



● ● ● ● By David Joachim

Projects That Defy ROI

By strict **ROI standards**, security and disaster recovery projects shouldn't get any funding because they don't **produce revenue** or cut costs. Here's how some IT shops make the case.



It's one thing for your bosses to insist on a business justification for IT projects that clearly cut costs or generate revenue. But what about those initiatives that do neither?

We're alluding to technologies that wouldn't exist in a world in which nothing went wrong. They include firewalls, intrusion-detection systems, high-availability servers and hot-backup systems. These categories defy conventional ROI analysis because on a typical day they don't produce any returns.

Management and technology consultants will tell you, though, that the benefits of any IT asset can be tracked and quantified. Take disaster recovery. You can use your own experience or industry benchmarks to determine the likelihood that your systems will be knocked out in the coming year, then take the dollar value of transactions lost during the estimated downtime to determine the potential loss, says Ken Neimo, COO at TMNG Technologies, a telecom consulting firm in Bethesda, Md. That number will tell you whether a hot-backup system is worth the expense, Neimo says.

But some IT execs don't buy into this approach. When it comes to technologies that address risk, they rely on intuition more than on any ROI calculation because, they say, the more you try to count every penny, the wilder—and less believable—the numbers become. For example, Neimo's formula assumes that every transaction attempted during a system outage is lost forever. That's not always true. In many businesses, employees and customers can wait until the systems come back up.

There's no shame in resorting to qualitative arguments now and then, says William Ellison, vice president of information systems at Medical Consultants

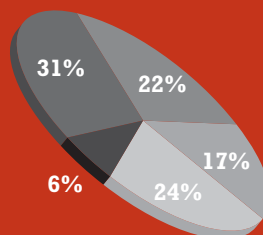
Network, a 100-employee company based in Seattle that performs medical exams for insurance companies. When Ellison joined Medical Consultants, executives were frustrated because each of the company's 13 regional offices kept a separate database to track patients. They couldn't see what the satellite offices were doing.

Ellison couldn't express in dollars the potential benefits of database consolidation—what is the benefit of management being able to run a report on where the company stands?—but his instincts told him it was the way to go. After the fact, Ellison is confident that Medical Consultants has recouped the seven-figure expense. Several new clients wouldn't have become clients were it not for his company's ability to demonstrate that it could track patients centrally, he says.

ROI analyses get especially fuzzy on security, disaster recovery and other IT projects that, in effect, require proponents to "prove a negative," says Phil Mogavero, CEO of Data Systems Worldwide, a systems integrator and outsourcer. If your network never gets broken into, you don't know for sure that you prevented an intrusion. It explains why companies tend to become inter-

E-MAIL POLL

How does your company track the ROI of IT projects?



- Formal, in the IT department
- Informal, in the IT department
- Formal, in consultation with financial management
- Informal, in consultation with financial management
- Do not track the ROI of IT projects

Source: NETWORK COMPUTING E-Mail Poll, 179 respondents

ested in intrusion detection only after their systems are compromised, Mogavero says.

It's also dangerous to think that new revenue can justify an IT project. Even after the project goes live, the results may not be measurable.

Exterior Wood, a 125-employee lumber producer in Washougal, Wash., invested about \$17,000 and 100 labor hours in a warehouse-automation system that generates labels for wrapped shipments so customers can determine

package contents without opening them. The system gets its information from a wirelessly buyers IBM AS/400.

The goal was customer satisfaction; buyers had complained the old labels weren't descriptive enough. But if someone asks IT manager Larry Miller to show a hard-dollar return on the investment, "I tell them it's not measurable," he says. "How do we know we wouldn't have gotten that phone call anyway?"

Security is different from other technology categories

Business Case: Antivirus Installation

Some business analysts contend that you can calculate the payback of security installations. Here's how ROI consultancy Alinean tallies the benefits of a antivirus software deployed in a shop with three locations supporting 2,000 workstations and 50 Windows servers.

One-Time Costs

Hardware and Software	Units	Unit Cost	Total Cost
Dedicated hardware for antivirus software	3	\$3,500	\$10,500
Antivirus server licenses	3	\$500	\$1,500
Windows server licenses	50	\$150	\$7,500
Client licenses	2,000	\$8	\$16,000
Total Hardware and Software			\$35,500
Planning and Deployment Labor	Labor Hours	Labor Rate	Total Cost
Planning	20	\$61.49	\$1,230
Procurement	8	\$39.79	\$318
Setup and installation	80	\$54.26	\$4,340
Testing	140	\$47.02	\$6,583
Deployment	100	\$54.26	\$5,426
Total Planning and Deployment			\$17,897
Professional Services	Consulting Days	Unit Cost	Total Cost
Planning	1	\$2,000	\$2,000
Setup and installation	1	\$2,000	\$2,000
Total Professional Services			\$4,000
Training	Units	Unit Cost	Total Cost
Class fees	1	\$2,500	\$2,500
Travel	1	\$1,750	\$1,750
Total Training			\$4,250
Learning and Teaching Labor	Labor Hours	Labor Rate	Total Cost
Training and independent learning	16	\$54.26	\$868
Teaching	16	\$54.26	\$868
Total Learning and Teaching			\$1,736

