VERTEKS CONNECTION

VERTEKS VOICE & DATA NETWORKS

AS GOOD AS GOLD

For Sunshine Air Conditioning, Inc., the 'IP' in IP telephony could stand for 'instant payoff' — thanks to Verteks Consulting.

Any business investment that pays for itself in five years is considered good. One that pays for itself in five months is pure gold.

That's the kind of return on investment Sunshine Air Conditioning, Inc. has enjoyed from its 3Com NBX IP telephony system. Verteks Consulting implemented the system to replace an aging PBX that lacked the features Sunshine Air Conditioning, Inc. needed to provide top-notch customer service and to support its growing business. Five months later, owner Candy Hoffman said without hesitation that the system had already paid for itself because it eliminated the need to hire a receptionist and cut other costs as well.

"Everybody is busy on the phone all the time. With our old phone system we had reached a point where we were going to need somebody just to direct calls," she said. "The new system has an auto-attendant option that enables customers to reach whoever they need to reach via a menu. This saved us from having to hire another person. Plus, the new system has voice mail and call forwarding capabilities that enabled us to eliminate our after-hours answering service. Between those two things it has pretty much paid for itself."

Beyond Cost Savings

Of course, Sunshine Air Conditioning, Inc. is a customer-driven firm. Providing staff with a new tool to help them better serve customers was just as important as any bottom-line benefits.

"Our builders and our customers like the new phone system better because they don't have to wait for someone to answer then wait to be transferred — they can go directly to whatever extension they want," Hoffman said. "It saves them time and saves us time as well. It has really improved productivity in the office and has reduced the stress level because when your phone rings you know it's for you. We're all extremely happy with it."

Some might argue that an automated system lacks the "personal touch," but in many ways it improves customer service. The phone system never gets sick, never goes on vacation and never sleeps.

"We provide 24-hour services to our customers. In the past, after-hours calls would sometimes get dropped by the answering service — it was a real problem," Hoffman said. "Verteks set up the new phone system to automatically call the service technician when a call comes in after hours. If he doesn't respond in five minutes it calls him back. If he still doesn't respond the system calls my service manager and if he doesn't respond it calls me. As a business owner, I guarantee my customers are taken care of in a timely manner, and this new system helps me ensure that they're given the level of service I want them to have."

Ensuring Success

Verteks Consulting shares that same dedication to customer service. The Ocala-based technology provider has extensive experience implementing and maintaining voice and data networks, and understands how vitally important technology is to small business customers.

"Verteks got us up and running on the new phone system with virtually no downtime," Hoffman said. "They had us on dual systems for awhile — they installed and tested the new system and made sure it was working properly and that we knew how to operate it, then switched over from the old system."

Verteks Consulting believes end-user training helps ensure the success of any project. The Verteks team made sure that Sunshine Air Conditioning, Inc. staff could set up

and access their voice mail and take full advantage of their 3Com IP phones. Verteks also showed Hoffman how to handle many basic configuration and administration tasks.

"Verteks came in and personally trained us and when they walked out the door, we knew how to use everything. There were no questions about it," she said. "All you have to do is move a phone to a new station and it works — anywhere there's a computer there can be a phone. We're also able to access the phone system through the Internet. So if I'm at home and there's a problem I'm able to take care of it then and there without having to come into the office."

Golden Relationship

Sunshine Air Conditioning, Inc. became associated with Verteks because the firm is a provider for the Business-Works accounting package from Sage Software. The relationship has grown over time. In addition to the phone system implementation, Verteks completed a major network upgrade for Sunshine Air Conditioning, Inc.
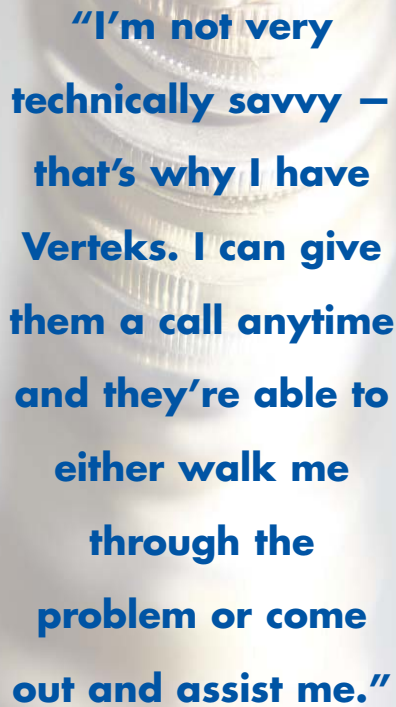
"Thanks to Verteks, we now have all the computers in the office hooked together through a server, which has saved us a lot of time and aggravation," Hoffman said.

