

## in this issue

1

**Dell Shuts Down White-Box Channel Effort**

2

**Why Communication Is So Important When Selling To A Global Market**

•  
**Microsoft to Pit 'Metro' Format Against Adobe PDF, PostScript?**

3

**Sybase to Security Researchers: Stay Quiet or We'll Sue**

4

**Trojan Masquerades as Microsoft Security Update**

•  
**Audit Assault Grows**

## Dell Shuts Down White-Box Channel Effort

Dell has pulled the plug on a program to sell unbranded desktop PCs through channel partners. The company said customers prefer to buy the Dell brand.

But channel sources interviewed by The Channel Insider said Dell Inc. had trouble signing up VARs for the program, which kicked off in August 2002, because they don't trust Dell.

Dell, however, is positioning its departure from the unbranded-systems market as a product end-of-life issue. Dell was selling the unbranded desktop PCs, or white boxes, to resellers through its Solution Provider Direct program, but found that the solution providers would rather sell Dell-branded products, company spokesperson Roe Thiessen said.

Bill Hook, president of Keystone Computer LLC, based in Dubois, Pa., said he always viewed Dell's unbranded system initiative as a ploy to take market share away from small systems builders such as himself.

But, he said, what Dell may not have counted on is that small, locally based systems builders have nurtured long relationships with customers who trust their

recommendations and enjoy face-to-face contact.

"People that I talk to generally don't buy the Dell after they talk to me," Hook said.

Bob Parsons, president of Automated Office Solutions, based in Evansville, Ind., also stressed the importance of relationships and face-to-face contact.

"It's a lot easier to drag me into your office because the system didn't work than it is to find a mail-order guy," Parsons said. "I've been in the business for 20 years. I have earned the trust from my customers."

Thiessen, however, said Dell has plenty of face-to-face contact with customers who want it. "We have a tremendous amount of contact with SMB [small and midsized business] customers. We're the No. 1 provider of information technology to this market," she said.

Geno Marcoux, vice president and general manager of components at distributor Ingram Micro, based in Santa Ana, Calif., said manufacturers cannot compete with VARs on value, even if the manufacturer offers lower prices.

"Although a manufacturer may have the best sticker [price], there's more to end-user relationships than just pricing. Service and support, especially when it comes to total, multivendor solutions, are critical points of value that VARs deliver better than most manufacturers," Marcoux said.

He speculated that Dell didn't get enough volume with the unbranded systems and decided to reallocate resources back to the branded lines.

VARs and system builders said that even if they wanted to sell the Dell desktops, they didn't see enough profit in it. Profit margins were low on both lines of products, and the price differential between the white boxes and Dell-branded systems was negligible.

McBride said he can sell custom-built machines at margins of 15 percent to 20 percent, while the unbranded Dell PCs had margins of only about six points.

Dell's Thiessen said the company looks for channel partners who can add value beyond the cost and profit margin on the box, by building or adding software, and through services such as network installations.

# Why Communication Is So Important When Selling To A Global Market

Today it is easier than ever to start and run a global business. Our advances technology has made the world shrink into one manageable market.

You can sell your product to customers in Bangkok as easily as to costumers in Florida. All you need is a good product and the willingness to work hard for your idea.

Running a global business successfully means you have to be crystal clear in your communication. Communication is defined as sharing information with others. You have to inform the public about your business and your product. And you have to do this in such a way that people will end up buying your product.

So whether or not your business is going to succeed depends on how good you are communicating. You have to make sure your potential customers understand what you are talking about

and what your business is all about. If you want to succeed in selling your product in a foreign country you have to be aware of the cultural, politic, linguistic and social situations in your targeted country. You have to make sure your information is presented in a correct and suitable way for the foreign market.

To be able to share your information with your potential customers and prospects you have to speak their language. The best way of doing this is to actually inform them in their own language – using anecdotes and terminology they are accustomed to. This gives them a feeling of security and familiarity, and they are more likely to trust you and buy from you instead of your competitor.