\$63,383

Ongoing Costs

Management and Support	Annual Labor Hours	Labor Rate	Total Cost
Systems management	12	\$54.26	\$651
Helpdesk support	43	\$39.79	\$1,724
Total			\$2,375
Three-Year Total			\$7,125
Support and Maintenance	Percentage of Software Cost	Total Annual Cost	
Year 1	0%		
Year 2	15%	\$3,750	
Year 3	15%	\$3,750	
Three-Year Total			\$7,500

\$14,625

Total Antivirus Installation Cost

\$78,008

in that companies tend to overspend out of fear, says Tari Schreider, the security practice manager at consultancy Extreme Logic. Schreider prescribes an annualized loss-expectancy model for security and disaster-recovery investments to ensure that a client's spending is commensurate with the real risk to its IT assets.

The model, which he calls reduced-risk return on investment, or RRROI, factors in which portion of your systems are vulnerable, as well as the likelihood that an outage will occur. If an IT asset is valued at \$1 million and an outage would knock out 20 percent of it, your vulnerability is \$200,000. If a devastating tornado tends to occur once every two years, your risk is \$100,000.

"So you need to spend commensurate with \$100,000 of risk rather than \$1 million," Schreider says. "No asset is 100 percent at risk 100 percent of the time."

The lesson? If you want to gain credibility with the MBA crowd, you won't score points by employing Chicken Little tactics. "IT has made a living out of scaring the hell out of the business side of the house," says TMG's Neimo. "They're like the life insurance guys who break you down by saying, 'Do you know what the statistics say about the likelihood you will get hit by a car?'"

Perhaps the best lesson comes from Rodric O'Connor, CTO at Putnam Lovell NBF Securities in San Francisco. When he wanted to sell to management the idea of consolidating five client databases to increase the efficiency of the firm's scattered sales team, O'Connor knew the productivity argument would never fly, even if he were right. "Do you say they will

be 10 percent more productive? No. You say it will help them," he says. "I wouldn't risk my reputation by putting a number on it."

So he combined his clout with that of a top sales exec who also believed in database consolidation, and he got the go-ahead—using the sales unit's money. "You can't win an argument just pitting IT against the CFO," O'Connor says. "For non-cost-cutting exercises, you need to get executive sponsorship from the unit gaining the benefit."

Still, qualitative arguments like this one don't sit well with Dale Troppito, managing partner at The Gantry Group, a consultancy that develops ROI calculators for tech vendors and IT organizations. Troppito tells clients that everything can be measured. Even e-mail, which most companies deem a cost of doing business, can be justified by quantifying avoided costs such as long-distance tolls and FedExing. "I don't think a gut feel is ever appropriate," she says.

Judge for yourself. The ROI formula for these classes of technology will vary depending on your company's goals and culture. But beware: If your ROI is too hard, you risk losing credibility by claiming to measure returns that are difficult or impossible to measure. If your ROI is too soft, hardliners will consider it mushy and overly reliant on intuition. It has to be just right.



David Joachim is NETWORK COMPUTING's editor/business technology. Write to him at djoachim@nwc.com. Post a comment or question on this story at www.nwc.com/go.ask.html.

Benefits Analysis

Virus incidents

Probability of experiencing same virus activity as typical company ¹	94%
Annual incidents expected per 2,000 PCs	20
Estimated annual incidents	18.8

Remediation labor costs for estimated annual incidents

Average remediation labor hours	40
Total annual labor hours	752
Labor rate	\$54.26
Total annual cost	\$40,804

Remediation labor savings

Total annual cost	\$40,804
Estimated savings ²	65%

Projected Savings \$26,523

Tangible Benefits

	Year 1	Year 2	Year 3	Total
Remediation labor savings	\$26,523	\$26,523	\$26,523	\$79,569
Downtime savings	\$28,639	\$28,639	\$28,639	\$85,917
Total Savings	\$55,162	\$55,162	\$55,162	\$165,486

Minus total antivirus installation cost (\$78,008)

Net Three-Year Benefit \$87,478

Source: Alinean

RemCost of downtime for estimated annual incidents

Downtime per incident (in hours)	8
Number of users affected	30
Average user labor rate	\$32.55
Total annual cost	\$146,866

Downtime savings

Annual downtime cost	\$146,866
Estimated downtime savings ²	65%
Projected downtime savings	\$95,463
Realized benefit factor (% of total downtime savings to consider for this business case) ³	30%

Benefit Realized \$28,639

¹Probability based on relative risk to this organization

²Estimate of relative effectiveness of antivirus solution

³Discount rate to adjust for continued productivity during downtime