

COMPLIANCE WEEK

THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

Case Study: ACS Conquers Identity Management

By Todd Neff — February 9, 2010

For Affiliated Computer Services, a Dallas-based IT and business-process outsourcing firm that does business in 100 countries, identity management had become not only a compliance concern by 2008—it was a business risk and productivity drain as well.

Many of ACS's 74,000 employees work in jobs known for high turnover, such as handling calls for major cellular carriers or doing document imaging and processing. Provisioning a new employee with proper system access took a full seven days, during which time the new arrivals were largely unproductive. And when new workers did finally get system access, they generally received broader rights than they needed.

"We have a lot of churn of employees," says Chris Leach, ACS's chief information security officer. "Because of that, keeping track of people's identities was really a big issue."



Then came the security risks. Terminating employees was an imperfect process for ACS in the middle of the 2000s, with time lags between physical and digital departures. And ACS grew largely by acquisition, meaning data centers, call centers, and business offices needed quick connectivity across multiple computing environments. The new additions tended to have their own security policies, and bringing new acquisitions into the ACS umbrella of control was a chore. It was, as Quoc Tong, ACS's director of identity and access management notes, "a huge concern."

But what finally prodded ACS to address its identity management problems, Leach says, were the compliance worries. ACS's client roster ran from government agencies and financial firms to healthcare providers and restaurant chains. That meant compliance with privacy regimes such as HIPAA or the Gramm-Leach Bliley, as well as ethics rules for good government contractors. Then there was the small matter of Sarbanes-Oxley compliance for ACS itself, which is a public company.

ACS had previously worked to address such challenges with one-off systems and software capable of synchronizing passwords and IDs across certain ACS computing environments. But even as recently as 2008, the company hadn't assembled an overarching identity-management strategy.



Over the course of that year, then, Leach developed an ID management strategy as part of a larger effort to consolidate IT security across the enterprise. His plan had three main principles. First, it had to simplify password and identity management across ACS's many IT environments.

Compliance Week can be found at <http://www.complianceweek.com>. Call (888) 519-9200 for more information.

Second, it had to give new employees fast access to the computing resources upon which their jobs depended—and revoke that access just as quickly when they left.

Third, regardless of whatever specific IT solution ACS might select, it could not be a costly “rip and replace” product, Leach says. It had to mesh well with all of ACS’s pre-existing systems. ACS had already deployed ID and password synchronization tools for some of its clients, “so it would be hard to go to Client X and say, ‘Guess what? We’re changing tactics midstream,’” Leach says. “They’d kill me.”

By late 2008, Leach, Tong, and colleagues had narrowed their list to five software companies: Hitachi, Oracle, Microsoft, RSA, and Novell, whose Compliance Management Platform came out on top. “With Novell I had an end-to-end solution—provisioning, workflow, everything was built in. So I have a single throat to choke if something breaks,” Leach explains.

Getting It Done

Implementation began in late 2008. Seven Novell consultants and 20 ACS employees (ranging from IT personnel to human resources, legal, and support staff, most of whom were part-time on the project) formed the core team that installed the system, Leach says.

The team’s cross-function diversity paid several dividends, he adds. First, the many viewpoints helped sharpen Novell’s understanding of exactly what the system had to deliver for various departments. But equally important, when ACS needed “a champion” to explain the need for better ID management to groups of employees, “it wasn’t just IT security geeks who were shouting,” Leach says. “It made the transition very smooth.”

Leach also appreciates Novell’s efforts to tailor its Compliance Management Platform to ACS’s various needs. Clients in healthcare, government, or banking, for example, all have different requirements, terminology, and even screen designs, he says, and Novell worked to design such customizations.

“From my perspective, the level of partnership and engagement we got very, very early on was important,” Leach says.

The Novell system first went live in August 2009, and since then has ramped up to 75,000 users. ACS continues to roll it out at new client locations as well as to new internal applications, Leach says.

So how does it work? Adding new employees now happens at “Zero Day,” as Tong puts it; if hiring managers hustle, they can have an employee ready to go with the right amount of access before the person shows up for his first day of work. Even in the worst case, Tong says, new arrivals have access to e-mail and basic tools such as employee training. Those leaving ACS lose IT access immediately.

Among the Novell system’s strengths have been its scalability, its ability to allow applications in different data centers to communicate securely, and most importantly its reverse Web proxy, which Tong described as “a big deal to us.”

Standard proxy servers from Apache or Microsoft work by fielding requests for data (either from employees somewhere else on the IT system, or outsiders submitting requests over the Web) and tapping internal servers for the requested data. But people shouldn't be able to access Web applications and their accompanying data directly; it's a security risk. A proxy server essentially collects a data request and eyeballs the person asking for it to be sure he has proper clearance to receive it. But in large IT systems with many proxy servers, *that* requires users to enter multiple user IDs and passwords—which gives rise to the age-old IT security threat of someone writing down all his passwords on a Post-It note next to the computer monitor.

Novell's reverse proxy server adds the ability to convert all those ACS user IDs and passwords into a single, universal Novell ID and password that works for different applications across the ACS landscape. The data is still protected, the user remembers his password, and whenever the employee ultimately leaves the company, ACS can kill the universal password (and all that worker's access privileges) in one stroke.

"Not only is the security requirement satisfied, but you also have the ability to do single sign-on, so you're killing two birds with one stone," Tong says.

On the compliance side, the controls inherent in the Novell system (it logs and tracks all user access for auditing purposes) has lessened internal and external auditors' access-control concerns and cut investigation time, Leach says. Should he, Tong, or anyone else need to determine who had access to what IT resource at which time, they can simply run a report.

Given the sheer size of the system, the multitude of locations and the range of user skills, user training was a challenge, Leach admits. But work to customize user interfaces helped, and ultimately, he says, the new system's performance was such that users saw its value and worked hard to get up to speed.

"We've had no outage, we've had nobody say they're going to kill the CISO," Leach quips. "It's been more about how they can get their applications on board. We have more requests than we can handle. That's how successful it's been."

RELATED RESOURCES

COMPANY BASICS

Company	Affiliated Computer Services
Headquarters	Dallas
Employees	74,000
Industry	IT Services
2009 Revenue	\$6.5 billion

THE CHALLENGE

Affiliated Computer Services, which specializes in IT and business-process outsourcing, needed to get control of identity management and access controls to satisfy auditors, boost productivity of new employees and reduce IT security risk for both ACS and the company's clients.

SOLUTION CHOSEN

ACS chose Novell's Compliance Management Platform, which the company used to drastically speed the addition of new employees (and deletion of departing ones) as well as providing single-password sign-on to both internal staff and customers.

This "case study" is the latest in a series of articles aimed at helping public companies understand how other organizations are using technology to comply with new regulations and standards. These are **not** advertisements or marketing vehicles for the companies mentioned; Compliance Week's editorial staff speaks with the public company that has deployed the technology, and the article is written without the input—and in many cases the knowledge—of the vendor.

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.