Verteks also provides day-to-day maintenance and support, which is of vital importance since Sunshine Air Conditioning, Inc. doesn't have an IT technician on staff.

"I'm not very technically savvy — that's why I have Verteks," Hoffman said. "I can give them a call anytime and they're able to either walk me through the problem or come out and assist me. The last time they had to come out, they were here within an hour. They're also able to access my computers remotely and fix a lot of the problems from their office, in which case we're taken care of immediately."

And so you might say that the company's relationship with Verteks has paid for itself many times over. With unmatched know-how and superior service, Verteks helps customers like Sunshine Air Conditioning, Inc. strike gold with their technology investments.

> "I'm not very technically savvy — that's why I have Verteks. I can give them a call anytime and they're able to either walk me through the problem or come out and assist me."

SMBs Investing in Technology To Boost Productivity, Mobility

Communications solutions that free employees from the tethers of their desks and offices top the technology spending priorities for small and midsized businesses, according to a new survey commissioned by the Computing Technology Industry Association (CompTIA).

The survey of more than 350 small and midsized businesses across North America found that upgrades to laptop computers are the top spending priority over the next 12 months. Investment in wireless local area networks (LANs) is the number two spending priority for these businesses.

Replacement or upgrade of existing phone systems ranked third on their list of technology investments for the next year.

Among companies with fewer than 100 employees, phone system upgrades are the number two buying priority, ahead of wireless LANs and behind laptop upgrades.

When asked what factors are driving their investment in new communications solutions, 46 percent of the organizations surveyed said savings generated through streamlining business processes. Another 30 percent said cost-cutting within their information technology and communications

spending; while 23 percent said initiatives to launch new services or capabilities are the driving factor

"While the majority of businesses surveyed said their current communications systems are easy to use and can be operated and maintained at a relatively low cost, these systems are not viewed as a competitive advantage," said John Venator, president and chief executive officer, CompTIA. "Businesses reported that with their existing systems, they find it hard to manage multiple sources of communications; hard to find people when you need them; and they are relying on devices that perform insufficiently to do their jobs well. Their spending priorities center on solutions that will make their employees more productive and mobile."

Know Thy Enemy

Analysts say five types of cyber attacks will dominate in the next two years.

Gartner is advising businesses to plan for five increasingly prevalent cyber threats that have the potential to inflict significant damage on organizations during the next two years. They are targeted threats, identity theft, spyware, social engineering and viruses.

"We are seeing an increasingly hostile environment fueled by financially motivated and targeted cyber attacks. By 2008 we expect that 40 percent of organizations will be targeted by financially motivated cyber crime," said Amrit Williams, research director at Gartner. "Cyber attacks are not new, but what is changing is the motivation behind them. They are no longer just executed by hackers for hobby or cyber vandalism, but by professionals with a targeted aim at one person, one company or one industry. For example, we have recently seen several companies hiring private investigators to spy on their competitors. Private investigators used Trojans to install targeted spyware on competitors' computers to gather confidential information about such things as upcoming bids and customers."

Gartner said that social engineering and viruses will remain an everyday nuisance for chief information security officers through 2009. The research firm warned that in the next two years, at least 50 percent of organizations will experience a social engineering or a virus attack.

