



March 11, 2010

Case Study: A North American Energy Company Presents The Carrot, Not The Stick, Of PIM

by **Andras Cser**

with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

A North American energy company recently faced a serious challenge — it could not successfully pass Federal Energy Regulatory Commission (FERC)/North American Electric Reliability Corporation (NERC) and Sarbanes-Oxley (SOX) compliance audits because of the way it managed privileged users. Its manual PIM processes didn't scale. System administrators (SAs) spent a great deal of time locating, verifying, and changing administrative passwords manually for hundreds of systems. The company had to do something, so it decided to implement an automated privileged identity management (PIM) solution. The implementation was a success, in large part because the company overcame organizational resistance by recruiting technologically savvy SAs to provide feedback on policies and champion the rollout with peers. As a result, the PIM solution has not only reduced risk associated with the once manual PIM processes, but it has improved system administration and achieved regulatory compliance in understanding how it assigns and practices access to its sensitive systems.

SITUATION: REVOLVING DOOR OF SYSTEM ADMINISTRATORS PRESENTS A SECURITY RISK

As a leading North American utilities company, the organization operated in a highly regulated environment. It had to meet FERC/NERC and SOX requirements and establish effective controls for PIM, which includes securely storing, retrieving, and changing authorized system administrator (for both Windows and Unix systems) and database administrator account passwords. Administrators were using manual methods to store privileged passwords, including Excel spreadsheets, envelopes in safes, and email. Using these offline, unverified mechanisms to store sensitive passwords was not only risky but ineffective. It was risky because if someone were to find the printout of a spreadsheet, he would gain unauthorized access to many systems, and it was ineffective because you could never be sure that the password you had written down in spreadsheet, email, etc. was still going to work on a specific endpoint. Because the company was growing, it could not simply hire additional headcount to keep up with the additional PIM duties manually — it needed to change the way it handled PIM. There was another important driver of change. This company also outsourced part of its system administration to a global managed security services provider (MSSP). Unfortunately, the MSSP has about 55% turnover in the ranks of its SAs. This high turnover rate, coupled with the fact that the energy company was not immediately notified by the MSSP when a system administrator left, led to a serious security issue — it was exposing its critical administration of its critical systems to individuals who no longer were authorized to access the company's systems.

BEST PRACTICE: HIGHLIGHT BENEFITS TO EARLY PIM ADOPTERS

Resistance to change was initially high among the SAs, who were concerned that their ability to perform routine and fire-calls system administration would be hampered if they did not know all the passwords. Some of their in-house-developed system administration utility scripts had hardcoded passwords in them that would break if and when an automated password safe was introduced. The company overcame SAs' resistance to change by:

- **Finding and persuading savvy SAs to initially use the PIM solution.** Some SAs had to manually change more than 500 passwords in the environment on a regular basis. It's no wonder these folks were eager to try a solution that would make at least part of this task easier. IT risk management (the organization responsible for the implementation of the PIM solution) then identified "champions" among these SAs to be the first users of the Cyber-Ark Enterprise Password Vault PIM solution. The company listened to the champions' feedback on policy design, auditing, and automation and also asked them to socialize the benefits of using the PIM solution to convince naysayers.
- **Presenting a clear-cut, policy driven, and automated password management process.** The champions realized that a PIM solution would drastically reduce the time it took for an SA to find a password to a sensitive system. It turns out there were other benefits. Password checkout (which, for some key systems was tied to a workflow process for application owner or line manager approval) established accountability for the use of sensitive passwords and reduced finger-pointing, which was related to stress among SAs. A number of different policies were established, governing the use of privileged passwords across different systems. In addition, workflows were implemented for a user account provisioning and helpdesk ticketing system, which integrated with the PIM solution.
- **Eliminating inconsistencies in scripts, login screens, and banners.** PIM champions recognized early on that hardcoded passwords in scripts and the different login screens on the company's similar infrastructure assets (AD domain controllers, routers, etc.) were set up insecurely and inconsistently. This presented a challenge. It would require heavy customization for the PIM solution to recognize login screens and automate password change, checkouts, etc. effectively. As part of initial housecleaning, they eliminated all hardcoded passwords from scripts, made all passwords longer and more complex, and required that all sensitive passwords be changed every 20 days.

Next Steps: Use Automatic Sessions Without Releasing Passwords

Revealing checked out passwords to SAs, even for a short time, poses security challenges. SAs may share the passwords verbally or leave them lying around on yellow stickies — a violation of mutual exclusivity and unauthorized access on a system. To avoid this problem, the company started using a PIM proxy broker solution. After successfully checking out the access rights to the SA, the PIM

proxy broker automatically spawns a Windows Terminal Services or UNIX SSH session to the machine that the administrator now has access rights to. Not only is this more secure but the SAs can do their job faster (they don't have to manually start a Terminal Services or SSH client and then plug in the password).

BEST PRACTICE RESULTS: BENEFITS OF PIM REAPED FAST

With the early feedback of champions into the policy design and rollout process, a PIM solution was implemented in just six months for some critical systems. The PIM solution changes passwords every day on these systems, and as a result, the company achieved regulatory compliance and eliminated the risk of unauthorized access by terminated MSSP SAs. The PIM system also ensures that now 98% of the passwords are automatically, regularly, and successfully verified — moving the company along a great deal toward achieving regulatory compliance by being able to prove to its auditors that passwords are of higher strengths (longer and more complex) and are changed regularly as well.