VERTEKS
CONNECTION

VERTEKS
VOICE & DATA
NETWORKS

volume 14 number 1

A STRONG RELATIONSHIP

Orlando Steel trusts Verteks to provide good advice and reliable technology solutions.

There are dozens of different metrics for evaluating the effectiveness of technology solutions. Organizations often base IT investment decisions on characteristics such as processing power, capacity, scalability, throughput, availability and more.

However, the quality that matters most to Mark Wolsefer, President of Orlando Steel Enterprises, is trust. It's why he has depended on the team at Verteks Consulting to keep his company's critical IT infrastructure current, reliable and secure for more than two decades.

"They are basically my outsourced IT department," said Wolsefer. "They are just a good, solid, honest group of people. I trust them. They have access to the deepest parts of my computer and network."

Orlando Steel manufactures and distributes a range of products that includes steel buildings, carports, corrals and fencing. The company also provides custom services such as powder coating, metal fabrication and plasma cutting. Over the years, Orlando Steel has called upon Verteks to implement a

continued on page 2

VERTEKS CONNECTION

PRSRT STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

Orlando Steel

continued from page 1

wide range of IT solutions and support its entire technology environment.

Growing Together

The relationship began when another technology group hired to set up Orlando Steel's network went out of business before the job was completed, leaving Wolsefer's company "holding the bag." After that, he decided he needed to "go to some reputable people" for his IT needs.

"We got started with Verteks and ended up redoing our servers, our networking cables and the whole thing," he said. "Our relationship just evolved from there, and now we have an ongoing service contract with them. They do all our networking stuff, they set us up with remote access for our branch location, they helped us move to VoIP phones and they help us with a lot of security-related issues."

Verteks designed its managed services offering specifically for businesses like Orlando Steel — companies that have neither the staff resources nor the desire to manage and maintain a continually evolving technology environment. Orlando Steel is a midmarket company with about 60 employees, and Wolsefer understands that the business is better off focusing on workmanship, distribution and customer service than on troubleshooting network issues.

The technology landscape is changing dramatically for small and midsize enterprises such as Orlando Steel. Just a few years ago, they might have only needed a fairly standard menu of solutions involving the maintenance of servers, desktop computers and network gear. This is changing quickly as companies of all sizes embrace cloud services, mobile platforms, data analytics and more with an eye toward increasing competitiveness, efficiency and productivity.

"I don't think I have enough IT issues to justify full-time staff, but even with a full-time guy it can be hard to keep up with how much everything changes," Wolsefer said. "If you hire a guy, you're also going to have the expense of always sending him out for more training.

"Verteks, to me, is always on the cutting edge with their knowledge. They keep up with the training and certifications, so we always have access to the latest and the greatest. That's a big factor for me."

Boosting Security

Security is one area where it is particularly important to stay ahead of the curve. Smaller businesses often believe that they are safe from network attacks because they assume cybercriminals are focused only on large, enterprise organizations.

"That's actually not true," said Wolsefer. "I am the perfect size to get attacked but Verteks helps keep me up-to-date to reduce my exposure."

A recent ransomware attack actually prompted Verteks to suggest some significant updates to Orlando Steel's security environment. Through inadvertent exposure to a piece of malware, some files on one computer were encrypted by hackers who demanded a bitcoin payment in return for the encryption key. Fortunately, nothing of exceptional value was encrypted, and Verteks was able to wipe the machine and restore it to an earlier backup.

However, the experience led Wolsefer to accept Verteks' suggestion to upgrade security with Datto Total Data Protection, a system that integrates multiple data protection, backup, recovery and business continuity processes. The Datto solution takes snapshots of data and systems at regular intervals, and stores that data in a secure location. If a ransomware attack occurs, Datto makes it easy to "turn back the clock" to a snapshot of the business before the attack happened.

Additionally, the Datto system improves data backup and recovery processes. Data is backed up automatically to a small onsite appliance then replicated to the Datto Cloud. Files can be recovered quickly with just a few mouse clicks.

A Trusted Advisor

Verteks also replaced Orlando Steel's aging firewall with a next-generation firewall from WatchGuard. Along with traditional firewall capabilities such as packet filtering, network address translation and URL blocking, the WatchGuard appliance adds more robust features such as intrusion prevention, Secure Socket Layer and Secure Shell inspection, deep-packet inspection and reputation-based malware detection.

