, the security pros note that procedures should be in place to turn on and turn off access as efficiently as possible. As contract employee turnover rates tend to be higher than that of full-time employees, temporary workers need to be provisioned and deprovisioned quickly. This ensures that no gap exists between the official departure date and the time when access is shut off, according to the Forrester report.

4. Deploy a combination of preventive controls. Identity and Access Management (IAM) solutions help monitor and enforce security policies and verify that a worker's activity aligns with their job function.

Contract workers at Sands wear picture identification badges identifying them as temporary workers, and temp employees must wear a sticker that visibly identifies them. Old-fashioned keys and card keys, and security cameras are also deployed. "I would like us to use biometric assess and wireless cameras that would cover more areas in the conference center," says Zuck. Currently, cameras are in certain areas of the convention center, but not specifically on the show room floor, which Zuck says leaves the space vulnerable to theft by the temporary workers. To offset that threat, those employees are overseen by supervisors who follow the workers as they perform their duties.

At Ace, outside workers are expected to wear an ID badge and keep it exposed at all times. Additionally, a card access system is deployed that monitors employee access. Newcomer said he receives exception reports from the system that let him know if someone tried to access an area that did not have authority to do so. "Often, the person was just trying to find a short cut or got lost, but we have to follow up on all incidences."

In addition to color-coded identification badges, Freeman has designated entry and exit doors as a means for controlling access on site. "This gives us a better idea of who is clocking in and who has left," says Mike Feliciano, regional director of risk management for the company. "Once someone goes through an exit door, they cannot get back in to the building." The company is also researching how closed-circuit cameras and biometrics can be used for improved access control.

5. Establish a relationship with the temp agency. Security pros agree that one of the best ways to be confident in who is walking through their doors is by creating and maintaining a long-term partnership with the temp agency. By doing this, the agency gets to know your company, its requirements, its culture and the type of person that would best fit in at the organization.

Sands has taken this approach with its agency. Zuck explains that the agency will often send employees who have been at Sands before, which not only helps reduce training time upon arrival but lightens the stress level a bit for the security team that the person has been on the premises before and has not been any trouble.

For Ace Hardware, which hires outside help to perform specific projects, it is important that the agency sends over a committed worker. "We don't want a revolving door," says Newcomer. "We want the same person we get at the outset to be the same person throughout the process. We can help assure this by maintaining a relationship with our provider." SECURITY

Badging Security – Four Levels to Secure Your Facility

There are a number of badging solutions that provide varying levels of security depending on the size of the location, frequency and number of visitors, and/or temporary workers. To help identify the solution most appropriate for a specific application/venue, here are four levels of badging security.

Level One – Paper Label Badges

This system employs standard paper badges (basically labels) and delivers a minimum level of security. Badges can be issued either manually or electronically and can usually be customized with color and graphics depending on your print output capabilities. Paper label badges are generally intended for one-time use only and often used simply as name tags.

Level Two – Paper Label Badges with Color Photos

Badges with photo identification scanned from driver's licenses or captured via an on-site camera system offer a medium level of security. To further help identify visitors and temporary workers, these badges may also contain additional use of color, symbols and words.

Level Three – Electronic Badges

Included in this category are proximity, magnetic strip and bar code badges, as well as those containing biometric information. These semi-intelligent badges can be programmed for pre-determined levels of access and can be integrated with access control and video surveillance systems to electronically monitor activity. They offer a high level of security and system integration but do not offer any form of visual status indication.

Level Four – Time Expiring Badges

This technology delivers instant verification of security status plus all of the above solutions and benefits. Time expiring badges and indicators can be added to existing smart cards to provide instant visual verification of visitor status. Time expiring badges prohibit the unauthorized transfer and/or re-use of the expiring badge providing an elevated level of security. They are also extremely efficient with respect to both cost and manpower since they reduce the use of expendables and eliminate redundant registrations for recurring visitors.

Information provided by Brady Identification Solutions