

Streamline the security processes

Thomas R Cutler discusses how technology solutions can guard malevolent data tampering and in due course smoothen the data to work impeccably. Here both the principles of security and safety play a significant role and are to be seen as part of a lean manufacturing continued process improvement programme

Lean manufacturing principles call for productivity gains, which are increasingly dependant upon speeding up the flow of sensitive data throughout the enterprise. As proprietary data is managed through an ERP (enterprise resource planning) system industrial security requires that this precious information must be guarded from malicious data tampering. According to Evan Garber, President of Escape Velocity Systems, which specialises in formula-based process manufacturing, "Advanced auditing and security functionality is not simply preventing unauthorised data manipulation...risk management, it provides a context for a data management plan that includes process improvement." Technology solutions must provide direct security and user accountability for one's actions along with the ability to manage the ancillary attached data through an approval, lockdown, and version control process; security also requires efficiency of electronic document handling. Garber suggests that there are specific questions that process manufacturing CFO's must be able to answer from ERP reports including:

- Who are all the people who

touched this document and how long were they working on it?

- What reasons were provided for making additions, deletions, or modifications?

- Did a supervisor approve the changes?

- What safeguards are in place to ensure that the user, not someone else, made changes?

Other aspects of internal data security

According to Stephen Parker, CEO of Datacraft Solutions, "To ensure security, data must be working seamlessly with existing visual board systems. Digital kanban solutions allow individual cells or entire supply chains to realise an immediate and dramatic return from an extremely small process automation investment, by vastly reducing the management time." Routine, repetitive tasks are automated, and exceptions are instantly highlighted in this highly secure 'Software as a Solution' (SaaS) model, so that managers can focus their time and skills on responding to and eliminating problems before they reach the plant floor. On-demand Internet-based delivery platform further streamlines the process by eliminating the cumbersome, time-consuming and costly implementation required to

integrate new hardware and software into an IT infrastructure. Mr Parker noted that the security of the data is impeccable: "We host all the data at our data centre. We have a server farm with 100 per cent redundancy and three OC3 lines. Our data is 99.999 per cent secure, and our clients have never experienced down time, thanks to a multiple UPS power backup system and 900 kw diesel caterpillar generator. We also have biometric scanners for data centre security."

Other SaaS solutions support customer data security

Larry Caretsky, President of Commence Corporation, the leading SaaS CRM provider, marking their 20th year in business in 2008, noted, "No data is more important than customer data. The customer information, including buying trends, ordering patterns, and general database contact information is the backbone of every organisation and security precautions must be taken to protect the sanctity of that information, particularly in a SaaS environment. Data breaches are not an acceptable outcome and we have taken extraordinary steps to guard the data of our customers." Caretsky's assertions were recently corroborated by Linda Foley, who

founded the Identity Theft Resource Centre after becoming an identity-theft victim. The organisation lists more than 79 million records reported compromised in the US through December 18, 2007; that is almost four times the nearly 20 million records reported in all of 2006. Attrition.com estimates more than 162 million records were compromised through worldwide compared to 49 million the year earlier. These soaring and unprecedented incidences require that solutions providers take extreme measures to protect valuable customer information.

The safety component

As outsourcing shifts the manufacturing model to a distribution centre modality, no where is employee safety more

compromised than on the distribution floor. Unlike the days where all the items were shipped by the case load and carefully palletised, many retailers are demanding partial shipments.

All these specialised pick and pack distribution requirements could dramatically increase the safety concerns. According to Jerry List, VP of QC Software, "The old WMS (warehouse management system) model of advanced forecasting of the picking and shipping process does not work in a real-time dynamic warehouse. The WCS allows for real-time information and routing."

Only the bottom-line drives industrial safety and security

While it sounds politically correct and ethically appropriate to speak of employee well-being, too often

this mantra is little more than corporate public relations spin. It is fine to speak of the responsibility of every company to establish, supervise.

Unless security and safety are seen as part of a lean manufacturing continued process improvement programme, it is usually an afterthought to a 'problem'. This seemingly cynical perspective is played out in thousands of press releases daily; and safety concerns are 'carefully investigated.' Bottom-line impacts, from reduction of accidents and expensive product liability litigation, drive industrial safety and security...to think otherwise is naïve. 🚫

The author is President and CEO of Fort Lauderdale, Florida-based TR Cutler, Inc. He can be reached at trcutler@trcutlerinc.com

Half Page AD
Rajamane
Industries