

## Tackling the Issue of Employee Identity

September 23, 2011

By Lin Gensing-Pophal

***While no one wants to think that their organization's security can be breached, incidents do occur. And since it happens so rarely, even the best policies and procedures can be forgotten if HR fails to regularly train and communicate on the issue.***

There's a charming, albeit likely apocryphal, story about Steven Spielberg sneaking onto the Universal lot as a teenager and setting up shop in a vacant office. "Every day, for three months in a row, I walked through the gates dressed in a sincere black suit and carrying a briefcase," Spielberg said in a 1969 interview with the *Hollywood Reporter*.

Charming!

Not so charming, however, when 17-year-old Matthew Scheidt of Osceola, Fla., impersonated a physician's assistant for five days at a hospital in central Florida. Scheidt now faces felony charges for spending time in the OR and emergency room, conducting exams, providing patient care and accessing restricted patient information.

How did it happen? He gave two different stories to two separate HR staff members, yet ultimately managed to secure a badge with his name and photo, stating he was a physician's assistant, giving him access to areas of the hospital -- and patients -- to which he should have had no access, police said.

Could this happen in your organization?

Chances are, to some degree, it already has.

According to the Association of Certified Fraud Examiners, U.S. organizations lose more than \$660 billion annually to fraud and abuse. Further, they say:

- \* More than 85 percent of all resumes contain errors, omissions and false statements

- \* 60 percent of college registrars regularly experience attempts to document false credentials

- \* 45 percent of potential employees have a criminal record, bad driving record, workers' compensation claim or bad credit history

Whether you're an HR professional in a hospital, a movie studio or a retail store, breaches of security can be a big deal.

### **Types of Security Breaches**

The types of breaches organizations face can range from the relatively benign (exaggerating credentials on a resume) to the extreme, as seen in the recent Florida situation, says Anthony Roman, owner of Roman & Associates, a global security, investigation and management firm located in Lynbrook, N.Y.

While criminal impersonation is much less common than lying about credentials, it is not all that rare, he says. While some individuals take such a route because of mental illness, others do so for economic enrichment, says Roman.

While many HR professionals are likely aware of the role that they should play in guarding against these types of incidents, not all take it seriously enough, says Chuck Papageorgiou, chairman and CEO of International Screen Solutions Inc. in Kennesaw, Ga.

"There are two types of HR managers when it comes to security and background checks," he says. "Those that actually believe it's a critical part of the job and those who just want to check a box and move on."

In an environment where these types of situations are on the upswing, he says, the second approach simply doesn't work -- and HR must take the lead in responding proactively to security issues.

But, he notes, security needs to be part of everybody's job.

### **The Importance of Being Proactive**

Sarah Cullins, president of Finesse Staffing of Rancho Cucamonga, Calif., advises HR managers to work with senior leaders to identify areas of potential security risk.

"It varies by company," she says. "For one company, the personnel files may be the main security issue; in another, it may be trade secrets."

HR does not stand alone here, says Roman. Issues of security cross many organizational lines, involving legal, insurance, public

relations, information security and compliance, both internally and externally.

Effective security measures involve establishing policies and procedures, training and educating managers and staff about those policies and procedures, and creating a culture where employees are driven to actually follow the procedures.

Too often, says Joe Gagnon, who is of counsel in the Houston office of Fisher & Phillips, organizations develop plans and policies, but neglect the critical training and communication that should come next -- and continue as an ongoing process.

### **Maintaining Awareness**

Gagnon tells of a Texas case he recently worked on involving a former employee who made threats to co-workers before and after termination, including statements such as: "I have my guns and it won't be long now before I come back."

Yet, shockingly, says Gagnon: "In some cases, the staff who received the calls never bothered to let management know."

Of particular concern at this organization was that nobody knew whether the employee's identification badge was taken when he was terminated, Gagnon says.

"Risk management, security and HR can not let their guard down," he says.

Organizations need to generate constant reminders to management and staff, and provide drills to provide both ongoing reminders and experiences in responding to various types of threats.

Staff need to know not only about observing and identifying risks, but what to do if they see or hear something of concern, Gagnon

says. Who do they inform? What is the process for sharing this information?

Since, in most organizations, these incidents are not exceedingly common, over time it can be easy for employees to let their guard down.

No-exception cultures, while they may create some inefficiencies, "can also really help to secure a workplace," says Gagnon. "So, if a CEO comes in and says: 'I lost my badge and I need a new one, that CEO should be expected to go through the same series of protocols as any lower-level employee.'"

Importantly, the organization must stand behind employees who follow the required protocols and not berate, hassle or demand exceptions.

### **Responding to Security Incidents**

If security breaches or incidents arise, Cullins says, HR should investigate in the same manner they would any other employee issue or infraction.

"You need to investigate the cause and effect of what happened," she says.

This involves investigating process as well as people. Is this a case of an employee failing to follow a guideline or policy? Or, did the process break down at some point, requiring a process improvement of some kind?

Disciplinary action may sometimes be advised, up to and including termination, depending on the specifics of the incident and the employee's performance record.

"I counsel disciplinary action and not necessarily termination," says Gagnon,

"especially if dealing with someone where there's a breakdown for the first time."

While security -- of employees, patients, customers, vendors or the public -- should always be an organization's first concern when it comes to security, says Gagnon, liability needs to be a concern as well.

The bottom line for organizations is that security needs to be considered the responsibility of everyone in the organization, potential threats should be identified and addressed through policies and education, communication should be ongoing, and HR and other organizational leaders should respond immediately and consistently to issues that arise.

Although Universal Studios doesn't seem to mind being part of Steven Spielberg's story, the Osceola Regional Medical Center -- and probably your organization -- would likely rather stay out of the limelight.