JANUARY/FEBRUARY 2007

Quest STRATEGIC ADVISOR

www.questsys.com

Quest | CASE STUDY

Getting an army of IT expertise – on budget

"I think everyone should be doing what they're best at," says Tom Day, director of information technology at BI Nutraceuticals.

Headquartered in Long Beach, CA, BI Nutraceuticals is both small and global: this full-service supplier of dietary supplement and functional food ingredients has a reach that covers all of North America as well as the vast Asia Pacific region. The company's 160 employees depend on both sophisticated application software and networking technology to keep business humming.

"My work," Tom explains, "is concentrated on making sure that our application software, some of which is older and fragile, is working. And, of course, I'm always being asked to take on new projects. The network and backup responsibilities were, to be frank, a distraction. Quest takes care of this without me having to be distracted from what I do best."

THE BOTTOM LINE

Quest network, system, security, and backup services give BI Nutraceuticals the expertise it needs — so everyone can focus on what they do best.

"Quest respects the budget"

Today Quest is BI's primary IT resource for all network, system, and security support 24 hours a day, including backup all of BI's data for disaster recovery/business continuity. From its Network Operations Center (NOC), Quest monitors and manages BI's router/switch/server environment and its firewall/virtual private network. Quest also consults on all new IT projects and initiatives.

Tom's relationship with Quest began in early 2004 when he was struggling with BI's Exchange email server. "It just became a real pain in the neck," he recalls, "so we decided to out-task it."

He chose Quest after extensive research on service providers nationwide and an excellent working relationship followed. "The integrity of Quest's people is very important for me," Tom notes. "When Quest had the opportunity to take advantage of my situation — for example, by getting me to sign on for more than I really needed — they did *not* do it," he declares. "Quest made it clear right from the beginning that they wanted to give me the very best solution for our company: a fair solution that doesn't ask me to spend more money than I need to. Quest respects the budget."

IN THIS ISSUE

Technology solutions deliver more benefit than ever before. The cost is complexity. Today's IT requires an army of experts.

BI NUTRACEUTICALS *(Continued from p.1)*

And using Quest managed services enables budget planning. "I know what my costs will be in the coming year because they're based on a flat fee," says Tom.

Tom cites other advantages to using managed services: availability of expertise, the ability to be proactive that comes from 24/7 service, and highly responsive support.

The right expertise when it's needed

"I could not hire one person to do what Quest does for me," Tom points out. "Today's IT requires an army of experts — you need experts in operating systems, servers, switches, routers, email, Microsoft licensing, etc. That's what Quest delivers."

> **"a fair solution that doesn't ask me to spend more money than I need to. Quest respects the budget."**
>
> — Tom Day

And the flip side is that BI no longer has to pay for expertise it isn't using. "When you have a full-time person and everything is going smoothly, you still have to pay for that person — and personnel are very expensive," Tom observes. "With Quest, I don't pay for highly-skilled staff unless I need it. And if I've got an emergency, Quest is right there."

24/7 services enable proactive management

Tom also likes the ability to be proactive that Quest provides him.

"Instead of finding out on Monday morning that we have an issue with one of our branch offices," he reports, "Quest will email me and call my cell over the weekend. That's been very helpful. We have branch offices in New York and New Jersey, and when those circuits go down on a Sunday, thanks to Quest I can have the problem resolved before the folks on the East Coast begin their week."

Fast, competent support on a first-name basis

Since the beginning of his relationship with Quest, Tom has gotten the support he needs.

"I find everyone at Quest to be extremely competent," he says. "If I have a day-to-day problem, I'll call the folks on Quest's support line — I think I'm on a first-name basis with almost all of them. And if I have a major problem, I call either Mike Collins, my dedicated Engagement Manager or Matthew Sick, my dedicated Tech Consultant."

Tom also likes the fact that he talks with a live person when he calls Quest's 800 number. "Quest's people are always responsive, getting back with a resolution in a few hours," he says. "Unless it's an emergency. Then Quest's response is immediate."

FROM TIM BURKE...