The Top Five

Targeted threats are financially

motivated cyber attacks aimed at one company or one industry. They lead to the exposure of customer-sensitive data, damage to corporate reputations and potential lawsuits. Gartner urged organizations to incorporate penetration testing into vulnerability management processes and investigate more aggressive intrusion detection and protection approaches that move beyond signature-based approaches. It also advised companies to evaluate managed security services when internal capabilities are not available or sufficient for advanced security activities.

Identity theft refers to the theft of an individual's personal or financial information for the purpose of stealing money or committing other types of crimes. A Gartner survey conducted in North America last year found that organizations considered identify theft to be the third-most critical security threat to their organizations. Although the number of victims has stayed relatively stable, defenses are poor and regulators, especially in the banking segment, are driving more protective measures. Gartner advised organizations to

combine fraud detection with user authentication and transaction verification to ensure that user authentication methods are matched to the risk of the transaction environment. Data must also be protected using a variety of complementary measures, including strong access controls, encryption or masking where feasible, and database activity monitoring.

Spyware is malicious software that can probe systems, reporting user behavior to an advertiser or other party without the user's knowledge. This continues to be a disruption as it can be used to send confidential information to unauthorized persons without the knowledge or consent of an e-mail user. Gartner predicts that, by 2008, 20 percent to 50 percent of organizations will experience a spyware attack. Gartner advised organizations to ask their existing desktop security vendor to provide an integrated anti-spyware solution. They should also use their gateway and network security devices to provide anti-spyware capabilities in the network, a strategy that has proved effective in the fight against viruses and spam.

Social engineering is the practice of obtaining confidential information by manipulating legitimate users. The simplest but still effective attack is to trick a user into revealing a password or other sensitive information. While this threat is well understood, it continues to be problematic because it requires human countermeasures. Defense against social engineering relies on deploying consistent security policies and practices that include educational and clear reporting programs

as well as appropriate technology management. For example, to minimize the risk of sending confidential corporate documents or trade secrets to inappropriate recipients, organizations should use content monitoring and filtering tools. To limit what a successful attacker can get access to, they should enforce the principle of least privilege when assigning access rights.

Viruses are malicious programs that use a propagation method to enable widespread distribution. Viruses are becoming more malicious and their effects could ultimately impact data or network integrity and security, e-mail privacy, and a corporation's reputation. Viruses can ultimately cause direct loss of money. Gartner said that organizations should continue to deploy signature-based antivirus software, but they should also improve patching configuration and vulnerability detection techniques to harden PCs against popular viruses. In addition, users should pressure their incumbent antivirus vendors to provide non-signature protection, or they should switch to vendors that offer this capability.

More Than a Nuisance

Williams said that organizations must not underestimate the lasting damage caused by traditional threats such as denial of service or spam, or cyber attacks that have become an everyday nuisance such as phishing.

"Phishers are now going after lesser-known brands and are starting to combine phishing and spyware attacks," he said. "Although the volume of spam has begun to level off, spam is a continuous highly visible and annoying problem for organizations. Forty percent to 70 percent of global organizations' incoming e-mail is spam, and this figure could reach 80 percent if organizations do not block spam at the gateway."

Looking ahead to the next five to ten years, Gartner highlighted "rootkits" as one of the most potentially damaging threats. A rootkit is a modified system file, such as Windows dynamic link library (DLL) or a collection of files that attackers use to replace desktop or server system files to gain undetected administrative access to the system. This enables the hacker to perform any function that a local administrator could.

"Rootkits represent an increasing threat to companies worldwide, and they are becoming more difficult to detect and prevent," Williams said. "Organizations need to be able to prevent, detect and remove infections. However, once a host has been compromised, it can be difficult to detect a rootkit as it conceals itself as a normal system file, which differentiates it from other threats."

Time for a Refresh

If your organization is supporting PCs and servers that are more than three years old, it's time to consider an upgrade.

Many organizations — particularly smaller businesses — try to squeeze every dollar of ROI out of their legacy systems, upgrading only when absolutely necessary. The concept of "if it ain't broke don't fix it" tends to rule their IT investment decisions.

