BUSINESS HEALTH, PATIENT HEALTH

FIVE PRESCRIPTIONS TO STOP HEALTHCARE DISASTERS
Managed service providers that specialize in healthcare currently face some unique challenges.

For example, for most of their healthcare clients, these service providers are dealing with the following problems:

- Compliance with ever-changing healthcare IT regulations is a moving target.
- "Acceptable" downtime is zero.
- Data access is often literally a matter of life or death.

In spite of these considerable challenges, healthcare offers significant business opportunities to managed service providers who are ready for them.

Secure backup and recovery, electronic health record (EHR) systems, and multi-year data retention are key requirements of healthcare IT regulations. Major compliance deadlines are approaching in 2013 and 2014 and almost half of the physicians and smaller practices in the United States will need help meeting these IT requirements on time.

The National Center for Health Statistics reported that in 2011, 46% of U.S. physicians in office-based practices had not adopted an EHR system. In addition, the NCHS found that larger practices and physicians under age 50 were more likely to deploy EHR systems.

A Commonwealth Fund survey of doctors in 10 countries found that 69% of U.S. primary care physicians reported using EHRs in 2012. However, the U.S. lags behind Australia, the Netherlands, New Zealand, Norway, and the United Kingdom, all reporting EHR adoption rates above 90%.

Small practices in the United States are catching up. An IDC Health Insights report predicts that government financial incentives, cloud computing, and mobility will encourage 80% of small practices to adopt EHRs by 2016.
WHY MEDICAL PRACTICES NEED DISASTER RESISTANCE

In the next few years, the healthcare industry will continue to increase IT spending.

According to market analytics firm Compass Intelligence, “expenditures on U.S. healthcare IT are expected to increase from $78 billion in 2012 to $92 billion in 2016.” Fueling the growth of the healthcare IT market are government regulations that promote technology such as EHR systems and secure data storage.4

An EHR is a record of the patient’s health information that can be created and shared by all healthcare providers for that patient. It includes the patient’s demographic information, clinical notes, medications, medical history, immunizations, lab and radiology reports, digital images, and more. The storage requirements for EHRs can quickly reach hundreds of terabytes for a medical practice.

With more medical practices converting from paper to EHRs—for compliance, convenience, or cost-cutting reasons—the need for disaster resistance is growing more critical. Medical practitioners are more concerned with patient care than data care (as they probably should be), so their MSPs must provide appropriate guidance and services for disaster resistance.

Health Management Technology magazine reports:

Disaster recovery planning is quickly moving up the priority list, as healthcare organizations migrate into paperless environments. Medical imaging and electronic health records are producing unprecedented amounts of data, creating complications in storage, recovery and security.5

As a result, MSPs with expertise in both healthcare IT compliance and disaster resistance are currently in demand by medical practices going “paperless.” In 2013 and beyond, MSPs who can provide cloud storage, data security, and reliable backup/disaster recovery to healthcare clients can gain a distinct advantage over their competitors.

DISASTER RESISTANCE

At StorageCraft, we like to use the term “disaster resistance” to describe the efforts the best modern businesses take to mitigate the effects of a disaster.

In these days of Big Data and our heavy reliance on technology for even the smallest pieces of our businesses, recovery doesn’t always cut it anymore.

Downtime and data loss are only getting more expensive and many businesses are finding creative ways to set up their IT environments so that when disaster strikes, they can keep operations up and running, even as they repair damage in the background.

Today, technology is making it possible to fight back against disaster and that’s what disaster resistance is all about.
WHY TO TALK ABOUT DISASTER RESISTANCE NOW

Seven healthcare trends suggest that now is an ideal time for MSPs to discuss disaster resistance with their healthcare clients.

1. Growth of Sensitive Data
EHRs, digital imaging, and other new applications are creating enormous amounts of data—all of which must be accessed in real time across disparate sites, with their integrity and confidentiality preserved.

2. Critical Data Access
As healthcare organizations become increasingly reliant on electronic data, downtime is not an option, since the data could be critical to patient outcomes. SearchHealthIT.com reports,

   Patients’ lives may depend on systems being up and running, and patients’ health could be jeopardized by lack of access to healthcare data in the event of system downtime.6

3. Increasing Requirements
Enforcement of Health Insurance Portability and Accountability Act (HIPAA) security requirements are increasing. Section 164.308 requires data backup, disaster recovery, and emergency-mode operations planning.

