West Penetone

Client name: West Penetone
Location: HQ in Quebec, Canada; offices in Carlstadt, New Jersey; Edmonton, Canada; and Wisconsin
Initial consultation: 2004 for NJ office and 2009 for HQ

Phase One: New Jersey Office
CATS met with the client at their request and implemented our four-step process:

Assessed: West Penetone is a very large commercial cleaning chemical manufacturer that is headquartered in Quebec, Canada, and has offices in Carlstadt, NJ; Edmonton, Canada; and Wisconsin. The head of the New Jersey office initially approached us because they were having a lot of problems with their IT system. They were down on a regular basis and were losing productivity and money. They had twenty computers and two servers, and were experiencing system failures and many other issues.

Recommended: We recommended revamping the entire system, stabilizing their current servers, and installing new software which included a backup system and security measures. We also recommended new T1 and voice providers.

Stabilized/Implemented: We upgraded the server, installed a backup system, implemented Windows 2003 domain with Microsoft Exchange, added MX Logic for email protection and backup, corrected the domain controllers and group policies, installed a new corporate class firewall—Sonic Wall—with a redundant Internet connection in case the first one failed, and reimaged some desktops, cleaning them all of viruses and spam. We implemented Symantec Endpoint security for antivirus protection, which is a centrally managed solution. Before, each desktop had its own copy of antivirus software, and the company had no way of knowing which ones needed updates or weren't working. With Symantic Endpoint, each workstation's antivirus protection is centrally monitored and updated. We can see the status of all the workstations at a glance. Not only did this increase virus protection significantly, but it also saved the client money on by preventing new software update purchases for each computer. We used UPS technology to ensure that they have clean power and to minimize power outages. We also supported their payroll application on their local network with ADP, allowing remote access. We developed a new corporate website that gave them a much more professional appearance on the web. We also set up a conference room with a projector that is linked to the network for use in client presentations. In addition, we set up the system for their remote office in California using VPN technology to integrate them into the main network. We set up Outlook Anywhere and Web Mail for their sales force allowing them to access their exchange mail, as well as BlackBerry Enterprise server so that their BlackBerries were synced with their mail for all contacts, calendar information and mail. We installed Corporate Copiers to be shared on their network for copying, scanning and faxing. We set up wireless technology for their warehouse. We also did license management for their Microsoft Open License Program, ensuring that they were compliant. We completed an integration of their phone system into their mail server for voicemail servers. We

set up Online Backups with a Traditional Backup for maximum data protection providing them with additional benefits. All of their power is managed with UPS protection.

Maintained: West Penetone-NJ has been under monthly contract for our Ultimate-Care support and Guardian monitoring services for the past five years. They have never had a system failure or significant problem. We serve as their single source for all of their IT needs, including handling their warranties and all new hardware and software purchases. We also maintain their Website, T1 lines and phone systems.

Client benefits: We saved the client a great deal of money through measures such as installing the central antivirus solution—where they pay for managing the server copy and subsequent updates instead of 20, and don't have any more repair costs related to virus infections and also by giving them the ability to manage the content of their Website in house, rather than paying someone. Also, they no longer incur any costs due to system failures or lose any income due to downtime. The staff is able to focus on business rather than deal with computer-related issues.

Update: For five years, the New Jersey office has operated at top performance with no major issues and no system failures. The owner of the New Jersey office is also part owner of the parent company, headquartered in Quebec, Canada. That location was encountering major problems with their computer system. Our client was so pleased with our performance at the New Jersey location, in January of 2009 he asked us to fly to Canada and fix their situation.

Phase Two: Canadian headquarters

Assessed: We spent a week at the Quebec office, evaluating the situation. They had five servers that had no warranties, cloned parts and were constantly failing, they were down a lot, the Internet connection was spotty, and they didn't have good backups. Disaster recovery was put in place but never worked properly and there was no email spam filtering. They had paid other IT companies to develop various functionalities for them in the past, but they didn't work.

Recommended: Our recommendations focused on stabilizing the system, fixing what didn't work, and adding new functionality, performance, security and reliability.

Stabilized/Implemented: We installed all new Enterprise Dell servers with Enterprise Platinum Support and Windows Server 2008, Enterprise 64-bit technology, Exchange 2007, and Terminal Services 2008. We leveraged VM ware to reduce hardware expenses, which allowed us to run nine virtual servers on three physical hardware servers. We redesigned the data center network infrastructure the proper way. Proper air flow and ventilation systems and proper locking and physical security on the data center were installed. We installed primary 10MB fiber connection and backup T1 lines with redundant Internet connection so all branches can continue working if one line goes down; all new managed Cisco switches with a GB Backbone; a corporate-class Sonic Wall firewall for proper network security throughout; MX Logic for email filtering and backup; and a combination of an online backup system and traditional tape backups for maximum data protection and security. We rebuilt their data center in Quebec and Edmonton (see photos) to look good and perform better. We installed a new rack and ensured that their power source is clean using high-powered redundant UPS technology and backed up with generator

power keeping this worldwide company up and running 24x7. We added wireless infrastructure, upgraded their domain controller, configured new group policies, and cleaned up their domain. We installed an IP KVM—keyboard video monitor—to manage all the servers through a single location, and provided end point security. We implemented Web content filtering to report, monitor and block employee Web usage. Everything we installed has additional layers of remote access support using IBoot Bar technology and Dell Drac Enterprise cards allowing us to support this 24x7 environment from our own location, around the clock.

We also implemented True Blue Disaster Recovery, which was an application they had previously paid another IT company to install, but it had never worked. Using VM ware technology and replication services, we ensured that if their primary server's hardware went down, or if there was a catastrophic failure in Quebec, we could then move their application on the fly to the Disaster Recovery Site with minimal downtime, ensuring service continuity. Additionally, we incorporated DoubleTake, which backs up their systems by taking data from the Quebec network every hour and replicating it in their Edmonton office. In this way, the servers are completely replicated in a separate location, so if the main server goes down, they will be back up with complete info within the hour, regardless of how long it takes to fix the main server. We created redundant connections from the server to the remote offices so they can keep working even if one connection fails.

We accomplished all of this in four weeks for the Quebec office and one week for the Edmonton office.

We also worked on the Wisconsin and New Jersey offices to ensure that their networks were redundant through VPN.

Maintained: All of the company's locations are now protected through our Ultimate-Care support and Guardian monitoring services. There has been no downtime and no significant issues since we implemented our recommendations.

Client benefits: Our efforts provided the company with increased network reliability and security, much better performance, and no downtime. We have saved them money by eliminating repair costs and using VM ware to reduce hardware expenditures. With a stable, smoothly running computer system to support them, they are able to focus on their business. The client is very happy.