Did you for instance know that in Japan the colour white represents mourning? So if you are selling party gifts to Japan make sure you don't wrap them in white paper! The examples of businesses not succeeding because of such cultural

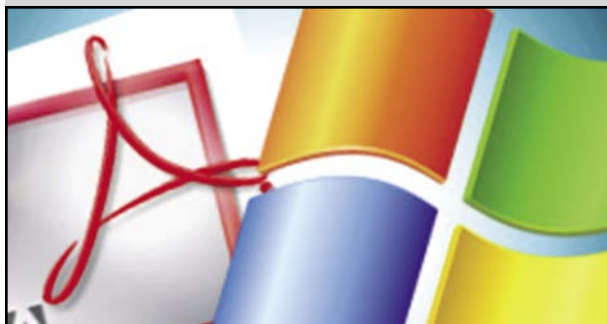
misunderstandings are many. Make sure you don't make this mistake!

This means you might have to adapt your communication strategy. The sales letter that works at home might not bring any sales in a foreign market. Have a look at your web page, your brochures, your information leaflets etc. Is this information presented in a suitable way for the foreign market?

If you fail in bringing your message across - your business will also fail. If you can't excite the people about your product – if you can't get them to trust you – you will not be making any sales.

So make sure your business will be a success and get your information ready for the foreign market!

*"If you are in need of any of these services or would like to have additional information please contact our translation division TranslationSmart at 866-442-6334 ext. 243 or email Dan Barus at [dbarus@translationsmart.com](mailto:dbarus@translationsmart.com).*



## Microsoft to Pit 'Metro' Format Against Adobe PDF, PostScript?

But now it appears that Microsoft is equating Metro with its Longhorn document-management technology.

"It sure sounds like it's meant as a PDF killer to me," said Roger Kay, an analyst with International Data Corp., who was at this week's WinHEC conference. But Microsoft officials, predictably, denied that the company is gunning for Adobe with Metro.

"One aspect of what we're addressing with Metro is fixed document format, which happens to be tied into (Longhorn's presentation subsystem) Avalon and XAML (Avalon's XML Applied Markup Language)," said Microsoft lead product manager for Windows, Greg Sullivan. With its huge installed base, "PDF is not going away," Sullivan continued. "We're solving a much narrower set of challenges for IHVs (independent hardware vendors) and

ISVs (independent software vendors." Microsoft officials told WinHEC attendees that Metro is a "new fixed document format built on top of XML" that Microsoft will make available royalty-free. Microsoft is releasing publicly the specification for Metro on Monday, officials said.

According to information from Microsoft partner Global Graphics, Metro "is an open format that allows users to share, print and archive paginated-layout documents and used in document workflows."

"As a Page Description Language (PDL), 'Metro' will offer significantly improved screen-to-print fidelity to meet knowledge worker demand for documents rich in graphics content as well as the high fidelity needs of the digital imaging marketplace," according to a Global Graphics press release.

SEATTLE—Microsoft took the wraps off a new document-workflow technology that it is readying as part of Longhorn during the Windows Hardware Engineering Conference (WinHEC) here on Monday.

Officially unveiled as part of Microsoft Chairman Bill Gates' kick-off keynote, the new Microsoft document workflow format, code-named "Metro," sounds from initial explanations like a page-description language meant to compete with Adobe's PostScript.

Microsoft has been telling partners and software vendors for some time that it was planning to include document-management functionality as a core part of Longhorn.



## Sybase to Security Researchers: Stay Quiet or We'll Sue

run on the program may not be disclosed to any third party without Sybase's prior written consent."

According to Litchfield, Sybase's letter states that, due to the license agreement clause, the company will consider it a "material breach" if NGSS publishes details on the security flaws.

Sybase is thus equating NGSS' work of finding security bugs as being the same as benchmarking and performance

testing—a unique interpretation, at least in the history of NGSS.

