Virtual Watchdogs

From dealing with tricky U.S. accounting rules to ever-determined hackers, information bosses are turning into security experts, too.

FORREST JONES • MIAMI

Mention the words chief information officer (CIO) and most people think about a classic tech geek. The guy who decides what all computers we have on our desks. His staff members are the people we love to yell at when our email is too slow.

Things are different now. Sarbanes-Oxley and other U.S. regulations that emerged in the post-Enron accounting scandals require companies to disclose more and more information to regulators, most of which is stored digitally these days. Plus, in a merger-crazed and credit-card happy world, increasing levels of data need to be kept confidential, especially during sensitive business dealings like due diligence. Not an easy task considering all the data potentially sitting out there on email, in smart phones leaving the building and on public instant-message files.

While auditors and regulators tend to focus on the CEO or the chief financial officer for proof of a tight ship, it's exactly those two executives who are turning to the CIO more and more for advice on how to keep the house in order. The tech post is becoming more of a watchdog role.

"All the critical information and the business information has become digitalized. The bits and bytes have become the most valuable company assets," says Douglas Wallace, director of systems engineering for Latin America at Symantec, a provider of security software. "They are just as valuable as the paper documents or even receipts or government papers. Therefore, the role of the CIO now is to protect all digital, data and communications."

On top of keeping information stored, the CIO must be able to retain information should anyone ask for it. Some of that data can be quite old; regulators now require publicly traded companies to keep it for seven years. "If you don't have archiving software, it can be very difficult," Wallace says.

Compliance aside, there are other threats on the horizon. Sixty percent of the email on the Internet is spam, many of which contain viruses and other harmful programs, Wallace says.

The CIO must define the security parameters and get everyone to comply. Even company consultants need to 'fess up when it comes to what's been downloaded. "Right now, seventy-five percent of the investigations regarding [Sarbanes-Oxley] is based on email research. This is very interesting because 80% of the company assets are on email," Wallace says. Imagine shifting through seven years of email from 10,000 employees looking for a suspect email. Quite a daunting task. But Latin America, Wallace says, is holding its own. "Right now, countries like Brazil, Mexico, Chile and Argentina, for example, are at the same pace as the United States on requirements on security, availability and compliance."

That makes the CIO the best friend of the CEO and the CFO. When it comes to compliance, really close friends: The CIO is not held accountable for company reporting in the eyes of regulators. The CEO and CFO feel the heat there. So what they do? They make everyone else account for his or her business. It can go down quite a ways, and technology is the answer to doing just that—all to make sure that when upper managers sign off, the documents are accurate and defendable.

TOBIAS FELBER/DPA

"The CIO has to find the tools to offer the CFO to automate systems," says Leticia Cavagna, program manager for management visibility and control for SAP Latin America. "The CIO is the enabler of the CFO's wishes."

Since many U.S. companies want their suppliers to abide by Sarbanes-Oxley in some shape or form, many in Latin America are taking note. According to Cavagna, 88% of Latin American companies when asked about the U.S. accounting regs wanted to comply with U.S. regulations even though they didn't have to. Of that group, 81% said the benefits would outweigh the technological costs of adapting, Cavagna says. Most are still big companies. But smaller companies are jumping on the learning curve.

Quiet. Despite all the headlines about disgraced CEOs in the United States, protecting data is not just a U.S. story. Any company that lists equity in the United States is subject to U.S. rules—wherever they are. When companies merge, too, they need to keep quiet to meet stock market information rules, no matter where they are. In Latin America, that means there are three types of companies that need seriously to protect and retain their data: Latin American subsidiaries of U.S. companies that are publicly traded; large Latin American companies that trade in the United States; and, lastly, privately held Latin American companies that distribute or supply the previous two examples. All have a vested interest in complying, since listed companies must disclose information related to their business partners.

"Bits and bytes have become the most valuable company assets."

CIOs and other executives who protect data say that they find themselves becoming more involved in the business side of company operations, and not just on the technology issues, says Chris Day, senior vice president of security services at Terremark, a U.S. company that owns a network access point, or NAP, that caters to Latin America and retains and protects data for corporations.

Today, a CIO could spend half of his time making sure technology helps comply with all the different regulations as well as keeping company data secure, Day says. The best way for a CIO to do just that is to receive some sort of certification that shows compliance, like international standards organization ratings on security. Doing so takes care of meeting Sarbanes-Oxley requirements and any other regulations and security compliance that a company might face in any part of the world. "Move towards operating in best practices, then it's not so hard," Day says. "You get a lot of what you need for [Sarbanes-Oxley] compliance."

