



ROGUE IT

With their credibility on the line and cost-cutting at fever pitch, strategic CIOs are cracking down on “ghost IT”

BY PERRY GLASSER

TWO WEEKS AFTER BRUCE GOODMAN SETTLED into his new job as CIO for Humana Inc., his bosses came to him with a problem. There was this little information technology project, see, that a business unit had independently begun—off the radar screen of the IT department—and guess what? It was spiraling out of control, millions of dollars over budget and months past its deadline. Could Goodman help? The Louisville, Ky.-based

healthcare company’s accounting department had taken it upon itself to beef up a basic billing system so it could process payments from many more customers.

But the technology wasn’t working. “They used an outside consultant to build it, and then it became a runaway project when a key person left,” Goodman recalls. And that was just the half of it. The people testing the new system had been using hypo-



thetical numbers. When fed actual customer names, addresses, dates and amounts owed by thousands of clients, the new system simply shut down. “It was designed to all the wrong specs,” Goodman says. “In the real world, it simply could not work.” To turn things around, Goodman says, he had to wrestle with a beast that was projected to take a year to develop, but ended up taking three years to fix. Meanwhile, he says, “the \$9 million budgeted for the project skyrocketed to a total cost of \$30 million” before it was all over.

Sound familiar? Humana is not alone. Many CIOs get stuck cleaning up the mess of ill-fated “ghost IT” projects—those “shadow” technology projects that result when a business unit goes off and self-finances a technology project under the radar of the CIO, and frequently without the green light, cooperation or knowledge of the rest of the company. The resulting duplicate projects, systems that won’t scale across the com-

pany and ill-designed initiatives can bleed a company white, wasting enormous amounts of time and money. In these anemic times, such underground activity is being frowned upon as never before. “It’s a different ball game now,” says Unisys vice president and CIO John Carrow. “Given the sheer cost of technology, you just can’t afford to have everybody doing their own thing anymore.”

Just ask UPS CIO Ken Lacy. He says UPS partners, on the fringes of the UPS extended enterprise, “sometimes feel there are ways to get around us in IT,” perhaps believing they can do IT projects more cheaply and quickly than Lacy’s corporate IT shop. “Somebody can say, ‘I can do this for \$150,000 when it would take Ken Lacy \$1 million to do the same job,’” he says. The trouble with that? “Most of the time,” Lacy says, “when people go out on a limb, they’ll end up spending that \$1 million they said they could save by going outside [the IT

department], and then still not have the ramp-up they need” to make the project work on a larger scale throughout the corporation. In those cases, Lacy says, he is called in to redo the project, often at many times the original dollar cost, and at the expense of time that could have been spent on other initiatives.

Blind No More

Sure, “ghost IT” isn’t a new phenomenon. During better economic times, says Chell Smith, vice president of technology services for Cap Gemini Ernst & Young, CIOs could occasionally afford to turn a blind eye to such rogue projects. In the healthcare and pharmaceutical industries, for example,

throughout the company.”

Indeed, some CIOs are finding themselves stuck between a rock and a hard place, with too few resources to meet too many demands, and without sufficient input from higher-ups, in some cases, to make the tough trade-offs required.

The result? Some CIOs tend to make high-impact decisions in a vacuum, triggering credibility problems that can snowball. “In extreme belt-tightening situations, where there is an unrealistic expectation to contain the overall cost of IT, a CIO can feel as if he or she has no choice but to effectively say ‘yes’ to everything a business unit wants—and that sets up business units to be disappointed because [there aren’t



“ ROGUE IT MAKES THE NEED FOR IT AND BUSINESS TO COOPERATE ON STRATEGY MORE IMPORTANT THAN EVER.” —Richard Nolan, Harvard Business School

where rule-breaking is thought to increase the odds of innovative breakthroughs, IT executives have often been known to look the other way.