NGSS' working relationship with Sybase has been "excellent" up to now, Mark Litchfield said. "This is unprecedented for a vendor and for us, and we've dealt with IBM, Microsoft [Corp.], Oracle [Corp.], all the big ones," he said. "This is completely new for us."

NGSS is now seeking legal advice to see what it can and can't do, according to Mark Litchfield.

In a post to the BugTraq security mailing list Monday, the company said that, given Sybase's actions, it didn't feel comfortable publishing the full details of the research yet.

In a follow-up posting later in the day, David Litchfield said Sybase's legal maneuverings sent a bad message.

David Litchfield had written a white paper that included some instructions for exploiting the vulnerability that the worm attacked, and the worm's author appropriated some of the sample code.

Since then, the company has hewn to its policy of not releasing any details of a flaw until a fix is available. In fact, Sybase went so far as to thank NGSS for its restraint in the customer advisory the software vendor published on the ASE flaws.

"Please note that to protect the security and integrity of the existing operating

environments, NGS Software Ltd. has not published the details of the security vulnerabilities," the company wrote in its advisory.

"However, if NGS follows their stated policy, they will publish details of the issues they identified on or after March 21, 2005. Sybase Inc. appreciates the efforts of NGS to continually strengthen software throughout the industry by monitoring and testing."

Following inquiries, Sybase issued a statement saying it was "working closely" with NGSS to resolve the matter.

"Sybase constantly strives to improve the security and functionality of its software," the statement said. "Sybase appreciates the efforts of its customers and companies like NGS who occasionally find issues which are brought to Sybase's attention. The issues identified by NGS have been fixed by Sybase, and the fixes have been and are available to customers here and here.

"Sybase's primary responsibility is to ensure the security of its customers, which include Fortune 50 companies and federal government entities, including branches of military, transportation and other agencies," the statement said.

"Sybase does not object to publication of the existence of issues discovered in its products. However, the company does not believe that publication of highly specific details relating to issues is in the best interest of its customers. As such, Sybase requires that any third-party disclosure of issues discovered in Sybase products be done in accordance with the terms of the applicable Sybase product license. Sybase has been working closely with NGS to resolve this matter."

This all likely amounts to pressure from Sybase's customer base, Mark Litchfield said, which flooded Sybase's support lines following NGSS' initial filing of its report on the flaws. "It's probably pressure from the client base," he said. "Most [of Sybase's] money comes out of Wall Street."

**S**ybase has threatened legal action against a security research firm if it releases details of vulnerabilities it found last year in Sybase's Adaptive Server Enterprise product, even though Sybase already has issued patches for the flaws.

NGS Software Ltd. found eight buffer-overflow and denial-of-service vulnerabilities in Sybase ASE 12.5.3 in 2004 and subsequently notified the company of the problems. Sybase Inc., based in Dublin, Calif., released an updated version of the software earlier this year and alerted customers that they should upgrade to the latest version.

NGSS, based in Surrey, England, follows a self-imposed policy of not releasing specific details of any vulnerabilities it finds until after a vendor has either fixed the problem or has had ample time to do so and has decided not to release a patch, usually three months.

The company had planned to release the details of the Sybase flaws on Monday, but that idea was scuttled when NGSS received a letter from Sybase's legal department informing NGSS that it would be subject to legal action if the company went ahead with its plans to publish the details.

David Litchfield, a research scientist and one of the founders of NGSS, told eWEEK.com that the crux of the matter involves the license agreement for the Developer Edition of Sybase ASE, which reads, in part: "Results of benchmark or other performance tests

# Trojan Masquerades as Microsoft Security Update

Anti-virus vendors have raised the alarm for a malicious new Trojan masquerading as a critical Microsoft security patch.

The e-mail-borne attack comes just days ahead of Microsoft's scheduled patch day and highlights a growing trend of using social engineering tactics to dupe users into downloading malicious files.

According to an advisory from anti-virus specialist Sophos Inc., the attackers are using a coordinated e-mail campaign to direct users to download the bogus Microsoft patches from a malicious Web site.

