

ZyQuest comes home

In this issue ...

ZyQuest comes home cover

Industry Watch: phretting about cybersecurity 2

Government Watch: security in the hopper 5

Consultant Watch: Sheri Gardapee 7

ZzyQuest has come home. Our new office building is complete, and we are busy settling into our new headquarters.

Designed by architectural firm Millennium Architects, the new building is located in the Ashwaubenon Business Centre, 1385 West Main Avenue, De Pere. Jacob C. Basten Construction Co., Inc., served as contractor for the project.

ZyQuest decided to build the new 13,000-square-foot structure to accommodate its growing business, according to ZyQuest president and CEO, Al Zeise. Named in *Inc.* magazine's year 2000 list of the 500 fastest growing companies in

America, ZyQuest currently employs more than 100 information technology consultants and support workers. About a quarter of those employees are expected to work in the new office building, which will house ZyQuest's



corporate offices and the Development Center, ZyQuest's in-house software development facility.

In addition to ZyQuest, the new building will provide office space for ZyTax, LLC. Originally a subsidiary of ZyQuest, the company was begun to promote *FuelTax*, the leading industry

software for calculating state and federal fuel excise tax. ZyTax was bought by the Texas-based company FuelQuest, Inc., in 1999.

The new building will also house training facilities for advanced technical courses, which ZyQuest offers with its technical education partner, Binary Training, Inc.

To celebrate our new home, ZyQuest will be hosting an Open House on June 15 from 4 p.m. to 7 p.m. We invite all our consultants, clients, and friends to join us for champagne and hors d'oeuvres, tours of the building, and presentations of ZyQuest history and services.

industry watch

Phishing, pharming, phleecing... ...phretting about cybersecurity

Paranoia seems to be running rampant in the computer world these days. But is it really paranoia, or are the fears well founded? With identity theft, phishing and pharming scams, spyware, and now even the possibility that hackers could cause life-threatening damage to your car's computer system, a little paranoia may be sensible.



Computer fears have gotten so bad that a Washington Post staff writer, after reading a recent warning in *Random Access*, suggested that it might be a good idea to disconnect from the Internet, turn off your computer, and find something else to do.

The report that prompted this sense of impending doom focused on pharming, one of the latest in a phlurry of phleecing scams intended to separate you from your money. (Apparently, there is no end to the lexicon of words in which the substitution of “ph” for “f” creates terms

that give computer mavens everywhere the heebie geebies.)

What's the scam?

Phishing, also referred to as brand spoofing or carding, attempts to scam users into surrendering private information by directing them to bogus websites made to look like genuine business sites. The bogus site instructs the hapless victims to update personal information, such as Social Security and credit card numbers, passwords, and bank account numbers. Bogus email often claims to come from eBay and various large, national banks – the kind of organizations that a lot of people are likely to do business with. Phishers work on the assumption that if you send out enough bait, you're likely to catch a few people who do business with the companies named and will actually surrender their personal data.

While phishing hooks the unwary Internet user one at a time, pharming goes after whole schools of victims. According to Chris Riley, president and

CEO of Nominum, “Phishing is to pharming what a guy with a rod and reel is to a Russian trawler. Phishers have to approach their targets one by one. Pharmers can scoop up many victims in a single pass.”

Pharming works by redirecting users from legitimate commercial sites they thought they were visiting to malicious sites where their personal information will be harvested. The bogus sites usually look the same as the genuine sites, making it difficult for the unwary web surfer to tell the difference.

DNS vulnerability

So sophisticated have pharmers become, that they can hack into the domain name system (DNS), which translates web and email addresses into numerical strings. By “poisoning” the DNS, pharmers can shuttle users to bogus web sites even though the correct web name has been entered. Because of DNS's vulnerability to this type of malicious attack, many Internet experts, such as

Continued on page 4...

government watch

security in the hopper

The problem of spam, which generated so much attention and legislation in the 108th Congress, pales in comparison to identity theft, the hands-down leader in computer-related legislation for the 109th Congress.

Only in its sixth month, this Congress has already seen nearly two dozen such bills thrown into the hopper. And the Senate has held hearings on what many see as major scandals in computer security.

Why all the fuss

The first of those scandals involved one of America's biggest information brokers – ChoicePoint, a company that routinely sells the private information, such as Social Security numbers and credit histories, of millions of Americans to businesses and government agencies. (Senator Paul Sarbanes of Maryland called ChoicePoint the “world’s largest private intelligence operation.”) In mid-February, ChoicePoint admitted that identity thieves had gained access to the information files on

upwards of 145,000 people.

In the second major debacle, which came close on the heels of the first, Bank of America lost digital tapes containing credit card account records of 1.2 million federal employees – including 60 U.S. senators. Small wonder that the Senate Banking Committee convened hearings to rip into Bank of America, whose loss was the result of transmitting the data tapes on a commercial airline flight.

