

LASCO POSITIONING STATEMENT

Lasco provides Information Technology (IT) solutions for small to mid-size financial institutions, businesses and organizations across the Upper Midwest. Lasco also serves as a data processing center for financial institutions providing numerous bank services to assist institutions with their day-to-day operations. For almost 40 years, Lasco has worked in an honest, ethical manner with its commitment being to assist its clients in achieving success. Lasco's client relationships are built on this commitment and trust with each of its clients.

Note from the CEO:

Dear Valued Customer:

As we begin to end 2006, we would like to share with you some of our 2007 goals:

- Convert Lasco's first non-Metavante client to the Lasco/AFS Check 21 product
- Determine the long range strategy/implementation for voice over IP
- Complete a full test of Lasco's DR center
- Convert Lasco's first document image bank client to Treeve
- Relocation of Iron Mountain facility to Marquette facility
- Begin Merchant Capture conversions

These are just a few of our goals. As always, our most important goal is to ensure that we continue open and honest communications with our current clients and our prospect clients so we may meet your needs. If you ever need to discuss a matter regarding Lasco's service level, please contact me at 800-800-6197, extension 151 or directly at 906-228-1051.

Happy Holiday Seasons – Dennis VanLandschoot, CEO



**FROM THE MANAGEMENT AND STAFF AT
LASCO**

Conversion Cost Savings

Voice over the Internet Protocol (VoIP) continues to revolutionize telecommunications by providing a cost effective and feature rich alternative to traditional phone systems. Technically, VoIP technology compresses voice (audio) data into packets that can be efficiently transmitted over data networks, the public Internet or corporate Intranets, and converted back into voice at the receiving end. This is the basic architectural change that drives integration with web-based applications and the development of new features that would be impossible using traditional technology. More importantly, companies are realizing significant cost reductions as voice becomes just another form of data. With this being the basis for change, what are the driving factors in making the decision to migrate to VoIP? Company executives are looking at three major areas for savings:

Increased Productivity: Though these soft costs are more difficult to quantify, there are real savings through increased efficiency, intuitive call handling, reduced travel to remote sites and improved contact center service through calls, e-mail and interactive web sessions.

Reduced Software, Hardware and Maintenance Costs: Because the IP process combines multiple and separate voice, data and video applications into a single network, there are savings in network consolidation and centralized call processing, desktop wiring costs, system connection expense and system maintenance and upgrade fees.

Line Optimization: A converged network, with its efficient use of communication lines, cuts the recurring expense of traditional voice services, including lower voice circuit costs and decreased long distance charges.

Lasco has the ability to bring you VoIP solutions to your business and assist you with realizing these cost savings. If you would like more information on how Lasco can assist you, please contact Dan Fezatt, Senior Vice President – Operations at 800-8000-6197, extension 157 or direct at 906-228-1075.

Direct Merchant

Direct Merchant is collection of distributed capture applications designed to allow the merchant to select one or more consumer interfaces so that the merchant has the correct solution for the merchant and the consumer.

- **DirectMerchant: Smart Deposit** operates behind the point of presentment and is designed using the Microsoft Smart Client capabilities. The solution is built for high check volume merchants or corporations. No immediate connectivity is required, allowing a fully functional capture application without internet connectivity. The system includes CAR/LAR, IQA, duplicate detection, corrections, balancing, user definable fields, and transmission.
- **DirectMerchant: WEB Deposit** is a browser based solution. A simple ActiveX device driver is downloaded to the local PC. All other features are provided by the DirectAggregator: Collector WEB server. The solution is designed for low volume users and includes CAR/LAR. IQA, duplicate testing and user definable fields that facilitate accounts receivable processing.
- **Direct Merchant: POS** is a point of presentment application that allows a small business to handle all forms of payment, including coupon capture. POS allows the customer to pay at the cash register and includes checks, credit cards, debit cards, smart cards, and cash. In addition, the solution allows the financial institution to provide their small business merchant better control over inventory and accounts receivables.

For further information on DirectMerchant solutions that Lasco can provide you, please contact Dennis VanLandschoot, President/CEO at 800-800-6197, extension 151 or direct at 906-228-1057.

ATTENTION – Charter Business Customers

Charter is offering clients currently hosted on its Negaunee server to be migrated to the newer Virginia web and mail server. The new state-of-the-art hosting platform is more efficient and reliable than the legacy hosting server. The new web interface allows more options to manage accounts online, access detailed web logs and full 24 hour support. On the new server your company may have access to additional email accounts. You will also have access to anti-spam programs to reduce junk mail, email filters to block unwanted mail and allow specific mail to be delivered. The new web hosting service supports web development in Perl, PHP, Personal CGI's, Python, FrontPage 2002 Extensions, SSI and Site Builder. There are additional features to customize the look and functionality of your website and may be available to your company for little or no cost from Charter.