Even though Microsoft never sends out updates or security alerts via e-mail, Sophos senior technology consultant Graham Cluley said the public's rising paranoia about the security of Windows computers plays into the hands of the attackers.

The e-mail includes the Microsoft Windows logo and is disguised under one of the following subject lines: "Update your Windows machine," "Urgent Windows Update" and "Important Windows Update."

It purports to come from "Windows Update" (update@microsoft.com) and includes links pointing to an "Express Install: High Priority Updates For Your Computer."

If users follow the link in the e-mail and attempt to download the fake patch, a Trojan Horse is installed instead, allowing the attacker to hijack the computer remotely.

Sophos has identified the file as Troj/DSNX-05, a backdoor Trojan that runs in the background as a server process allowing a remote user (using a client program) to gain access and control over the machine.

When first run, the Trojan copies itself to the Windows System directory using the name of a randomly chosen DLL file and a .exe extension.

Sophos warned that the Trojan then creates a registry entry to run the file automatically each time the infected machine is rebooted.

"This criminal campaign exploits the public's rising paranoia about the security of their Windows computers. If users fall for it, they may put themselves at risk of being spied upon or having their credit card and online banking details stolen," Cluley said.

He recommended that users keep up to date with the latest security patches from Microsoft, but stressed that users must be very careful to avoid downloading files received in e-mails.

"[They must make sure] they are going to the official update Web sites, rather than just following links in e-mails which have been sent by hackers," he said.

"Microsoft does not issue security warnings in this way—so users should be on their guard whenever they receive an e-mail like this," he added.

Sophos has posted disinfection instructions for the Trojan.

It's not the first time a bogus Microsoft security patch was used to trigger a worm attack.

Back in 1994, a patch promising to protect users from the MyDoom worm turned out to be a malicious virus targeting Windows machines throughout Europe and parts of North America.

That attack was also e-mail borne and arrived with a subject line of "Microsoft Alert: Please Read!"

## AUDIT ASSAULT GROWS

Tax audits are quickly on the rise. There are a number of reasons for this, not the least of which is that upon taking office, IRS Commissioner Mark Everson promised Congress that he would dramatically increase the number and scope of tax audits. The statistics indicate that Mr. Everson is achieving his goals.

The number of audits went up 11 percent from 2002 to 2003 and 25 percent since 2000. As a key element in his plan, Everson pointed the IRS's guns right at tax returns claiming income of more than \$100,000. Audits of these returns are up 40 percent from 2000 to 2003. Audits of business tax returns are up about 24 percent in 2003 alone. And correspondence audits are up about 37 percent from 2000 to 2003.

Correspondence audits are fast and cheap for the IRS to perform. The typical correspondence audit takes only a fraction of the time to complete compared to a face-to-face audit and nets the IRS, on average, about \$3,400. This is why the agency is focusing heavily on these audits.

The IRS also recently concluded 46,000 compliance exams on individuals. The results were staggering. The IRS says that the difference between what taxpayers SHOULD pay in tax and what they DO pay is about \$325 billion. IRS recovers only about \$50 billion of this via audits and other enforcement activities.

Congress has given the IRS, and Commissioner Everson, the green light to increase its audit coverage. The likely targets are:

- 1 High Income Tax Return**  
As stated previously, the IRS is targeting tax returns that exceed \$100,000 of income.
- 2 Self-Employed**  
Unreported income and over reporting of expenses, some personal, make up the largest segment of the tax gap.
- 3 Partnerships and S Corporations**  
A large portion of income doesn't seem to find its way onto the tax returns of partners and owners.
- 4 Tipped employees**  
It is estimated that billions of dollars in gratuities disappear.

The IRS has also developed a new "special formula" that sniffs out returns with potential for unreported income better than the previous formulas used in the past.

*"If you would like to have additional information please contact our financial division Premier Financial Solutions at 866-442-6334 ext. 240 or email Mike Koziol at [mkoziol@intelligentsolutions.net](mailto:mkoziol@intelligentsolutions.net).*