But those days are over. In these cost-conscious times, ghost IT is being forced out of the shadows—increasingly viewed as more of an absolute no-no rather than a tolerable exercise in well-intentioned ambition. Indeed, in many companies, ghost IT is being seen as a symptom of poor technology management and a sign of chronic communication problems between IT and business units. Worst of all, some company executives interpret ghost IT as a sign the CIO has lost control of costs and technology projects. “CEOs are very dependent on the CIO to manage and explain costs, and make them transparent,” says David Mark, principal and leader of McKinsey & Co.’s North American IT management practice. Adds Bill Zollars, CEO of the Overland Park, Kan.-based freight company, Yellow Corp.: “IT decisions are strategic decisions, central to the business strategy. ‘Rogue IT’ is a sign that all is not right in the IT department, and, maybe, out of whack a bit

enough] IT resources to do all projects well,” says Bob Gold, a vice president and practice leader for strategic information technology management at Balanced Scorecard Collaborative Inc., a technology strategy consulting group. “The next time, a disappointed business unit is going to be more tempted to go it alone.”

And yet it’s precisely in skittish economic times that ghost IT threatens to haunt CIOs’ cost-cutting efforts the most, says Gold and others. In some cases, business units turn to rogue projects in desperation; “it’s a survival move,” Gold says. Adds Gartner EXP group vice president Ellen Kitzis: “The argument for ghost or guerrilla development is that some business units can’t wait for the big technology decisions to get made. Their markets are changing very rapidly, competitors are making really significant moves fast—and IT has to keep up in order to serve them better.”

To be sure, rogue IT can’t be—nor, some say, should be—stamped out completely. But how much is too much? Gartner’s Kitzis suggests CIOs work to keep such projects to a minimum if they want to keep their jobs. “You can’t let [ghost IT] happen too often.

If everything becomes guerrilla development, you get anarchy. That's where good IT governance has to come in." Rogue IT, says Harvard Business School professor Richard Nolan, "makes the need for IT and business to cooperate on strategy more important than ever."

How pervasive is rogue IT? Off-the-book spending on technology projects could amount to the equivalent of as much as 5 to 15 percent of a company's total IT budget, estimates Bobby Cameron, principal analyst at Forrester Research Inc. Even the best-run companies, he says, spend the equivalent of between 5 and 10 percent of their total IT budget on ghost IT projects. And it can get worse than that. "An auto industry OEM, for

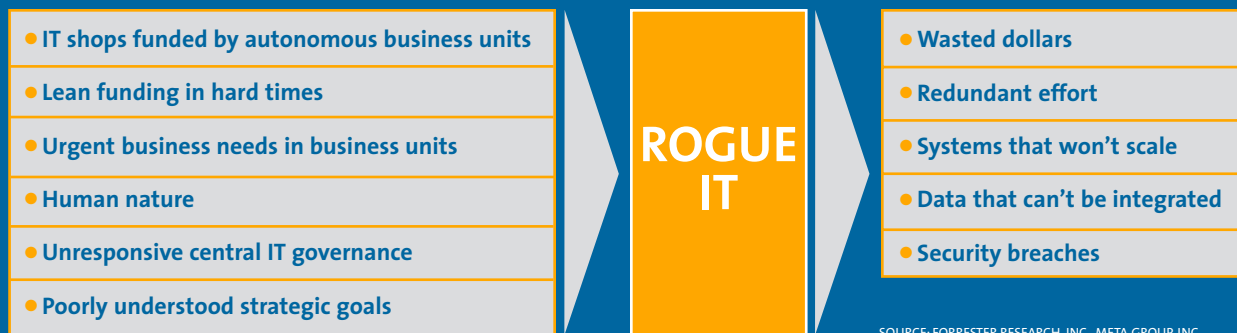
cutting costs, integrating data is an insurer's second-highest IT priority, Cecere says. Without data integration, "the company cannot present its customers with a single face." When rogue IT shops generate bad data, "bad in format and bad in truth value, it can't be rolled up and collected," Cecere says. Rogue IT may cost a company its ability to leverage whatever knowledge the rogue systems gather, and damage its relationship with customers.

