

## Navigating a Sea of New Security Threats

Mary K. Pratt

**January 01, 2007** (Computerworld) The IT folks at Louisiana State University have had some tough tests lately.

They survived Hurricane Katrina with their own systems in Baton Rouge intact, only to see that campus turned into an emergency work site used by rescue agencies and the University of New Orleans.

Then they found themselves combating a homegrown phishing scam executed by a student posing as the university registrar.

Those incidents were on top of the everyday challenges facing LSU's IT department, which is also charged with maintaining the open environment that academic institutions consider key to preserving a culture that promotes sharing and the free exchange of ideas.

part of the  
Special Report...



“While we have to pay attention to the survival issues, which disaster recovery and security are very much a part of, we have to continue to make sure we do the other things we’re here to do, too,” says Brian D. Voss, LSU’s CIO.

It’s a dangerous world out there, and IT leaders like Voss know it. Last year’s headlines about calamities and breaches have put disaster recovery and security at the top of IT agendas.

In *Computerworld*’s [Vital Signs](#) quarterly trend survey, 31% of IT executives placed disaster recovery/continuity planning at the top of their priority lists, while 27% identified data security/privacy as their No. 1 issue. Combined, these results show how IT leaders have a stronger focus than ever before on data integrity as they head into the new year.

IT executives said their top IT

project priorities for the next year are:

1. Disaster recovery/continuity planning
2. Data security/privacy
3. Data management implementation or upgrade

Source: *Computerworld's* quarterly [Vital Signs](#) survey, 252 respondents

## **Maturation, Not Just Continuation**

To be fair, most IT executives have had an eye on these areas for many years. As a result, the way leading companies approach business continuity planning and security is evolving, increasingly moving these critical areas from project mode to more of a process mentality.

“I see it as a maturation of the processes,” says Scott Laliberte, global product lead for the security assessment practice at Protiviti Inc., a Menlo Park, Calif.-based firm that provides risk consulting and internal audit services.

Several factors are contributing to this maturation, Laliberte says.

On the data security and privacy front, the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard and the ISO 17799 best practices standard are among the forces pushing companies to enact tighter controls. Security breach notification laws have also driven IT directors and business executives to give the issue more attention and resources than in prior years.

Meanwhile, companies are learning hard lessons about business continuity from organizations that suffered through the 9/11 terrorist attacks and Hurricane Katrina. In addition, technology vendors are delivering more mature products to help IT executives accomplish what they need to do to ensure overall data integrity.

“Companies are looking to improve the maturity of their processes and investing in that on a risk-based approach,” Laliberte says.

## **An Evolving Threat**

The risks out there are significant. Just look at the area of security.

“The threat profile is evolving from a teenage hacker to a well-financed, determined intruder that may be working for organized crime, a hostile foreign government, a terrorist group or a competitor. These are people who are willing to spend a considerable amount of time and money

to accomplish their objectives,” according to Jonathan G. Gossels, president and CEO of SystemExperts Corp., a network security consulting firm in Sudbury, Mass. “Further, their objectives may be to subtly, rather than blatantly, impact a system, so the subversion may go unnoticed for a long time.”

That’s in addition to the worms, viruses, phishing scams and old-fashioned hacking attacks that remain pervasive even today.

Companies also need to worry about their own workers, who often inadvertently and sometimes maliciously handle data in ways they shouldn’t. They might e-mail sensitive information without encryption or deliberately walk off with a USB stick containing intellectual property.

Yet, Gossels says, “many companies still think in terms of ‘If we make this inconvenient, the hacker will go somewhere else.’”

Many companies also have plenty of weaknesses in their infrastructures, adds Dick Mackey, vice president of consulting at SystemExperts. The ID information provided by customers may not be unique enough to identify them securely, user authentication may be lax, or workers may not be fully aware of their duties to keep information secure.

### **New Threats, New Action**

Voss says he hired a firm in 2005 to conduct a security audit of LSU’s IT infrastructure; although it gave the school a “fair” rating, the auditor still listed 90 areas that needed improvement.

Voss is taking action. He’s ridding most systems of Social Security numbers. He created the positions of security officer, deputy security officer and disaster recovery/business continuity officer. And he had his team develop a strategic security plan.

Such approaches demonstrate an overarching trend in security as we head into 2007: the integration of security into all aspects of IT.

Gossels points out that companies are increasingly planning security reviews, application vulnerability testing and penetration testing as part of their regular operations, budgeting for them as they do for other fixed costs, such as electricity.

