5 Quick Questions: Securing Data Without Hindering Work Flow

Jeff Reinke, Editorial Director - @JeffReinkeABM

How do you ensure that your data is secure without holding back your employees from doing their job?

Dean Wiech is the managing director of Tools4ever, a company which offers a combination of robust software and consulting services in the Identity and Access Management (IDM/IAM) market. He recently took some time to discuss how using technology that exists today can improve workflow on the shop floor by giving employees access to the data they need to do their jobs without a cumbersome process of multiple logins and credentials.

1. What are some of the biggest issues manufacturing enterprises face in keeping operational data secure?

The biggest challenge in securing operational data is ensuring that only the correct people have access to the data needed to perform their jobs. I think manufacturers in general do a good job of protecting their data, but the task of making sure that access within the organization is restricted on a need-to-know basis can be monumental. Applications are available in the market to easily allow the creation of roles within an organization. Known as role-based access control (RBAC), it basically defines who should have access to what data and application based on several factors, such as department, job title and location.

2. Do you feel enough emphasis or resources are being allocated towards data security?

I believe that manufacturers are keenly aware of data security and the need. I also believe that most do the best job they can, time and money permitting. Finally, there needs to be new tools available to reduce the efforts required to secure data while providing an even higher level of integrity. One component of this is to insure

accounts are provisioned and de-provisioned in a timely and accurate fashion. Commercial software tools are available to link HRM systems to network accounts and ERP/MRP solutions. This insures that when an employee joins an organization they have the correct rights to do their job and when they leave, all access is revoked.

3. What can manufacturers do to help keep information secure without creating time-consuming obstacles for accessing this information?

I think there are really three components required to increase security without introducing more overhead:

- Utilize RBAC templates to insure that people in a specific job only have access to specific data
- Insure that when an employee's role changes, the security permissions are updated appropriately
- When an employee leaves the organization, their access must be terminated immediately

4. ERP software generates a tremendous amount of data. Speaking in general terms, which data sets do you feel plant operations personnel should focus on? How might this change for others in purchasing, inventory management or maintenance?

I think that each department needs to have access to the data relevant to perform their tasks in the organization; no more and no less. A properly configured RBAC template within the network and ERP system allows a higher level of confidence in this matter.

5. If you could give U.S. manufacturing one thing, what would it be?

A modernized ERP solution. I have seen companies where some employees had to have up to seven sets of credentials to access different parts of their ERP. Imagine the time-consuming process of remembering which set of credentials allowed you to access specific pieces of data. It is important to note here that any RBAC or identity management solution should have the capabilities of interfacing with the ERP solution to properly set, update and revoke roles automatically by interfacing with the HRM solution. This reduces or eliminates the need for manual intervention, saving time and money.

Source URL (retrieved on *08/20/2014 - 5:41am*):
http://www.foodmanufacturing.com/blogs/2014/05/5-quick-questions-securing-data-without-hindering-work-flow