

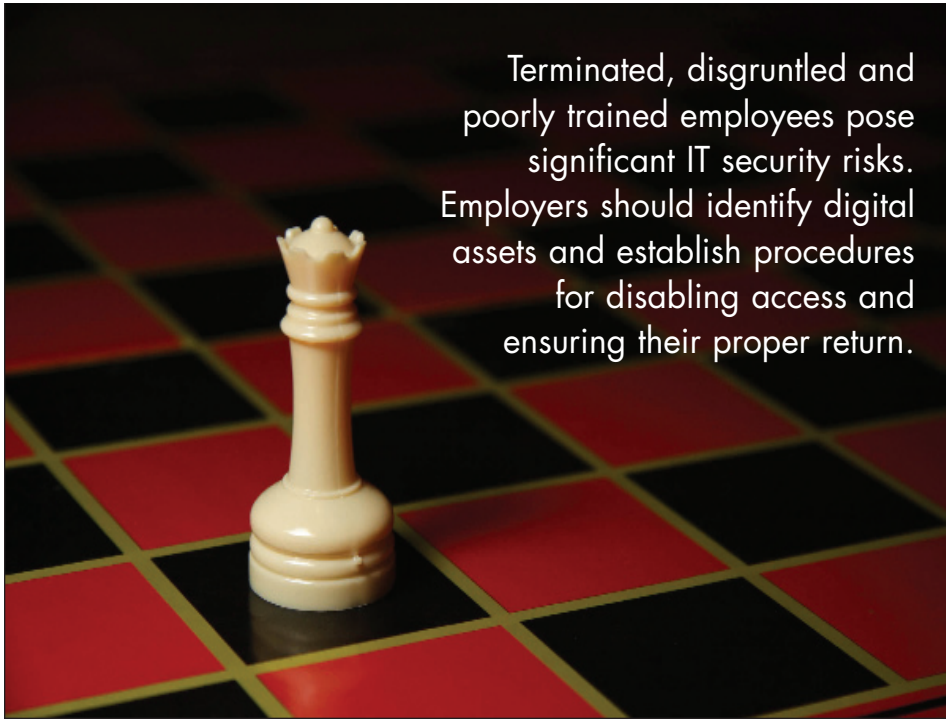
# St. Louis Technology News

**THE TECHNOLOGY SPIRIT OF ST. LOUIS™**



TECHNOLOGY SOLUTIONS AND STRATEGIES FROM ISPIRIAN, SYLLOGISTEKS® AND ULTRATECH

## END-GAME STRATEGY



Terminated, disgruntled and poorly trained employees pose significant IT security risks. Employers should identify digital assets and establish procedures for disabling access and ensuring their proper return.

**M**any people have trouble thinking about the “end game” at the beginning of a relationship. However, things can (and do) turn sour, particularly in an employment relationship. It’s important for employers to consider the possibility of an intentional or inadvertent security breach at any phase of an employee’s relationship with the organization.

“Employers simply must develop IT asset security procedures for preemptive data preservation,” said Tom Smith, CEO of Ispirian, Inc. “The starting point in preparedness for employment exit begins at the beginning of employment and runs continuously from there. The best procedures include pre-contemplated steps that are prioritized and triggered much like triage in an ER. These are usually classified as ‘anticipated’ and ‘unanticipated’ departures. The timing and urgency of executing the steps varies accordingly.”

Unfortunately, processes surrounding “unanticipated” departures become even more critical in difficult economic times. If layoffs are anticipated, an employer should immediately begin IT asset security procedures. Even

*continued on page 2*

St. Louis Technology News

PRSR STD  
U.S. POSTAGE  
PAID  
Tulsa, OK  
Permit No. 2146

# End-Game Strategy

continued from p. 1 ...

if layoffs can be avoided, low morale and pay cuts can increase the risk that a disgruntled or inadequately trained employee could pose a security threat.

“Organizations should be concerned about internal security breaches due to lower employee morale,” Smith said. “Deloitte Touche Tohmatsu recently surveyed senior security officers from the world’s top global financial institutions. More than a third expressed concern about insider misconduct, compared to only 13 percent who said they are concerned about external threats. Furthermore, six in 10 survey participants said they are concerned about their ability to protect their organization from internal cyber-attacks. Clearly, organizations need to take additional steps to prepare for these very real threats.”

## Who, What, Where

Smith says the first step is to identify what digital assets are or have been under the control of each individual in order to ensure that access is terminated. Most large organizations have formal processes for granting and terminating access credentials, but many small to midsize organizations do not. Furthermore, smaller and downsized organizations often require functional overlap that makes it even more challenging to prevent unauthorized access.

“It’s not just a matter of terminating an employee’s network access and e-mail account. You have to consider every credential that employee might have been privy to,” said Smith. “For example, the accounts receivable clerk might have been tasked with ensuring that backups ran properly each night, and as a result have administrator credentials for your primary accounting server. You don’t want to think that this individual might log in from home and wreak havoc with your accounting data, but it could happen.”

More critical — and difficult — is identifying which digital assets are or have been in the possession of each individual in order to ensure that these assets are properly returned. Did an employee copy sensitive customer data to a thumb drive? Did she e-mail copies of internal reports and memos to her home account? Did she log in to the network remotely and download important files?

“These activities happen all the time, particularly given the proliferation of mobile media such as USB keys, MP3 players and PDAs. Most of the time, the motives are innocent, even noble — a dedicated worker trying to get work done in the evening or over the

weekend. But innocent or not, these activities pose a security risk. Each digital asset should be accounted for when the employee is terminated, whether voluntarily or not,” said Smith.

## A Bit of Detective Work

It may be appropriate to engage an attorney to craft employment policies designed to protect digital assets without running the risk of litigation for invasion of privacy. A digital forensic investigator should also be engaged to help ascertain what digital assets may have been compromised and to preserve evidentiary data. He or she can also ensure that digital assets are detected and properly removed.

“Some organizations have developed policies that require employees to agree that their home computers are fair game for image collection at any time during employment and for a limited number of days post-employment in exchange for the privilege of using them to access corporate networks,” Smith said. “It’s also important to determine which devices would be targeted for forensic imaging and archiving before assets are redeployed to others.”

Security attacks that exploit human error and breaches caused by distracted or disgruntled employees may be the root cause of information security failures in coming months. While people are an organization’s greatest asset, they are also its weakest link, particularly in hard economic times when job insecurity and increased stress levels may lead employees to behave in atypical ways.

“Many organizations are well aware of physical security safeguards — such as not allowing a former employee to have access to areas only open to employees — but digital security is too often an afterthought,” said Smith. “How many times do we hear about the ex-employee’s breach enabled by a still-active user account months after termination? It may not be pleasant to think about an employee’s termination when you’re preparing his new-hire paperwork. However, that’s an essential consideration, particularly in today’s economy. Employers must establish processes to protect digital assets throughout the employment lifecycle.”

---

**Eight-six percent of respondents to a recent Deloitte Touche Tohmatsu survey say that human error is the leading cause of information systems failure, and they fear more breaches due in part to employees who are distracted or disgruntled because of job insecurity and increased stress.**