Data Chaos

Rogue IT also can present technology incompatibility problems. Cecere says he recently consulted for a global media corporation that had six rogue IT projects under way,

OUT OF CONTROL

Rogue IT projects can be a symptom of poorly managed IT—and may signal a communication gap between IT and business executives that may impede strategies aimed at boosting the bottom line.



SOURCE: FORRESTER RESEARCH, INC., META GROUP, INC.

example, can run about 30 percent shadow spending," Cameron says. BSC's Gold adds that doesn't include the cost of failed rogue projects that end up in the lap of the CIO "to untangle the mess."

Giga Information Group Inc. vice president Marc Cecere, who has studied 150 IT operations, says between 100 and 150 IT people with "half again as many business people" work in the typical rogue shop at a large corporation. "That's already a few million dollars of waste right there," he says. But that's not all. Unless rogue IT projects are able to scale, they're all but useless.

Consider the insurance industry. After

each involving 10 to 30 people. The different divisions all had similar business needs—sales, marketing, procurement and so forth—but each rogue shop was devising its own technology solution. At this company, the integration of systems to track license fees and retail products was crucial to maintaining and reviving products' lifecycles, but the rogue shops made integration nearly impossible; data was chaotically distributed and stored in different projects hidden in different divisions. Cecere estimates it cost the company \$1 million for each rogue system, but many times that—perhaps as much as five times more—to fix the problem with

a successful, final integration. If that wasn't bad enough, "The rogue systems did not scale," Cecere says. "What they did was break, so add another few million dollars for repair and added maintenance."

Rogue IT also can cause a credibility gap between the CIO and the rest of the company. Cecere says rogue IT projects may fuel a perception that the corporate IT shop isn't good enough or fast enough to get the job done. Cecere recently consulted for a large finance company that had "at least two tiers of rogue shops" that gave lip service to corporate IT standards. "They were creating systems for business functions in the different units because they believed corporate IT was fiddling with silly things like architecture instead of helping run the business. 'To heck with standards, we have to get checks processed,' was the rogue shop's attitude," Cecere says.

ects often skirt around corporate best practices: In this case, a more secure VPN could have helped to keep predators out.

What to do? First, don't hide from the problem. Learn from it and start working to minimize ghost IT with new governance policies and strategies. Centralizing IT spending and security policies is one way to start. Good IT management these days, says Unisys CIO Carrow, involves "resource control. You can speed up or slow a project if you have control of your resources."

But when an organization gives discretionary funds to business units, such as sales or marketing, these groups can afford to end-run corporate IT. They might hire an outsourcer who feels no allegiance to any central IT governance, for example. Without a central IT governance group backed by senior business executives, expect business units to begin to commission independent

“ ROGUE IT SAYS ALL IS NOT RIGHT IN THE IT DEPARTMENT, AND MAYBE, [IT'S] OUT OF WHACK A BIT THROUGHOUT THE COMPANY.”

—Bill Zollars, CEO, Yellow Corp.

Besides hurting cost control and credibility, ghost IT haunts security initiatives. Ever since Sept. 11, says CGE&Y's Smith, corporate executives have been "becoming more concerned with unauthorized IT projects not under the control or accountability of the CIO, and worry that they might pose a security threat to the entire organization."

Just in case you are sleeping too well, think about how rogue 802.11 wireless LAN projects can proliferate through the corporate sales force. Cheap and convenient, a shadow-IT project taken up by a sales team could broadcast your organization's most valuable data into the local Starbucks, an open door to road warriors and rival corporations. Still not convinced? Ask Best Buy Inc.—last year, a customer stole transaction data from two of the electronics store's cash registers, taking a Wi-Fi card he had just bought inside to his car in the company's own parking lot, where he used it to crack into Best Buy's unsecured wireless LAN. Rogue IT proj-

IT projects. Putting an end to ghost IT demands strategic CIO leadership, says Gold, and a dialogue with business units seeking to go their own way, so as to help ease the risk of costly missteps later. In addition, CIOs who can negotiate for more power over the purse strings—as well as a seat at the executive table—are finding their efforts can help limit runaway projects.

