

Proactive Compliance

Mazda's European IT operations prepare for Japan's Sarbox regulations as part of a broader information protection strategy

Clement Laeremans oversees IT for Mazda Motor Logistics Europe NV, but he keeps a close eye on his counterparts in Asia. And for good reason: Like many organizations that have operations in Japan, Mazda's remote IT departments must comply with J-SOX (the Japanese version of Sarbanes-Oxley) within a few months. "We absolutely have to be J-SOX compliant, and our users' systems have to play by the rules of J-SOX," says Laeremans, manager of the company's information system operations in Europe.

Mazda isn't alone. All Japanese businesses and their subsidiaries worldwide need to comply with J-SOX requirements for fiscal years beginning on or after April 1, 2008. Much like the Sarbanes-Oxley regulations in the United States, J-SOX calls for businesses to audit their financial, business, and technology operations, more closely. J-SOX also

requires businesses to tighten their IT security and information protection efforts. "This is going to be a big challenge for hundreds—perhaps thousands—of companies that have ties to Japan," predicts Ed Golod, president of Revenue Accelerators Inc., a technology consulting firm in New York. "Sarbanes-Oxley was a major distraction here in the United States for many IT managers. Now, J-SOX will be a similar distraction."

While some businesses are struggling to jumpstart their drive towards J-SOX compliance, that's not the case at Mazda Motor Logistics Europe (MMLE). Indeed, corporate compliance is just one piece of the organization's broader information protection strategy. Leveraging several solutions from Symantec, MMLE has both fortified and simplified its data protection environment while saving 70,000 Euros.

That's no small feat. MMLE has a complex IT environment spanning an IBM mainframe environment running IBM DB2 database; a HP-UX server running Oracle database; and dozens of servers running Red Hat Enterprise Linux, Novell SUSE Linux Enterprise, Microsoft Windows, and VMware. If the data residing on these disparate server environments was compromised or somehow lost, Mazda Europe could face fines or other penalties related to J-SOX.

Still, ensuring corporate compliance isn't MMLE's only concern. As an enterprise serving 17 national sales companies, it must push beyond compliance regulations to ensure that its data is highly available for 24x7 business operations.

One solution, multiple platforms

Until recently, MMLE used a mix of backup-and-recovery solutions across its servers. But Laeremans went on a quest to find a single information protection platform to blanket the heterogeneous network, and therefore simplify data management.

Enter Veritas NetBackup, which now protects Mazda Motor Europe's sales, financial, marketing, and after sales support data. Leveraging NetBackup, the mainframe, HP-UX, and industry standard servers receive incremental backups throughout the week as well as a full weekly backup. "NetBackup's cross-platform support all comes together in a single unified console, which Mazda Motor Logistics managers can

By Joseph C. Panettieri



Clement Laeremans,
Manager, Information
System Operations,
Mazda Motor Logistics
Europe

leverage for real-time monitoring, historical reporting, and alert management,” notes Laeremans.

This information protection strategy has paid immediate dividends. By standardizing on a single backup-and-recovery solution, the company saves 40,000 Euros (approximately US \$55,000) annually on maintenance and license costs.

Email compliance

Increasingly, regulations like J-SOX and Sarbanes-Oxley require companies to protect both structured information (typically stored in databases) and unstructured data (like email systems).

In MMLE’s case, email is a business-critical application that connects 250 internal users with more than 1,000 users in the 17 national sales companies. The system, based on Microsoft’s Exchange Server, is a pipeline that can’t afford to suffer information loss. To safeguard the system, the company leverages Symantec Enterprise Vault for archiving and e-discovery, including policy management. Enterprise Vault helped MMLE condense the size of its Exchange Server system by 45 percent.

There’s also a clear compliance benefit here. If, for instance, regulators visit the company’s European operations and request specific information—such as email exchanges between specific employees on specific dates—the e-discovery functionality in Enterprise Vault would allow Laeremans to fulfill that request.

Protecting PCs

MMLE’s information protection strategy extends well beyond servers onto desktops and notebooks, where its security efforts start with some basic requirements. Each user who logs into a MMLE system must have complex passwords that need to be

“We’ll be ready. With help from Symantec, J-SOX is something we’re well prepared to address.”

—Clement Laeremans, Manager, Information System Operations, Mazda Motor Logistics Europe

changed every 90 days, according to J-SOX requirements. Notebooks and PCs containing mission-critical information—such as accounting data—require higher levels of security. “In the case of accounting information, we have to encrypt the data in order to comply with J-SOX,” says Laeremans.

Now, for the challenge: Many encryption technologies have considerable overhead and therefore slow down the performance of a PC, notebook, or server. “We’ve seen that first-hand,” concedes Laeremans. “So we’re looking at a few solutions at the moment and doing some proof-of-concept work to determine the best encryption option for us.”

Meanwhile, MMLE has to maintain a delicate balancing act with its dealers. On the one hand, the company has to fully safeguard its network. But on the other, dealers need timely, comprehensive access to the automaker’s portals. “When it comes to our dealers, the only way they can access our dealer portal is through virtual private network connections,” says Laeremans.

When those remote systems attempt to connect to MMLE’s portal, the network checks the remote PC to ensure it has the appropriate antivirus and anti-malware software in place. The network also checks the remote PCs to verify that they are, indeed, Mazda-approved systems. “If the remote system isn’t fully up to date, we can provide limited access or no access at all, depending on the scenario,” says Laeremans.

Coordinated defense

Like an engine that fires on all cylinders, Laeremans works with several peer departments to ensure MMLE’s security strategy is implemented effectively.

Naturally, he reaches out to Mazda’s headquarters in Japan for guidance, and his counterparts in Asia also seek ideas from time to time. For instance, MMLE was the first division within the company to use HP-UX, which required it to embrace UNIX-oriented backup and recovery technology as well. But that wasn’t a big challenge, because of Symantec’s commitment to cross-platform support. “When we introduced HP-UX into Mazda a few years ago, the Japanese team came over for a couple of weeks to look at it and determine if it might be a fit for them as well,” recalls Laeremans. “A couple of months later, they started down the road with HP-UX.”

Looking ahead, Mazda Europe only has a few more months to ensure its systems comply with the March 2008 J-SOX deadline. But Laeremans isn’t worried. “We’ll be ready,” he says. “With help from Symantec, J-SOX is something we’re well prepared to address.” ■

Joseph C. Panettieri is VP, Editorial Content at Microcast Communications. He has covered Silicon Valley and the business of technology since 1992 for such publications as InformationWeek.

Read Online:
[www.symantec.com/
ciodigest/emea/mazda](http://www.symantec.com/ciodigest/emea/mazda)