Prioritizing security threats can reduce costs

I was lucky enough to recently take part in a roundtable discussion of an FBI cybercrime survey. One finding stood out: those companies investing the most in protection also reported the most security-related issues.

What does this mean? Is there some way that more security actually *attracts* attacks?

Well, no - just the opposite, in fact. Companies without adequate resources devoted to security *are* being attacked — they just don't know it. The lack of a security solution isn't protecting them. The lack of information is blinding them.

Even companies who've invested — sometimes heavily — in security point solutions suffer from security information problems. In such cases, there's too much information.

That's because security point solutions' event logs make no distinction between serious problems and minor ones. The answer is, of course, to analyze these events over a specified timeframe, correlating them to a vulnerability index that prioritizes them. Thus armed, security managers have a much-improved grasp of the threats they face and where their vulnerabilities lie — and can focus their security resources accordingly, often reducing security costs.

But this takes both substantial effort and significant expertise. I strongly encourage exploration of these issues within one's own organization at any phase — whether for analysis, planning, design, implementation, operations, or optimization. For many, the most cost-effective way to do this is via an experienced, trustworthy managed security services provider.

Quest's Managed Security Services:

Custom-tailored protection you can count on

As your business increasingly relies on information technology, the security threats it faces are evolving faster than ever.

Yet there's a limit to what any organization can spend on security, regardless of accelerating infrastructure complexity, the growing sophistication of threats, and the escalating level of security-related effort and expertise you need.

Round-the-clock security — affordably

The right managed security service provider is perhaps the best way to keep technology infrastructure security affordable. Quest's Managed Security Services give you round-the-clock access to a ready-built team of security experts dedicated to protecting your networks, servers, databases, and applications.

With a portfolio of Managed Security Services designed to be custom-tailored to your enterprise, Quest assures seamless integration of all services with your existing systems, policies, and procedures — whether you opt for standalone assessments, ongoing remote or on-site monitoring, or system-specific knowledge transfers.

A security services portfolio for the whole enterprise

Quest's Incident Protection Services, all of which can be enhanced as you require, include

- *Managed Network and Host Intrusion Detection* Service, remotely monitoring network traffic 24/7,
- *Enterprise Reporting,* which provides executive and technical reporting for all platforms,
- *Event Correlation,* consolidating all your security logs into one common report,
- *Security Posture Assessment Service,* which regularly assesses the vulnerabilities of your IT infrastructure,
- *Enterprise Managed Firewall Service,* delivering cost-effective enterprise firewall protection and reporting, and
- *Quest's Security Response Team,* which instantly detects and responds to potential security breaches.

Choosing Quest's Managed Security Services means your organization gets a fortified frontline backed by the latest research, tools, and leading-edge technologies as well as dedicated knowledge and expertise focused 24/7 on your organization's security preparation, protection, detection, and incident response.

DID-YOU-KNOW?

Virus attacks still dominate cybercrime

According to the 11th annual *Computer Crime and Security Survey* conducted by the Computer Security Institute and the FBI, virus attacks are the leading cause of financial losses.

Virus attacks as well as unauthorized access to networks, lost/stolen laptops or mobile hardware, and theft of proprietary information or intellectual property account for more than 74 percent of reported financial losses, according to the survey.

A skewed view

Although the survey is anonymous, organizations remain loathe to report cybercrimes, though in the 2006 national survey the percentage of respondents reporting intrusions to law enforcement jumped to 25 percent from 20 percent in 2005.

In a similar survey conducted by the FBI in the Sacramento, CA area last summer, 81 percent of respondents reported experiencing some kind of computer security incident, and nearly 50 percent reported dealing with viruses, spyware, and computer theft.

Despite the fact that 99 percent of these respondents use both firewalls and antivirus software, 49 percent of them had been impacted by a virus attack within the previous 12 months, and 48 percent endured spyware incidents.