Despite the tighter IT budgets expected for 2007, Mackey says he sees companies spending more money on security, although it’s often listed with other items and not necessarily tallied together under one line item. It’s an accounting practice that reflects how security is becoming integrated as part of other processes, such as new application development.

“Folks are starting to realize they have to take a business approach to security,” Laliberte says.

Consider what’s happening at ChoicePoint Inc., an Atlanta-based data services provider that revamped its approach after a major breach in 2004.

“The approach companies take around security and risk management is moving beyond the idea that it’s just a technical thing to something we all have to be aware of,” says Darryl Lemecha, CIO and senior vice president of shared services at ChoicePoint.

Employees there receive ongoing training and technology tools such as automated e-mail encryption, he says. Systemwide software now helps catch security breaches, too. The company has also established a board-level privacy committee and a senior-level security advisory committee.

“You’re creating a large [security] ecosystem,” Lemecha says, adding that he believes other companies will take similar steps in the year ahead.

ChoicePoint isn’t just taking a top-level look at security, says vice president of information security Aurobindo Sundaram. He says security and privacy processes are getting embedded at much earlier levels. He points to data truncation as an example. Security workers there are cutting out unnecessary data requests from workers processing various business tasks.

“Security and privacy are evolving, and I definitely think it’s more proactive than it has been in the past. We’re now looking forward to what’s coming and what we’re going to do,” says Kimberly Van Nostern, chief information security officer at Allstate Corp.

### **Continuity Planning Redux**

Van Nostern says the Northbrook, Ill.-based insurer has taken that approach not only with security but also with disaster recovery and continuity planning. Like others, she says disaster recovery is moving from something companies think about once when putting together a plan to a process that’s much more ingrained in the enterprise.

Recent events have highlighted the need for that new thinking, she says.

“9/11 was definitely a wake-up call for everyone. And Hurricane Katrina — that was another impetus for continued diligence around business continuity planning for our enterprise,” Van Nostern says. “We now plan for the worst possible scenario.”

Take, for example, Allstate’s planning for a potential flu pandemic. Van Nostern says that even if a pandemic never occurs, the plan helps prepare the company for other potential crises. “Planning for the pandemic isn’t just planning for that; it’s planning for any scenario where your workers can’t come to work,” Van Nostern says.

For that reason, IT has learned to think about disaster recovery as more than just backup centers, she says. Planning for the pandemic has required the IT, human resources and facilities departments to work together to develop a plan that addresses technical as well as business unit issues, Van Nostern says.

Others are taking a similar approach.

Patrick Luce, deputy CIO at the Los Angeles Unified School District, is working on a new continuity plan as part of the organization's switch to a more modern ERP system.

Luce knows he has to think not only about earthquakes but also about the more routine events, such as power outages and severe weather, that can shut down part or all of his district's operations.

He also knows he has to bring in other departments as he develops this continuity plan, a lesson reinforced by experience. Luce says the district is just closing out the books on damage done during a 1991 earthquake. That process has proved the importance of bringing finance folks and other business leaders into the planning process so that they know what information they will need to best handle the crisis, such as the financial figures required when applying for government emergency relief funds.

But not all companies are at that point yet, says Michael Porier, a director in Protiviti's technology risk consulting division. He says many companies still dedicate time and resources to update their continuity plans only occasionally and if they feel that the risks warrant it.

"Right now, the challenge is taking it from a project mentality to a process mentality, because the business continuity plan has to be formalized and integrated into the business process," he says.

Porier says he expects some of that in the future. He says more mature organizations are already addressing business continuity on an ongoing basis, so as they plan infrastructure upgrades or go through mergers, they consider how they're going to sustain the organization during a crisis.

Moreover, Porier says, many companies aren't spending what they must to develop and maintain continuity plans. "Our biggest challenge is fighting complacency. Companies know the risk is there but don't want to allocate enough funds to put a robust plan in place," he adds.

"We've seen year after year more and more attention, more professionalization of the people doing the work and more resources put into this area," says Bruce Brody, vice president for information assurance at CACI International Inc., an IT and network services provider in Arlington, Va. "The awareness has grown, but we're still climbing that mountain. We're not near the top. But in 2007, we'll still see positive ascent up that mountain."

IT executive respondents ranked the top five critical technologies for their companies today:

1. Antivirus protection
2. Data security/privacy
3. Servers
4. Disaster recovery/continuity planning

## 5. Networking equipment

Source: *Computerworld's* quarterly  
[Vital Signs](#) survey, 252 respondents

*[Don't miss the rest of Forecast 2007.](#)*

*Pratt is a Computerworld contributing writer in Waltham, Mass. Contact her at [marykpratt@verizon.net](mailto:marykpratt@verizon.net).*