Speaking at that hearing, Senator Patrick Leahy of Vermont questioned that apparently routine method of transmitting data tapes, saying that the airline industry’s propensity for losing luggage hardly gives one faith in the security of airline holds. And while the bank issued an apology, Leahy was not satisfied. Leading the call for a Senate inquiry into the need for more government regulation of data brokerage, Leahy stated, “I hope this latest incident at least will bring the issue closer to home so Congress will pay better

attention to the rapid erosion of privacy rights that ordinary Americans are facing as more and more of their personal and financial information is collected and sold on databases that too often have too few privacy protections.”

While the ChoicePoint and Bank of America security breaches made big headlines, smaller cases of identity theft in less high profile companies are occurring at an increasing rate. One of these breaches occurred recently at Lexis Nexis, which admitted that intruders had gained illegal access to information on 32,000 U.S. citizens. Overall, the FTC estimates that 10 million Americans were victims of identity theft between 2002 and 2003.

And private businesses are not the only vulnerable



cybersecurity ...Continued from page 2

“Phishing is to
pharming what a
guy with a rod
and reel is to a
Russian trawler.

~~ Chris Riley

Paul Mockapetris, who helped design the DNS, say it's time to overhaul the system.

Realistic solutions?

Another solution to the problem is to have browsers authenticate website identities. Netcraft, for example, offers a toolbar that displays the physical location of a website's host. How does that help? Well, if you're about to make a bank transaction and you notice your local bank is hosted in Russia, you'd think twice – and probably make a phone call or two to authenticate the site – before entering your name and password.

An even easier solution to pharming and phishing scams? It may sound quaint, but how about an old-fashioned, land-line telephone. Some banks are already experimenting with telephone call-backs to confirm that a transaction is about to take place. Of course, telephone authentication is useless if your only phone operates through your computer.

Right to privacy

Still aren't reassured? Maybe you shouldn't be. Because even if you turn off your personal

computer, even if you don't own a computer and wouldn't know how to surf the net if your life depended on it, you could be a target for identity fraud. If you've ever used a credit card, bought a house, gotten married, seen a doctor, taken out a car loan, paid income taxes, gone to college, or gotten a driver's license, data banks have a detailed file on you. And for a fee, they'll hand that information over to what they assume are legitimate businesses. But not always.

Case in point, the recent ChoicePoint scandal. An information broker, ChoicePoint compiles data on millions of Americans and sells that data to businesses and government agencies. Earlier this year, ChoicePoint admitted selling data on some 145,000 people to criminals posing as legitimate businesses.

Deadly hacking

The question of why even legitimate businesses should have access to your personal information aside, the problem of computer security – or lack thereof – may soon become a life and death matter. According to a recent rumor, a computer virus

had infected Lexus cars and SUVs. While the rumor was promptly denied by Lexus, the possibility of a virus running rampant in your car's computer, which controls such critical systems as air bags, transmission, anti-skid systems, steering, and throttle, gives one more than a little pause.

Turning back the clock

So now are you ready to trade in your late-model sedan for a Ford Pinto or an AMC Gremlin or a Chevy Vega? You can have them to drive to the bank where you will fill out a piece of paper that you hand to a human teller to make a deposit or withdrawal.

But if you're not quite ready for such drastic measures, take heart. Some experts say DNS poisoning is not a major issue, and car makers, aware of the virus potential, are already taking steps to prevent it. In the meantime, you can do a lot for yourself by authenticating websites, strengthening firewalls, maintaining up-to-date anti-spyware and anti-virus software, and being alert to phishing and pharming scams.

employee watch

Sheri Gardapee

What do you get when you combine a restaurateur, a landscape architect, a home remodeler, and a photographer? A computer programmer, of course. Sheri Gardapee, to be exact.

Like many of the best IT professionals, Sheri has an inventive imagination and is attracted to projects that allow her to solve problems and create elegant solutions, whether at the stove, in the garden, or on the computer.

Square one

Sheri started her IT training at the age of 27 when she enrolled at NWTTC. At that time, the program focused on mainframes, although Sheri was exposed to some smaller applications in business classes. And while Sheri admits that her primary skills are still on the mainframe, she has worked with many smaller, PC-based tools such as Access, Sequel Server, and Unix.

ZyQuest has been quick to exploit Sheri's ability to jump platforms. That's not

always the case for some consultants and some consulting companies. Sheri explained that consulting can be somewhat rigid, because clients often have very specific needs, and the consultant has to meet the required skill set. She commented, "However, I guess if you've proven you have initiative or determination to learn, and you've just got those general skills, you're more likely to be put into a different type environment. For example, at Shopko, because I had a retail background, they were willing to let me work with Unix even though I had never worked with it before. Then I worked with Visual Basic for six years for Boscovs. And I got that opportunity because I knew the system background."

