

From Network World's Security: Identity Management Newsletter, 10/22/07

Roles make governance easier

By Dave Kearns

Aveksa CEO Deepak Taneja and the company's new Marketing VP, Brian Cleary, were on the phone with me a couple of weeks ago to assure me that Securent is not Aveksa's competitor - as I may have alleged earlier this month - but is a trusted technology partner. As Taneja and Cleary put it, Aveksa provides the business portion of governance while Securent provides the enforcement layer of entitlement. That's a good point to make, and one that reminds me to remind you that the business case and the technology case have to intertwine for identity management to be effective.

They also made two other points which endeared them to me – the importance of roles and context.

I've mentioned previously that I'll be doing a track on "context" at the 2nd European Identity Conference next April. The organizers are currently calling it "Risk-based authentication," but we'll make it broader than that as we include context in viewing data, authorization and governance. I'm hoping to have Taneja do a presentation on context in governance. More on that later.

Both Taneja and Cleary stressed that roles make governance easier. While they wouldn't commit to saying roles were absolutely necessary, they did agree that trying to manage governance without them could be a very expensive proposition. But, they emphasized, "role-based governance" does require the definition and management of roles.

A number of people in the area of governance and entitlement have emphasized that many IT departments take a decidedly last century view of roles, seeing them as some sort of extension to, or replacement for, "groups," as we know them in a network operating system way, i.e., the word processor group, the spreadsheet group, the materials group, etc. And while it's true that 20 years ago we used groups to allow access to network resources, there is no governance with groups, there are no policies or rules (no matter what the Windows Server documentation says) that can turn groups into roles. Groups are a purely IT functional entity. Roles, on the other hand, are business objects. Roles consist of business rules ("materials buyers cannot approve invoices") and IT groups ("materials buyers are members of the 'Excel,' 'Word' and 'Oracle Financials' groups") working together, subject to methods and policies created by the governance process. It is not necessary for all employees to be placed into roles, but it is often necessary for a particular employee to simultaneously inhabit multiple roles.

Implementing role-based management is not difficult but it does require attention to detail and it does require that IT and business management cooperate fully. It's that cooperation (or lack thereof) that can torpedo an otherwise well-planned project.