For some companies, though, it's not easy, and it's especially hard for the smaller ones. They are starting from scratch and may need to pay out consultants to get them there. "Going from zero to full compliance can be very difficult," says Day. Even when the company complies, the CIO must continue to keep an eye on his own people. There have been

cases where an employee does not feel comfortable with a new system and continues to enter sensitive data—like customer credit cards—in a spreadsheet file that ends up on a company computer that could be easily stolen. “If you can’t protect it, you can’t say you have controls,” says Day.

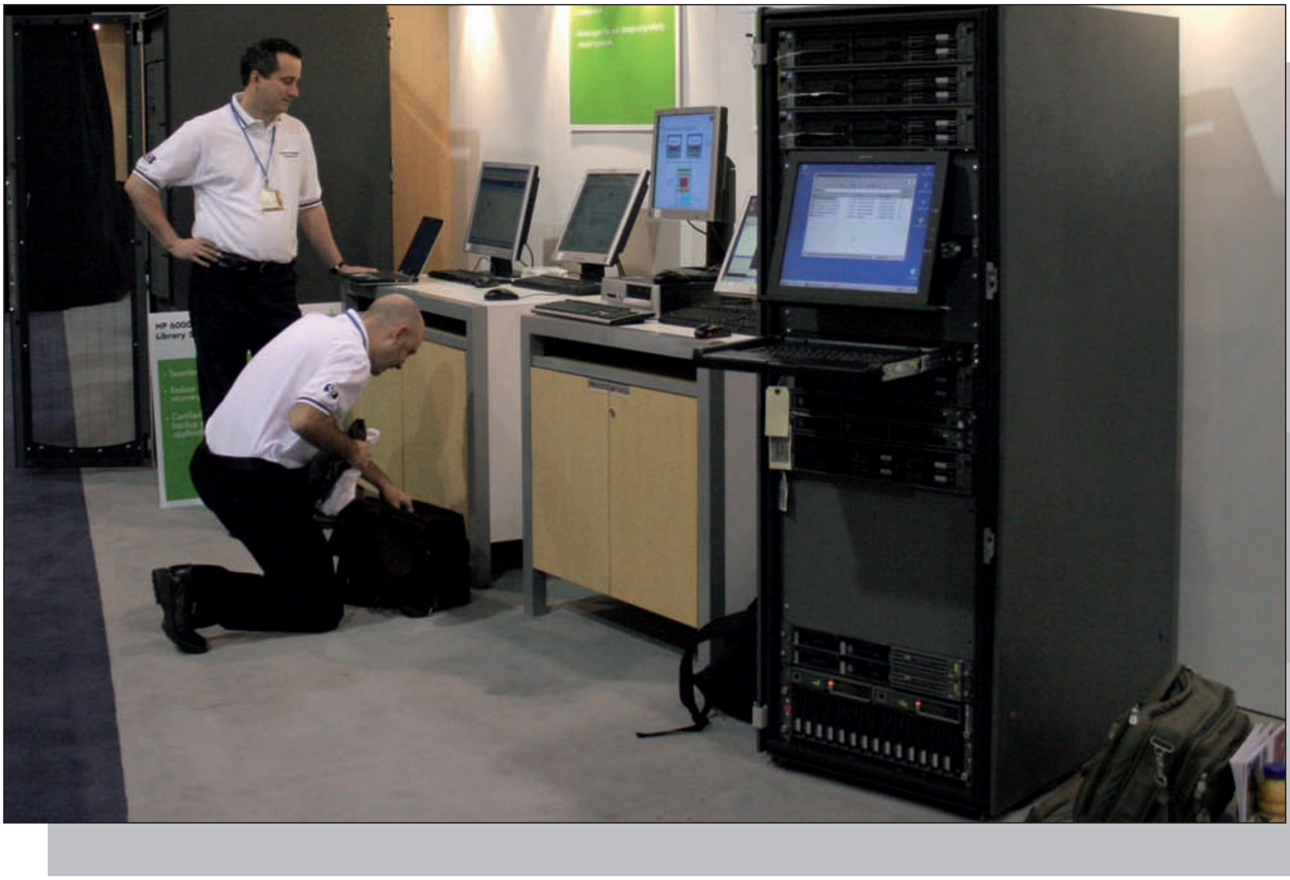
For many Latin American companies, Sarbanes-Oxley is not the only problem. There are domestic regulators too. Central banks and the domestic stock market regulators want to see all the receipts these days. Some companies must meet regional standards, too, says Jesús Estévez, CIO for South America at PricewaterhouseCoopers, a U.S. accounting firm. “There are other regulations besides Sarbanes,” Estévez says. “There are countries where besides international regulations, there are local sub-requirements and sub-regulations that need attending.”

Most companies in the region have done a good job of getting technology up to par, Estévez says. Argentina took a hit after the economic meltdown in 2001 and early 2002, but today, tech spending is back, he says.

