Do You Have a Gaming Identity?

By Jon Greene

Few industries have seen the explosive growth in employment and revenues experienced by the Native American gaming industry. Fewer still are as dependent on information technology infrastructure (IT) for the delivery of positive customer and employee experiences. This makes automating identity management (IdM) — the processes for creating, maintaining, and deleting user IDs, passwords and privileges — essential to a successful gaming enterprise.

Because of their relatively recent emergence as market leaders, Native American casinos, particularly Class III sites, have some of the most advanced IT infrastructures in the gaming industry. From day one, many have implemented computerized systems for not just financial management, but the management of human resources, gaming, retail, and hospitality operations and facilities. Every level of staff, from senior management utilizing analysis tools to track business performance to the housekeeping staff managing cleaning and maintenance tasks, is dependent on IT. Without efficient and secure automation of user access, business performance, customer service and employee satisfaction will suffer.

Identity management consists of the following functions:

- **User Provisioning** — The process of requesting, approving, and assigning user credentials, access rights and assets (employee on-boarding)
- **Password Management** — Processes for managing user passwords including self-service reset, policy enforcement and synchronization
- **User Deprovisioning** — The process of terminating user access rights upon termination (off-boarding)

The result is a comprehensive user lifecycle management system in which the HR system drives creation of all necessary accounts when an employee is hired; self-service user access request and password reset functionality ensures that the user's credentials and access are kept up-to-date; and HR-driven termination removes or disables access privileges when the employee leaves the organization.

The Business Benefits of Identity Management

Business drivers for automated identity management include: cost savings, enhanced operational efficiency, risk management, and compliance with internal and external regulatory requirements.

Cost savings — IT departments spend a major portion of their budget addressing identity management issues. Studies from major analyst firms indicate that password reset calls

alone account for 30 percent to 50 percent of help desk inquiries. At $10 to $30 per call, enabling users to solve their own problem via self-service password reset can pay for itself in well under 12 months. Similarly, replacing a manual provisioning system that utilizes costly and scarce administrator resources to create and manage accounts will generate immediate savings.

Operational Efficiency — Manual provisioning systems can take weeks to complete all of the necessary approval and administrative steps for on-boarding a new hire, and a similar amount of time to complete a promotion, transfer, leave of absence or termination. These delays reduce productivity and negatively impact user satisfaction.

Risk Management — Unauthorized access to critical casino and customer data presents major financial security, legal and public relations exposure. Identity management enforces access based on organizational policies, and provides the reporting and auditing tools required to assess risk.

Compliance — Even though Native American casinos are not limited by the state gaming regulations that govern their commercial counterparts, they may need to comply with NIGC regulations and must enforce strong internal controls as a matter of sound business practice. Whether it's providing an audit trail that illustrates what access was granted to an employee and who approved it, or ensuring that terminated employees have all of their access removed or disabled within a predetermined time period, effective identity management provides the control and transparency to meet organizational requirements. These may also include separation of duties (SoD) enforcement, which ensures that potentially dangerous combinations of rights — the classic example being the ability to authorize and disburse payments — are not issued to a single employee.

The Keys to Successful Identity Management Deployment

Some casinos have already reaped the cost, efficiency, security and compliance rewards from automating identity management. Along the way they've learned that a little advance planning and attention to a few principles greatly increases the likelihood of success.

Advance Planning — Identifying key business goals, limitations (budget, time or resources) and priorities will lead to a much smoother implementation. Consider a phased approach that delivers immediate business value while providing time for design and implementation of more complex portions of the project. For instance, initial implementation of self-service password reset can lower costs, reduce calls to the help desk and test out the identity management infrastructure. Then you can tighten password policies (length, complexity, frequency of change, etc.) without overburdening the help desk and add provisioning/deprovisioning as subsequent steps. Also consider rolling out to the highest priority groups first, such as those with high turnover that present the greatest administrative burden or those handling valuable assets that represent the greatest security and compliance risks.

Simplification — Start with what you know. Access rights and approval processes are generally assigned based on roles. If you've already built a comprehensive role model and corresponding approval workflow, then by all means go ahead and implement them in your identity management automation solution. However, even if you've only defined simple roles such as "Management," "Staff" and "Contractor," they can be the starting point for rapid deployment. Make sure your provisioning system will permit you to request additional access privileges and define approval workflow without complex programming or consulting services. Then you can go back and create more complex roles (e.g., Front Desk Staff, Front Desk Manager, Accounts Payable Clerk, etc.) based on actual usage patterns. You should even be able to select an existing holder of each role to use as a template.

Infrastructure Support — Make sure your identity management vendor can support all (or at least most) of the critical applications that drive your business. Because many applications implement their own user ID, password and privilege model, special "connectors" may be required. These enable the identity management system to "talk" to each application and manipulate a user's credentials and access rights. The vendor should offer an advanced architecture that simplifies creation and deployment of connectors as new applications are added to the gaming infrastructure. If, on the other hand, the answer is "we'll send out a programmer," then you may experience significant cost or delay during deployment or ongoing maintenance.

Gaming Knowledge — Your IdM vendor and their integration partners should understand the gaming business. Look for experience deploying in similar environments and recognition of the types of applications, roles and regulations that drive your business. They should have partnerships (or at least a willingness to partner) with your critical application vendors — including human resources and licensing applications, financial applications, gaming management applications, etc. Knowledge of the industry will also enable them to meet your reporting and auditing requirements.

Proof of Concept — While some identity management functions, such as password management, can be implemented without an onsite vendor PoC, a comprehensive roll-out including user provisioning and deprovisioning should be validated before acquisition. By focusing on your most critical applications and roles, the IdM vendor should be able to deliver a working proof of concept in just a matter of days.

Labor intensive, high-turnover industries like gaming are ideal candidates for automated identity management. In the high-growth, rapidly paced environment of Native American gaming, securely and efficiently automating the management of user identities is a "must have" to reduce costs, increase operational efficiency, manage risk and achieve regulatory compliance.

In his more than 20-year career, Jon Greene has established and grown product lines in such diverse market segments as network systems, storage management, security and network management. In his current role, Mr.Greene is responsible for the development and execution of marketing strategies for Avatier, a leading provider of identity management solutions.