"I've talked to Don (Gulling) and the folks at Verteks about security, and I feel like they understand how to keep me protected and limit my exposure," said Wolsefer. "I've always taken their advice, and it's always good advice."

Frequently, it is free advice, Wolsefer notes. When Hurricane Irma was bearing down on central Florida in September, he got a call from Verteks with preparation tips. Because of a likelihood of a power outage, they reminded him to unplug all computers to avoid damage from a surge when power was restored. They also suggested elevating all computer gear to keep it safe from potential floodwaters.

Verteks also made preparations to restore phones and computing at a temporary location in case Orlando Steel's offices were severely damaged. Fortunately, the company was spared significant damage, and those emergency measures weren't activated.

"They help us a lot," said Wolsefer. "They give great advice and help us deal with anything that comes up. They're just a good, good company."

News Briefs

Advanced Ransomware Targets Entire Networks

Although ransomware is typically considered an endpoint issue, information security experts warn that attackers are using more advanced techniques that target servers in an effort to take down entire networks. Unlike the vast majority attacks launched through phishing emails, these advanced tactics target unpatched servers and use them to compromise additional machines, including connected backup servers.

In a forum on these threats at the 2017 (ISC)2 Security Congress, security professionals recommended implementing the "3-2-1" method for backup, which involves having three sets of data, two different types of media, and one offsite, non-networked backup. They also said organizations must diligently scan servers for indicators of compromise such as suspicious web shells, which could be signs that attackers have already infected servers and are waiting for the right time to strike.

IoT Sparking IT Infrastructure Improvements

Organizations are planning to boost storage capacity, networking and other infrastructure to accommodate the increased data generated by Internet of Things (IoT) projects, according to a recent study by 451 Research.

The firm reports that the collection, storage, transport and analysis of IoT data is impacting all aspects of IT infrastructure from the edge to the cloud. As a result, those surveyed said that over the next 12 months they will invest in additional storage capacity (32.4 percent), network edge equipment (30.2 percent), server infrastructure (29.4 percent) and off-premises cloud infrastructure (27.2 percent).

Verteks Connection

Editorial Correspondence:
7360 E. 38th St.,
Tulsa, OK 74145
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Limiting Risk

Increasing cyberattacks underscore the value of cyber insurance.

Virtually all organizations are now dependent on technology to one degree or another, which means they are at risk of cybercrime. Given the increasing frequency and sophistication of threats, it is no surprise that there is growing interest in cyber insurance.

According to the 2017 Cyber Survey from the Risk Management Society (RIMS), 83 percent of organizations now have a standalone cyber insurance policy. Of those without a standalone cyber policy, 84 percent indicated that other insurance policies include cyber liability coverage.

"At any given moment, cyber-predators can unleash a new hack to infiltrate an organization's system, steal or lock critical data, and cause significant business interruption damages," said RIMS President Nowell Seaman. "RIMS Cyber Survey shows that risk professionals continue to invest in cyber insurance products and must work in tandem with their insurers and IT professionals to help develop innovative and adaptable solutions for the next generation of cyber threats."

SMBs Targeted

Ransomware has become especially threatening. Researchers at the University of California-San Diego recently estimated that cyber criminals have made more than $25 million over the past two years using malware that encrypts an organization's data and requires a payoff to unlock it.

On average, there were more than 4,000 ransomware attacks every day in 2016, according to figures from the Justice Department. That's a 300 percent increase over the previous year. Small to midsize businesses (SMBs) are particularly vulnerable.

That's no real surprise. Cyber crooks know SMBs don't have the security expertise or the budget of their enterprise counterparts. In fact, only 14 percent of SMBs rate their ability to mitigate cyber risk as highly effective. Too often, small businesses owners simply choose not to invest in preventive measures because they think they are too small to even be a target for ransomware. That could prove to be a seriously expensive miscalculation.

According to Osterman Research, 22 percent of SMBs that fell victim to a ransomware attack had to shut down their operations immediately. About 17 percent experienced downtime of 25 hours or more. On average, each incident cost SMBs more than $100,000 due to downtime.

Coverage Options

While cyber insurance isn't meant to supplant strong security measures, it can limit the financial damage from an incident and help organizations keep their doors open. A well-crafted policy will typically feature the following coverages:

Liability. This covers the legal fees, court judgments and other costs incurred after a cyberattack that results in financial harm to customers, partners or other third parties. This could involve the exposure of personal information or the unintentional transmission of a computer virus to another party.