Many older systems continue to do an adequate job. But there comes a time when the hard and soft costs of aging PCs and servers outweigh the cost of replacement.

First of all, there's the risk of hardware failure. Although people tend to think that computer components will last forever, they don't. Disk drives, fans and other components with moving parts have a life span of about five years. Failed hardware components can be replaced, but it's often not cost-effective to do so in light of other technical considerations. And downtime can be more costly than the equipment itself.

Legacy equipment also limits an organization's software choices, as newer applications won't run on older operating systems (OSs). When you also consider hampered productivity and security risks, the benefits of a technology refresh become clear.

The Tech Perspective

Lack of support for older OSs is a compelling reason to upgrade PCs and servers. Obsolete OSs are not supported with patches and upgrades, leaving them vulnerable to security risks. Some of these older OSs were plagued by gaping security holes anyway, making them favored targets of hackers and a serious threat to the organization.

With Windows XP, Microsoft began a process of continuous software maintenance. Security problems are addressed as soon as they are discovered, and patches distributed to IT managers and end-users as quickly as possible. This process has made the operating system much more secure. Unfortunately, it simply won't run well on many older systems.

It's not just a matter of processor speed. The latest equipment benefits from faster system buses and higher-performance memory. The latest OSs and applications were designed to take advantage of these productivity-enhancing performance gains.

A Boost for Business

Increased productivity is one of the key business reasons for upgrading PCs. Although difficult to quantify, the productivity gains can be significant. Time spent waiting for systems to boot up, applications to load and operations to complete can add up to hours of productivity lost per end-user each year.

The efficiency gains afforded by newer PCs are enhanced even further through their ability to perform many tasks in the background. The multi-tasking capabilities delivered in later versions of Windows allow users to continue to perform functions in the foreground while other functions go on behind the scenes. In general, multi-tasking is only limited by hardware constraints such as processor and memory speed.

Encryption and compression are good examples of processes ideally suited for background computing. Encryption has become essential to protect sensitive corporate data; compression helps conserve valuable bandwidth. Both require substantial processing power and time but can be executed as background processes that are invisible to the end-user given a sufficiently powerful system.

Virus scanning and client management processes can also occur as background tasks in newer equipment. Some organizations are also taking advantage of more robust desktop PCs for video distribution and other multimedia applications.

Money, Money

In addition to improving overall efficiency, upgrading PCs and servers also offers compelling financial benefits — one of those being the elimination of some of the costs associated with maintaining older systems. Newer OSs are designed to be managed remotely, and are less inclined to have problems in the first place.

Of course, the cost to the organization of a security breach or the compromise of sensitive data or intellectual property cannot be underestimated. Should an older system be used as a point of attack, the cost of that system

suddenly skyrockets. Similarly, newer systems benefit the bottom line through decreased security risk.

Although a piecemeal approach to PC replacement might seem cheaper, it's actually more cost-effective to replace groups of systems at regular intervals. New systems purchased at the same time can all be imaged with the same OS and applications, eliminating the compatibility headaches associated with older PCs running various versions of Windows and applications. With a three- or four-year refresh cycle, the IT department has only three or four possible configurations to support, reducing costs significantly and ensuring that users can share files efficiently.

Who, What, When and Why

There are, of course, cases when it's better to repair or upgrade than replace PCs — if it's a low-cost fix, or the equipment is still in warranty, for example. Some organizations also "cascade" older but still serviceable equipment to less-demanding users.

Still, many organizations have eked the last bit of usefulness out of their existing PCs and servers. It is estimated that millions of the PCs in use today are simply too old to perform the complicated processing tasks being demanded by newer applications. Only a fraction of them are powerful enough to run Microsoft's Windows XP operating system, which is quickly becoming the standard for desktop and laptop applications. Systems running OSs that are no longer maintained by Microsoft are particularly vulnerable to both hacker attack and failure.

Money is always an important consideration, and IT budgets are likely to remain tight for a while. But for those businesses with PCs and servers too old to efficiently handle today's workload or protect against the latest security threats, failure to upgrade could prove to be even more costly in the long run.