Not just a man's world

Sheri's willingness to take on a challenge is also typical of the best IT consultants. And being a woman hasn't slowed her down, even in a field still dominated by men. Sheri herself has never found that being a woman is a drawback to her career,

especially in a company such as ZyQuest that has always actively encouraged women when it comes to hiring, promotion, and compensation. In fact, ZyQuest beats the national average for hiring women IT workers.

Nevertheless, Sheri recognizes that women don't routinely choose to enter the field of Information Technology. She speculated that the problem may be that "guys are just conditioned for computer work because they spend so much time with video games and related activities. So it's possible that woman feel they can't compete." Sheri also agreed that young women may be put off by what they see as a "nerd factor" associated with computer programming. Sheri admitted that her two teenage daughters, neither of whom has any interest in IT, probably think in those terms.



Sheri Gardapee

security in the hopper ...Continued from page 3

“The federal government is largely failing in its responsibility to protect the nation from cyberthreats.

~~ Edward Lazowska

targets. A recent audit of IRS workers found that a third of managers and employees – people who handle your taxes and have access to your personal financial data – contacted by Treasury Department inspectors posing as computer technicians provided their computer login and changed their password.

The solution?

What is Congress doing? What Congress always does – introduce legislation. One of the most sweeping pieces of legislation, expected to be introduced any day now, is Senator Jon Corzine’s “Identity Theft and Victim Recovery Act”. Unveiled during Senate hearings on ID theft, the bill aims to prevent future cases of identity theft or other losses of personal financial information. The bill’s major provisions are:

- 1. establishing the FTC as the oversight agency;
- 2. requiring a company’s chief compliance officer or

- chief executive officer to personally attest that the firm’s information security safeguard systems are in compliance with federal standards;
- 3. authorizing security system audits every three to five years;
- 4. authorizing penalties for compliance failures;
- 5. notifying and assisting victims of information security breaches;
- 6. requiring fraud alerts on files of any individual whose personal information may have been accessed in an unauthorized manner;
- 7. calling for studies of alternative technologies (e.g., biometrics) to enhance information security; and
- 8. authorizing federal studies of cross-country transport of sensitive personal information.

One problem that Corzine’s legislation and similar bills need to address, according to the President’s Information Technology Advisory

Committee (PITAC), is the lack of federal investment in cybersecurity research. A report from PITAC indicated that the government should be funding such research through the National Science Foundation to the tune of \$148 million annually. PITAC co-chair Edward Lazowska stated, “The federal government is largely failing in its responsibility to protect the nation from cyberthreats.”

Will it help?

Will new legislation protect Americans from the growing problem of information theft? Time will tell. One can only hope that the government does a better job of tackling the crime of ID theft than it has of curtailing spam.

For more information about federal legislation of interest to the IT community, visit the government news page of our website, www.zyquest.com.



For the latest on technology information, services, and government activities, visit the ZyQuest website at www.zyquest.com. Find out what we can do for your business while you stay on top of the rapidly changing world of information technology.

Sheri Gardapee ...Continued from page 5

Fortunately for ZyQuest, Sheri is one woman who isn't reluctant to compete in a "man's" arena. And Sheri enjoys working with ZyQuest as much as the company is glad to have her for a consultant. In describing her relationship with ZyQuest, Sheri said, I like ZyQuest. They're all pretty easy-going people and I think pretty fair and reasonable with compensation. When I started with ZyQuest eight years ago, programmers could pretty much name their price. I had a lot of offers. ZyQuest just seemed to give me the better offer." And despite

the change in the IT employment market over the last several years, Sheri believes that ZyQuest continues to provide the secure work environment and generous compensation that she values.

Life without IT?

And if she weren't working in Information Technology? "I'd probably have my own business. Something in home construction or landscaping or the restaurant business. My husband and I are big do-it-yourselfers. I think it would be fun to build a house for someone and

make money from it. I also like to do digital photography. I make slide shows for family members and parties, that sort of thing," Sheri said.

But Sheri admits that working in the IT industry would be hard to replace. "I bought about \$200 worth of books last year to learn about the restaurant business and what it would take," she said. "After reading those, I decided it was probably too much work." That's good news for ZyQuest, which needs consultants like Sheri Gardapee who can be counted on to cook up consistently good code.

*You are cordially invited
to the ZyQuest Open House*

June 15, 2005

4 o'clock p.m. ~ 7 o'clock p.m.

ZyQuest Headquarters
1385 West Main Avenue, De Pere

ZyQuest
innovation through technology

1385 West Main Avenue
De Pere, WI 54115

Staff Augmentation and
Consulting

Project Management and
Outsourcing

ZyQuest

Internet Solutions

Technical Education

To learn more about how ZyQuest can provide cutting-edge technology for your business, call us at
1-800-992-0533. Or visit our website at www.zyquest.com