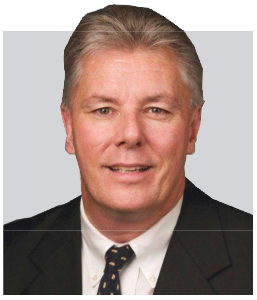
IT Intelligence

INTEGRATING ENTERPRISE ACCESS AND HR PLATFORMS

by Bob Stockwell



Bob Stockwell is Global Technology Leader for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

Editor's Note: SSI *is pleased to introduce this new column covering network security and featuring STANLEY Security's Bob Stockwell.*

The advantages of integrating an enterprise access control (EAC) system with a customer's human resources platform are enormous. Through critical integration of both systems, HR administrators are able to deliver real-time information updates to the security platform, and can thus more readily grant access to new hires and cancel access when required.

Global enterprise deployments can easily exceed 200,000 cardholders that must be managed, so this synchronization of information becomes crucial for accurate reporting and ensuring that all and only authorized personnel are allowed access to a customer's facilities. In order to achieve this level of communication between EAC and HR platforms, third-party active software program links are the common interface software being deployed.

Let's look at common challenges when attempting to integrate HR and EAC. Awareness of these challenges can promote proactive, strong communication between a client's HR department, IT personnel and the security integrator, thus resolving these issues to provide an effectively integrated HR and EAC solution.

A perception exists in the security and IT industries that integrators lack the expertise to manage and deploy an interface to integrate both HR and enterprise security platforms. In reality, most integrators don't have staff members that possess the same, applicable credentials as a client's internal IT personnel. Because of this, integrators are often "locked out" by customer IT teams, concerned with data conduits to "foreign systems" that could potentially bring down the entire revenue production cycle.

That being said, communication between each of these parties is key, and there is often the issue of being able to successfully coordinate all stakeholders together from HR, IT and security in order to define clear business rules of operation. With bidirectional capability, stakeholders may require multiple data conduits to link security access systems beyond the firewall, both internally and externally. Thus, isolated servers operating on more than one subnet can be disconnected and without notification will not receive updates — an occurrence that could result in catastrophic results. For integrators, a vital step in the successful deployment of an EAC security system and human capital management software heavily relies on working closely with and obtaining the approval of customer IT personnel.

When linking both the EAC solution and HR database, difficulties arise in effectively matching users' input in one system to their corresponding identity in the other. Often there is not a unique identifier (i.e. an employee ID number) in both systems to easily allow for users to be positively matched across the two systems. In large-scale businesses, it is also not uncommon to have individuals with the same first and last name and no other data available to differentiate them. In these situations, it's critical for clients to establish structure throughout the business in order to create specific identifiers commonplace throughout both platforms.

Linking these systems, while ultimately incredibly beneficial, also opens clients up to the possibility of dealing with incompatible or corrupt data. During the transition, information may have been incorrectly entered due to user error or not updated as needed (i.e. department and organizational changes, or including information for someone who is no longer with the company). There needs to be a process for validating or eliminating questionable data. Clients often operate multiple access control manufacturers and require each equipment type to integrate with multiple HR platforms.

For integrators, a vital step in the successful deployment of an enterprise access control security system and human capital management software heavily relies on working closely with and obtaining the approval of customer IT personnel.

Clients must find a source of ongoing support to maintain the active software link between both systems. Even after the interface is up and running, any changes to either the HR system or the access control system network configuration may require changes to the interface between the affected applications. Unanticipated data or changes in procedures may also require updates to the interface and implemented business rules. Integrators can assist in this process by partnering with internal IT resources at the internal level to create a single standard of support across both platforms for future growth and expansion requirements. ■