For the companies that audit financial statements, sound information technology systems are a critical component, says Steve Hasty, lead partner in the United States for information technology at KPMG, a global accounting and auditing firm. It’s important for companies to use technology in the controls of their business, Hasty says, including payment systems and other applications closely tied to financial reporting. Other systems are needed to monitor whether or not things are going smoothly in the business. Then you need systems to monitor the systems. Those could be different tasks for different companies, depending on the company’s size and the nature of its particular industry, says Hasty. “One of the challenges is to understand the requirements that you have as a company to protect information,” says Hasty.

The CIO, for instance, must know corporate policies and how to put a system in place for departments as varied as finance and human resources. In other words, the CIO needs to know more about what’s going on in a company-wide fashion as opposed to just the technology side, Hasty says. Regulations change. Laws change. The company could expand into new ventures or locations. Plus getting the system implemented is one thing, but keeping it up to date is another.

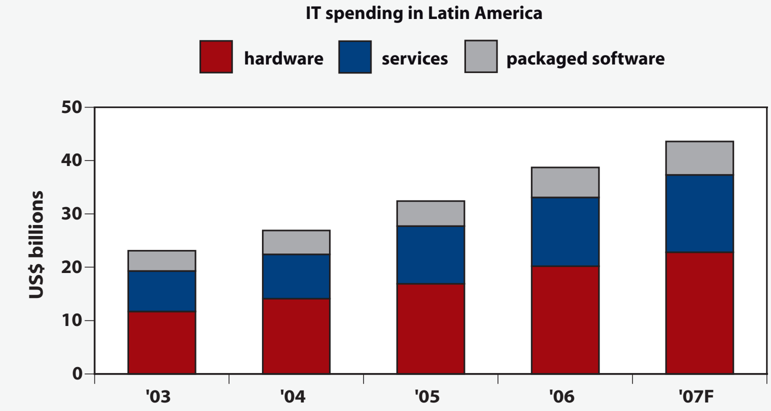
“The CIOs need to be prepared that their technology and the controls embedded in those technologies can meet the compliance requirements, not only for today but be sustained in the future,” Hasty says.



BARRY SWEET/BLOOMBERG

Plug In

Tech spending in Latin America climbs, leaving CIOs with more to protect.



F= Forecast
SOURCE: IDC

That goes for Latin America, too. Still, the region is not as demanding as the United States is, says Carlos López, an information technology advisory partner in charge of Mexico and liaison for Latin America at KPMG. Yet, soon, the entire region will catch up, he says. Latin American governments and regulatory bodies are starting to demand more disclosure from their companies as part of a global trend. Mexico recently passed a capital markets reform bill that toughened up accounting requirements. Brazil has rolled out the Novo Mercado, a stock index that requires companies wanting to list on it to meet greater disclosure requirements. "This is starting to set the tone of corporate governance to try to align the initiative of [Sarbanes-Oxley] in Latin America," López says. "A few years from now we will all follow these rules." That said, companies looking to comply should do so whether they need to or not. That's more than just getting used to disclosing more information. It means running the business to disclose more information more easily, López says.

> "Going from zero to full compliance can be very difficult."

Protection. Perhaps one of the most vulnerable pieces of information out there on the Web are what industry experts call personally identifiable information. Chances are, if you bought something—especially on the Web—your credit-card number and other sensitive data are floating around on some database.

Credit-card companies themselves can help out, in order to stamp out identity theft. They provide programs that allow vendors to protect credit-card information. They can also offer advice as to how a company can protect itself from those who would harm it: Go from the outside in, says Alfredo Pérez, senior vice president for support services for Visa's Latin American and Caribbean region. Protect the company's network first. Then the hardware and then the applications and then the data itself. That makes a hacker or anyone else looking to steal data break through many more levels of security to get to the goodies.

"The more difficult you make it, they go away," Pérez says of potential hackers. "They want the low-hanging fruit."

That's not an easy task. The CIO must continue to monitor all systems and go through routines such as changing passwords. Plus he has to make sure the right people have access to the right information. "Before it wasn't a big deal, but now it's a great deal," says Pérez.

So what about the employees themselves? Do they play a part? Absolutely says Kari Pérez at Visa's corporate communications office for Latin America and the Caribbean. "We are always getting emails from the company asking us to be compliant," says Kari Pérez. To help out, Pérez attends annual training sessions focused on keeping the data safe. It's also part of the initial training employees go through when they begin work at Visa, where people are taught what programs they can and cannot run on their computers.

What happens when data gets leaked? What if someone screws up an accounting journal? Should you panic? Not really. A well-run company should have a plan for this sort of thing, says Kevin M. Levy, a lawyer with the Gunster Yoakley law firm in Miami who specializes in business law and corporate finance.

A company should have a response team ready to act in case an event were to happen. That team should include attorneys, public relations experts and the IT team. And having that team ready is still not enough. "You've got to test that plan over and over and over so you've got it down pat when something happens," Levy says.