More Leadership Required

Trouble is, not all CIOs are up to the job—or think they are not, though many of them know that leadership is more important than ever. In February's *CIO Insight* survey, on the CIO role, 43 percent of top IT executives said leadership ability is the most important personal attribute required for success in their current position—an indication, respondents said, of just how tough a year it's been. In last year's survey, "business understanding" was named the CIO's most important personal attribute.

The February 2003 survey also cited “cost and budget pressures” as the top concern that “frustrates” IT executives most about their jobs: 78 percent of top IT executives said the CIO’s job was more difficult this past year than previously.

What does leadership mean in this case? Telling higher-ups they simply can’t have the technology-powered business strategies they’ve ordered without providing the funds required to get them—or, if cuts must be made, then asking business executives to help make the tough IT-business trade-offs that let a company downsize effectively and still execute strategy. “Accountability needs to be set up, and shared,” says Kitzis. “CIOs can’t do it alone—nor should they.”

Gold goes so far as to suggest organizations that allow CIOs to make tough spending cuts on their own are giving CIOs too much power. Such decisions, he says, need to be made in tandem with top-level business executives. “IT decisions are inseparable from business decisions,” says Gold. Yet today, especially in tough times, CIOs are being put in the position of deciding who wins and who loses in the race for scarce resources, he says. “Let’s say you have three business units—A, B and C—and each one has a business strategy that requires 40 units of IT resources to accomplish,” Gold says. “The IT organization has only 100 units of resources to dole out. The aggregate demand on the IT organizations equals 120—20 units more than IT has to give.”

So what happens? Who should decide which of the three business units gets the most funding and which one takes the most cuts? “If the organization says it wants all three of those business strategies to be executed, and all three of those strategies require IT, then all of a sudden the CIO may explicitly or implicitly be in the uncomfortable position of having to pick and choose and make a decision about which is the most appropriate business strategy,” Gold explains. “The CIO is, in fact, being empowered to make a decision alone that should be made jointly with the enterprise-level

executives.” Gold says this situation often “creates a political minefield for CIOs. There’s no political cover for him or her to say ‘No, I’m not going to fund your project.’”

Learning Opportunity

Susan Weiner, who covers Web governance strategies for Giga Information Group, suggests that a smart CIO might do well to view the ghost IT subculture at his or her organization as a “learning opportunity” to find out where the IT organization is perceived as falling short. This gives the CIO a chance to “find out what’s broken and take back control,” she says. Weiner suggests CIOs might ask: What problem is the ghost IT project solving? What barrier is being eliminated by doing it as a rogue project? What organizational processes are in the way of going through normal channels to get it done?

In addition, Gartner’s Kitzis says, CIOs should not wait for help to fall into their laps. CIOs facing tough spending decisions should start inviting business input—and finding ways to share decision-making across the company. “There are wise CIOs and there are bumlbers,” says Kitzis. “The bumlbers, the disconnected ones who rarely talk to the business side, are taking the biggest risk of all in this downturn because they are trying to make all the tough trade-offs in a vacuum. They’re trying to figure out how to make multiple constituencies happy and stay out of trouble and keep their jobs at the same time. But these people, in the end, will not be successful. Wise CIOs will make business leaders partners in their decisions.”

Of course, it can help a lot if the CEO is in your corner—or, even better, if you are the CEO. Yellow Corp. CEO Zollars, for example, is unusual in that he personally attends to IT governance discipline. In his company, IT is a distinct division, a business within a business. There are 10 executives, including himself, on what he calls the “One Yellow Team.” The group meets for half a day each week without fail. “That kind of continuity of leadership is needed not just in IT. But for IT, it can be critical,” says Zollars. “We avoid hand-

THE EQUIVALENT OF

5-15%

OF COMPANY
IT BUDGETS ARE
SPENT ON “GHOST
IT” PROJECTS.