Management liability. This option provides coverage for the liability risks faced individually by a company's officers, directors and key decision-makers while acting on behalf of the company.

Crisis management. This covers the cost of notifying consumers about a data breach that resulted in the release of private information, and also providing them with credit monitoring services. It could also cover the cost of retaining a public relations firm or launching an advertising campaign to rebuild a company's reputation.

Business Interruption. This covers loss of income due to an attack that causes an organization to temporarily shut down or otherwise limits its ability to conduct business.

Cyber extortion. This covers the settlement of a ransomware extortion threat.

Forensics. This covers the cost to hire computer forensics consultants to investigate the cause and scope of a breach, and to track down the source of the attack.

Data loss. This covers the loss, damage or destruction of valuable information assets.

It's also a good idea to look for an underwriter that provides threat mitigation services. This might include online training resources, best practices guidelines and risk assessments to help organizations learn how to avoid risk, along with incident response planning to help minimize the damage in the immediate aftermath of an incident.

Security threats are more complex, diverse and frequent than ever before. They require a layered defense that integrates a variety of hardware- and software-based tools, along with consistent training and education programs that reinforce the need for employee diligence. While it may not be possible to completely eliminate cybercrime, proper planning can limit the risk and a solid cyber insurance policy can minimize the financial exposure.

Data Center Building Blocks

Hyper-converged infrastructure accelerates deployments and relieves management headaches through modular approach.

The first known prefabricated house was developed by London carpenter Henry Manning in 1833 for his son who was emigrating to Australia. Based upon that prototype, Manning developed several models of various sizes and costs, advertising them as "Portable Colonial Cottages." Anyone capable of using a wrench could erect one of Manning's houses quickly and easily. That made them ideal for the British colonies, where skills and tools were in short supply.

Manning's 19th-century concept is seeing something of a renaissance in the 21st-century data center. Increasingly, organizations are implementing hyper-converged infrastructure (HCI) solutions — "prefabricated" IT systems that tightly integrate compute, storage, networking and virtualization resources along with management software. Preconfigured, tested and ready to deploy, they eliminate the need to design, implement and integrate data center infrastructure from scratch, reducing IT complexity, streamlining operations and accelerating time-to-value.

Those benefits have made HCI one of the hottest technologies on the market. Research firm IDC says the global HCI market surpassed $2.2 billion in revenue in 2016, an increase of 110 percent over 2015.

Even more impressive: a recent 451 Research survey found that HCI is currently in use at 40 percent of organizations, and analysts expect that number to rise substantially over the next two years.

"Loyalties to traditional, standalone servers are diminishing in today's IT ecosystems as managers adopt innovative technologies that eliminate multiple pain points," said Christian Perry, Research Manager at 451 Research. "Innovation inherent in hyper-converged infrastructure in particular is driving process efficiencies and agility that are increasingly tangible."

A New Architecture

In the traditional data center model, servers, storage devices and network gear are deployed and configured independently and managed manually by teams of specialists. While this approach enables organizations to leverage "best-of-breed" solutions, it creates a siloed IT environment that often becomes unsustainable as more and more boxes are added.

To relieve the complexity and bloat, vendors developed integrated infrastructure solutions with pre-integrated components certified to work together. This approach shortens deployment time, reduces risk and provides one-throat-to-choke support.

There are drawbacks, however. Integrated infrastructure solutions are built from separate hardware components, which can lead to vendor lock-in. In addition, rigid configurations can severely limit provisioning and expansion. Many integrated infrastructure products come in standard form factors with a maximum number of disks, CPUs and RAM and no way to deviate from those configurations.

HCI overcomes these limitations through a software-defined approach that collapses core storage and compute functionality into a single, highly virtualized solution. While integrated infrastructure solutions can be separated into their component parts, HCI solutions cannot. Compute and storage functions are delivered through the same x86 server resources with automated provisioning and single-pane-of-glass management.

Another distinguishing characteristic of HCI is a scale-out architecture that enables capacity to be increased by adding modules. This building-block

approach increases efficiency and helps organizations move toward a software-defined data center.

"We are seeing strong growth from products with new architectures, increased levels of automation and heavy use of software-defined technologies," said Eric Sheppard, IDC research director, Enterprise Storage & Converged Systems.