Coming in the next issue of *Quest Strategic Advisor:*

Case study of Redwood Trust

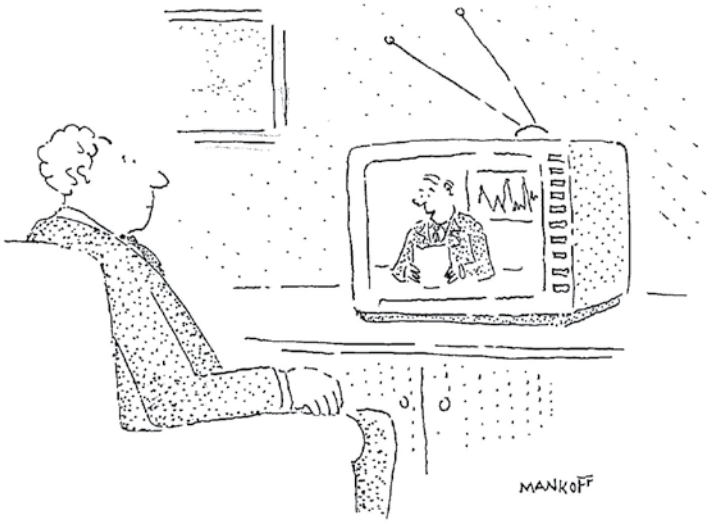
What's New...

Daylight Savings Time Extended! Are Your Systems Ready?

- This spring, Daylight Saving Time (DST) will be extended in the United States and other nations (notably Canada and Bermuda) by four weeks, beginning on the second Sunday in March and ending the first Sunday in November.

- If your business automates calendar or scheduling functions, uses date and time stamps, depends on accurate sequencing of transactions, or conducts any kind of date or time processing, chances are your software, operating systems, and/or firmware may need to be adapted. Even offshore systems supporting users, transactions, or applications interacting with those affected by the new DST rules may be impacted.

- A team of Quest experts is now available to help you both assess your technology environment for the potential repercussions of these new DST rules and to make the necessary changes to your information technology infrastructure. Don't wait until the second Monday in March to find out how the new Daylight Savings Time impacts your enterprise.



"Analysts blamed the market's volatility on computer-directed trading while computers blamed it on analyst-directed trading."

ON THE CALENDAR

Upcoming Quest Events

Master Your Disaster Lunch Briefing: Covers effective business continuity/disaster recovery plans and implementation. Santa Rosa, CA 1/25/07; Irvine, CA 1/31/07; Riverside, CA 2/1/07; Salem, OR 2/7/07, Portland, OR 2/8/07; San Diego, CA 3/1/07; Santa Barbara, CA 3/15/07.

Unified Threat Management (UTM) Lunch Briefing: Learn about rising threat levels, and vulnerability to your systems. Examines exclusive three-step review process including reports detailing appropriate recommendations. East Bay, CA 2/22/07; Fresno, CA 3/22/07.

Desktop Encryption Services Lunch Briefing: Explore encryption options for vulnerable corporate assets like laptops. Maintain control of your company's and customers' sensitive data - even if stolen. Sacramento, CA 1/24/07; Bay Area, CA 2/15/07; Reno, NV 3/8/07; Bakersfield, CA 3/21/07; Boise, ID 3/29/07. Upcoming event dates TBD: in Modesto, Redding, Santa Rosa, Riverside, Salem, Portland, Irvine, and San Diego.

Implementing Cisco Security Monitoring, Analysis and Response System - MARS v2.0
2 Day Hands-On Lab & Lecture Course:
2/12/07-2/13/07 $2295
Empowers you to identify, manage and eliminate network attacks and maintain network compliance. Prerequisites: Fundamental knowledge of implementing network security, CCSP or Security CQS and working knowledge of routing and switching.

CCNA 640-801 Bootcamp v2.3
5 Days (Extended Hours): 2/26/07-3/2/07 $3295
Focus: Enables students to pass the CCNA 640-801 exam. Prerequisites: Basic computer literacy, knowledge of fundamental networking components, terminology, and Open Systems Interconnection (OSI) reference model.

Events and dates are subject to change. Please contact Quest for registration, location, directions and all other information at 1-800-326-4220, or events@questsys.com.

Quest STRATEGIC ADVISOR

Publisher: Tim Burke
Editor: Barbara Klide

Contact the editor at
barbara_klide@questsys.com