SOURCE: BOBBY CAMERON, PRINCIPAL
ANALYST, FORRESTER RESEARCH, INC.


 RESOURCES

Books

Leadership

By Rudolph W. Giuliani and Ken Kurson
Hyperion/Miramax, 2002

Good to Great: Why Some Companies Make the Leap... And Others Don't

By Jim Collins
HarperBusiness, 2001

Throwing the Elephant: Zen and the Art of Managing Up

By Stanley Bing
HarperBusiness, 2002

Managing IT as an Investment: Partnering for Success

By Ken Moskowitz and Harris Kern
Prentice Hall PTR, 2002

ing strategy off to technology. That's dangerous because intentions get misinterpreted."

But even when the CEO is involved in cutting technology costs, it's not easy to negotiate changes in the way IT spending decisions are made. Unisys' Carrow recalls three challenges when he pushed to centralize IT governance at Unisys: "Business unit presidents did not want to see their IT operations gravitate to central control. IT people suddenly learned they had to walk between business units and strategic demands coming from the executive committee that set policies, standardization and processes. Our unique systems in Latin America and Africa had to be shut down and people on the ground had to readjust their work life to standard systems."

Taking Control

But Carrow made a convincing case to Unisys CEO Lawrence Weinbach, and got the backing throughout his push to be able to make the tough calls—and stick to them. The payoff? "Five years ago our IT shop had 1,300 people; now we have 850, and we are running better systems." Did this completely wipe out rogue IT at Unisys? No, Carrow acknowledges. "There is some leakage," he says. "There's always resistance because individuals want to make their marks." But the problem has diminished considerably.

At Boston-based FleetBoston Financial Corp., Joe Smialowski, vice chairman of operations and technology, remembers having to get similar buy-in from higher-ups to attack the ghost IT problem, which he said was costing the company millions of dollars, though he was unwilling to put a specific price tag on the problem. When the bank changed from a holding company intent on growth through M&A activity to a customer-service-oriented institution, data sharing became the center of CRM strategy, and ghost IT a more serious threat. In the bad old days, as legacy systems from Shawmut, Bank of New England, BankBoston and other acquisitions collided under the Fleet tent, shadow IT ran rampant.

To stop the flow of lost money, Smialow-

ski in 1999 established an Executive Tech Council, which meets three times each year and includes about 20 people who make policy, explore cooperative procurement and establish technology standards. Fleet brings in key personnel from Argentina and Brazil to participate. The Architectural Review Board, a subset of the larger group, ensures that all designs and technology make sense and can be leveraged throughout the company. FleetBoston now gets the sharing and discipline it wants. Smialowski believes it's a lot tougher to get a shadow-IT project off the ground because FleetBoston's Resource Allocation Process (RAP) requires sign-off by a centralized IT governance group. "There is no way to spend money when you have centralized control of the purse strings," Smialowski says.

At Humana, not only does CIO Bruce Goodman now control the purse strings, he employs a strict system for IT governance. After having to fix that first billing-project-gone-awry, Goodman vowed there would be no more clean-up missions under his watch.

Goodman requires that all proposed IT projects be scored based on set criteria, and must reach a specific threshold to be approved. Projects get the green light based on how well they do in a variety of formalized categories: Cost/Benefit Analysis, Strategic Alignment, Competitive Position, External Customer Impact, Negative Impact, Regulatory Requirements, and Risks to the Project. Today, he says, ghost IT has been minimized considerably. "If you've got good governance in place, you can head it off," he says.

Now, when he comes across a ghost IT project gone awry, Goodman says he asks two important questions of business managers in trouble: "You want me to do *what*? You want it *when*?" For Goodman, having the power to say "no" is the best way to convince business units not to strike out on their own—and give up the ghost, right from the start. ☺

PERRY GLASSER is a freelance business and technology writer who frequently writes for CIO Insight. Please send comments about this story to editors@cioinsight-ziffdavis.com.