Streamlined Approach

Although server virtualization provides greater flexibility and resource utilization, the traditional "three-tier" data center architecture essentially ties applications to specific servers. Virtual machines (VMs) can be spun up and moved on demand, but changes to storage and networking often require days or even weeks. That's a major drag on operations at a time when IT departments are facing increased demands from an explosion of applications, mobile devices and cloud services.

HCI helps to resolve this dilemma through resource pooling. The entire IT stack is delivered as one shared resource pool, increasing agility and providing built-in resilience.

Because it integrates server and storage resources into one simple component, HCI offers a scalable and low-cost replacement for traditional storage-area networks and network-attached storage. Some HCI solutions also ship with integrated local backup and replication, further simplifying the environment by reducing the need for separate backup infrastructures.

Centralized management increases IT efficiency, reduces operational costs and minimizes planned downtime when performing patches and updates. Because it gives IT the ability to patch and upgrade software and manage the environment from one location, HCI is ideal for multisite operations.

The simplified management of hyper-convergence can also benefit small and midsized businesses (SMBs) with limited IT staff. A 2016 study by Techaisle found that 10 percent of small and 27 percent of midmarket companies planned to adopt HCI, and the research firm expects those numbers to increase rapidly as more SMBs become familiar with hyper-convergence.

Meeting Today's Demands

The dramatic rise of HCI isn't just changing the technological makeup of IT environments. It's also changing the personnel who manage the technology. The larger the enterprise, the more prevalent the change — 41.3 percent of very large enterprises (10,000 or more employees) surveyed by 451 Research plan to alter their IT team layouts as a result of HCI adoption.

More than one-third (35.5 percent) of enterprises say they've added more VM specialists to support their HCI environments. This is more than double the number of organizations actively adding specialists in hardware-specific areas such as servers, storage and networking.

"Today's businesses expect the same flexibility from their internal IT that a public cloud service can provide," Perry said. "[HCI is] transforming the technology that underpins today's business and the teams that manage it. As a result, we're rapidly approaching the day when the generalist-driven infrastructure administrator emerges as the key cog in business operations."

Henry Manning developed an innovative solution to meet the booming demand for colonial housing in the 19th century. HCI builds upon Manning's concept, with "prefab" data center infrastructure that accelerates deployment, simplifies the IT environment and improves agility. The ability to deliver applications and services quickly to meet changing business requirements gives HCI an important role in the modern enterprise.

SEVEN MYTHS OF HCI

Technologies as hot as hyper-converged infrastructure (HCI) often come with a lot of hype and misinformation. Gartner dispels seven of the most common myths to help organizations make more-informed buying decisions.

Myth 1: All implementations are based upon standard and open architectures. In the software-defined world of HCI, the levels of standardization and openness depend increasingly on the codebase. One vendor's management tools may not work with another vendor's hardware, for example.

Myth 2: HCI cannot meet the requirements of mission-critical applications. HCI implementations will vary widely in robustness, scalability and security. For example, some HCI clusters scale only to eight nodes, while others claim to scale to hundreds or even thousands.