If you are interested in migrating to the new Charter hosting platform please contact Renee Gleason at 906-228-1062 or email renee@lascoinc.com to see if you are eligible to move. If you have any further questions regarding your web and/or email provider please contact Lasco at 906-228-1045 or email support@lascoinc.com for additional information.

SOCIAL SITES' INSECURITY INCREASINGLY WORRISOME

Personal web spaces on MySpace, videos on YouTube, and blogs - community sites hosting user-created content - have become increasingly popular. While the web has always been about publishing digital information, the stunning popularity of hubs for content created by the audience has attracted more people to the world of quick-and-easy publishing, but the trend has some security experts worried. In November, security firm Websense alerted internet users over a handful of MySpace pages hosting videos that, when played, attempted to install adware on a viewer's system. The videos used the digital rights management facilities built into Windows Media player to start installing the software, earning the fraudster money as an affiliate of adware purveyor Zango. The incident underscores that such content should not be trusted, said Dan Hubbard, senior director for security and technology research at Websense. As more internet companies develop tools for turning their audience into the prime source of content, online fraudsters and data thieves are looking to exploit the systems to reach mainstream audiences, he said. "User created content is definitely a big security shift," Hubbard said. "I don't even think the companies have really thought about how to control things that they don't have (direct) control over." The number of incidents involving user-created content hubs is increasing. Microsoft researchers have found that a loose collection of websites, or an "exploit net", play host to malicious content and use comment spam to attract potential victims. And social networking sites are at the centre of the storm. For example, a large number of the intermediary sites, as many as 17,000, are hosted on Google's Blogger service. The internet search giant has its eye set on services that turn visitors into content creators. With Google's \$1.6bn purchase of YouTube, the popularity of user-created content hubs will only rise. Giving the audience the tools to turn their creative energies into attractive content is a key piece of that popularity puzzle, but the sites need to weigh such decisions against the security implications, said Christopher Boyd, director of malware research at messaging security firm FaceTime Communications. "It's a huge problem," Boyd said in an email interview with SecurityFocus. "These sites rely on an anything goes approach to attract users, with pretty much everything you could think of switched on for the user to customize." And that makes the sites a potentially fertile ground for malicious coders and online fraudsters, he said. MySpace has been a favorite target. A year ago, a worm constructed using Javascript crawled through the accounts of MySpace, adding one user - "Samy" - to everyone's friends list. The social-networking site has also become popular with online fraudsters that attempt to phish for log-in credentials from unsuspecting users, said Boyd, who has written about various adware threats on his VitalSecurity blog. MySpace failed to comment on the issues after being contacted numerous times. It's not just MySpace that finds itself the focus of fraudsters, however.

Wikipedia, the online community encyclopedia, has also had to deal with such problems. The various Wikipedia sites that allow online users to add and edit content could open the door to potential malicious content, according to security experts. That's almost what happened in November when a fake site masqueraded as a German version of Wikipedia hosting an entry on a variant of the MSBlast, or Blaster, computer worm. Instead, the web page attempted to compromise visitors' machines. While neither the site nor the content had been hosted on Wikimedia's servers, the phishing scam had such polish that it fooled at least one antivirus firm. The Wikimedia Foundation, the organization that operates the Wikipedia sites, has seen the writing on the wall and taken steps to limit what users can do. "We do not allow linking from executables," said Brad Patrick, general counsel for the Wikimedia Foundation. "The intent here is that we are always providing our readers with at least one additional step between us and any malicious content." Even the virtual world of Second Life, which depends on user-created content to keep its economy going, has had to deal with virtual viruses, known as "grey goo."

For about two hours on 19 November, the company that manages Second Life, Linden Lab, scrambled to contain an outbreak of *Sonic the Hedgehog*-esque gold rings. The objects spread within a region, slowing down the servers that maintain the Second Life world, or grid. It's the third major attack since September, each time the world has been overrun with quickly reproducing digital objects that have taken hours to clear out of the system. Google, Wikimedia, and Linden Lab have all built defenses into their systems, and MySpace has hired former Microsoft investigator Hemanshu Nigam to beef up the social networking site's security. "Specific to our own products and properties, including sites which host user generated content, we work constantly to prevent people from misusing our services to distribute malicious software," Barry Schnitt, spokesman for Google, stated in an email interview. "When we become aware of an instance where this happens, we take immediate action to limit user exposure." That's good, but the companies need to attack the broad range of threats, rather than focus on, for example, child porn at the expense of malicious videos, said Websense's Hubbard. "A lot of their security is geared towards child pornography, taking down content that they don't want on their site," Hubbard said. "They need to get more savvy and build up their security teams, because we are talking about hundreds of millions of pages changing daily." And, at that rate, the risk will only likely increase, he said.

ORIGINAL ARTICLE AVAILABLE AT http://www.theregister.com/2006/12/05/social_sites_vulnerable/