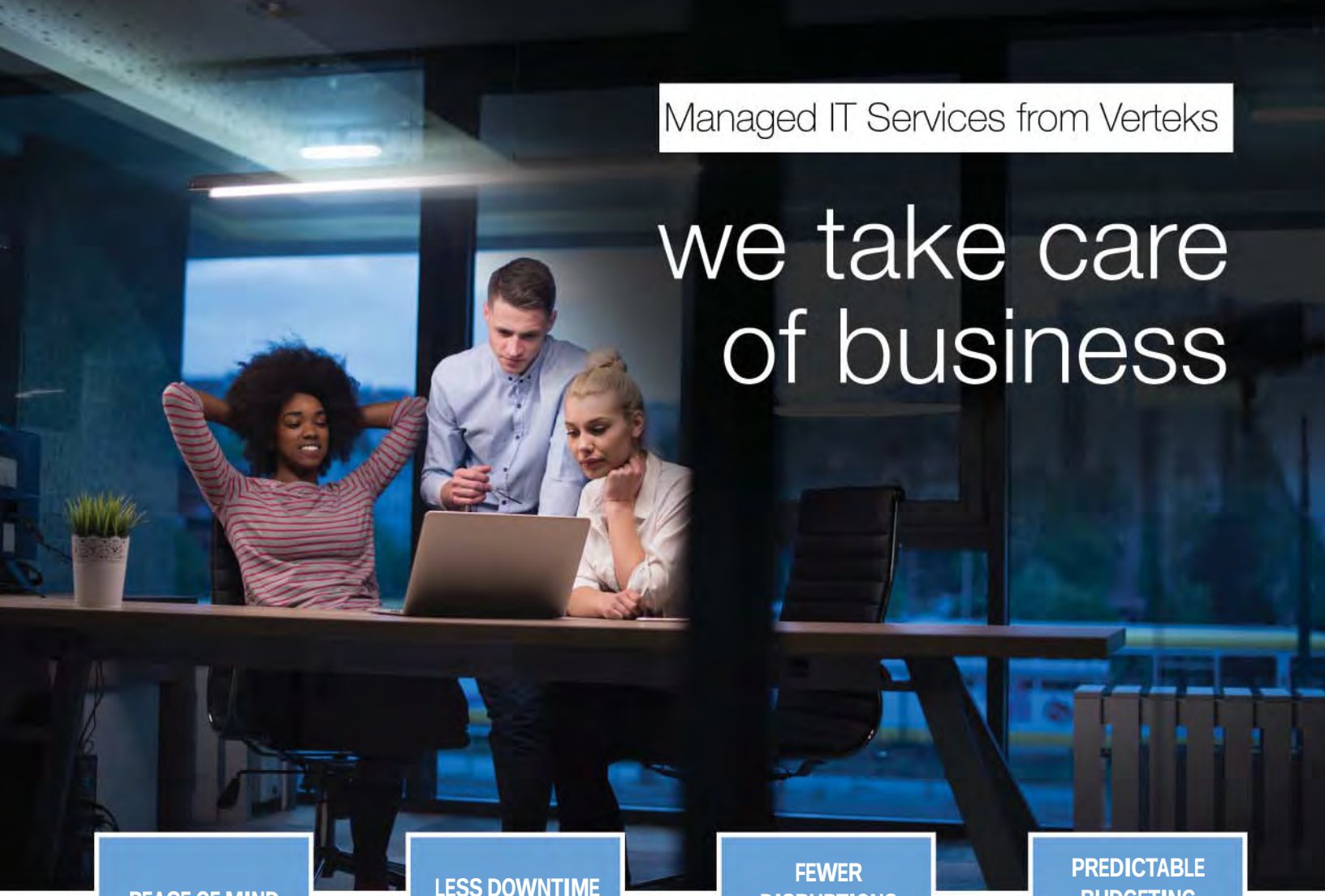
Myth 3: HCI is the least expensive deployment model. HCI can be scaled easily by adding nodes but the cost of this incremental approach can add up over time in use cases where demand increases regularly.

Myth 4: The ideal use case Is virtual desktop infrastructure (VDI). While VDI has become the "celebrity" use case for HCI, many general-purpose workloads are now a good fit.

Myth 5: HCI spells the demise of traditional storage arrays. HCI has huge potential to replace smaller, general-purpose disk arrays in highly virtualized environments. However, it may be less effective for large, mission-critical applications that require predictable behavior and proven reliability.

Myth 6: HCI eliminates data center silos. On the contrary, HCI lacks tight integration with existing traditional infrastructures, which positions it in silo deployments. HCI enables organizations to switch from hardware stack management models to simple-to-deploy virtualized platform delivery.

Myth 7: Traditional vendor selection preferences will remain the same. Many organizations are willing to look at innovative HCI solutions rather than sticking with known vendors. The commodity pricing of parts and infrastructure alleviate some of the risk of engaging with vendors that lack a solid track record.



PEACE OF MIND
Your systems are monitored 24/7

LESS DOWNTIME
We identify and fix issues before they cause problems

FEWER DISRUPTIONS
We provide most services remotely or overnight

PREDICTABLE BUDGETING
All-inclusive flat-rate IT services

With managed IT services from Verteks, we manage your technology so you can focus on your business. Our comprehensive portfolio of services includes remote monitoring and management, help desk support, and on-demand access to executive-level expertise. Our engineers and technicians perform day-to-day operational tasks to ensure that your systems are well-maintained and up-to-date. We also manage your network, security systems and backups, provide strategic planning and guidance, and serve as your liaison with third-party vendors. Give us a call and let us develop a customized managed services solution that can enable operational efficiencies, reduce risk, support new business opportunities and create a better experience for end-users.

VERTEKS
VOICE & DATA NETWORKS

1-877-VERTEKS | 352-401-0909 | www.verteks.com