4. Associates Now Included
The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 has raised the bar on HIPAA by increasing penalties, oversight, mandatory breach notifications, and the extension of obligations to business associates. Business associates (and their subcontractors) in healthcare organizations will be held to a higher standard in 2013, and the risk of non-compliance is great.

5. Incentive Deadlines
Time is running out for meeting the Meaningful Use technology requirements to qualify for CMS (Centers for Medicare & Medicaid Services) federal incentive payments. One requirement is the ability to recover electronic patient health information (ePHI) in the event of a disaster.

6. Records on Demand
Another Meaningful Use requirement is to provide patients with an electronic copy of their records upon request—and enable them to access and download their record online within four business days of it being available. System availability and disaster resistance are absolutely necessary for medical practices to meet this requirement.

7. Data Breaches
Data breaches and cyber attacks are on the rise. According to the Verizon Data Breach Investigations Report, there were 174 million compromised records in 2011, up from 4 million in 2010. In the healthcare sector, organizations experiencing breaches were in the small-to-medium business category, most of them outpatient care facilities like medical and dental offices.7
WHO NEEDS IT

More than 90% of healthcare organizations say they have suffered at least one data breach in the past two years, according to a recent Ponemon Institute survey.8

The survey also found that 45% of respondents had experienced more than five incidents.

Underscoring the need for disaster resistance in the healthcare field is another Ponemon Institute survey from 20119 that reveals:

- 55% of respondents from the healthcare sector reported low confidence in their ability to recover data following a disaster.
- 33% of healthcare sector respondents said they could not recover quickly following a disaster.
- 42% of healthcare sector respondents said they would expect substantial downtime following a disaster.

These trends point to business opportunities for MSPs who can offer disaster resistance services to their healthcare clients.

PRESCRIPTIONS FOR FIGHTING DISASTER

On the following pages, four managed service providers with 78+ years of combined experience offer five prescriptions for success with disaster resistance in the healthcare industry.

In the healthcare IT specialty, disaster resistance skills pair well with compliance skills—as these four managed service providers demonstrate.

Let's take a look.
MEET THE EXPERTS

VAN HEATH, SENIOR DISASTER RECOVERY ENGINEER, SPEROS

www.speros.com

Founded in 1984, the Speros name is synonymous with customer service and technical innovation. Speros launched their own Speros Cloud Service in 2010. Almost half of its clients are in the healthcare arena.

Van has been with Speros for more than two years. He is a Microsoft Certified Desktop Support Technician, a Microsoft Certified Professional, and a Certified StorageCraft Engineer with a true passion for disaster recovery.

DAVID SPIRE, PRESIDENT AND CEO, UNITED SYSTEMS COMPUTER GROUP

www.uscomputergroup.com

Since 2004, United Systems Computer Group has been providing IT service and support—with a 100% satisfaction guarantee—to small and mid-sized businesses. Approximately 18% of their clients are in the medical field.

David specializes in understanding the client’s business flow and the role of each server and workstation in that business. His company offers managed services, IT consulting, cloud solutions, virtualization, business continuity planning, and more.
MEET THE EXPERTS

DAVE PATEL, COO, COMPUTECH CITY
www.computechcity.com

With more than 10 years of IT experience in healthcare, Dave brings skills in network systems design, cloud computing, EHR hosting, data virtualization, datacenter operations, and storage area network (SAN) management to CompuTech City.

Established in 2002, CompuTech City serves the healthcare sector with a focus on customized and managed services, including EHR hosting and support, for more than 500 medical practices.

STEVEN SASLOW, VICE PRESIDENT, INFORMATION TECHNOLOGY GROUP
www.itgct.com

Information Technology Group has 30 years of experience in information systems consulting. Approximately 80% of their customer base is in the healthcare industry, mainly specialty providers such as cardiology and radiology practices.

A network systems engineer, Steven builds custom technology solutions designed to fit each client’s business. He helps customers plan to prevent failure, implement disaster-resistant solutions, and regularly test their solutions. His company is a leading provider of cloud and virtual desktop solutions.
When a medical practice gets a new practice management system (PMS), it often requires migrating patient records to a completely new database.

This is a time-consuming process, but after a few months, one pediatrics firm had finally finished migrating their last record to the new database. It should’ve been a moment to celebrate—but somehow, the medical practitioner had accidentally changed the security rights for the database. Now everyone in the practice was locked out. With no access to patient data, medical transcripts, prescriptions, or appointments, no one could do any work. The PMS vendor’s only solution was for the practice to send the database to them and wait for two weeks to get it back.

Fortunately, this pediatrics firm was a Speros client. Van Heath, Senior Disaster Recovery Engineer, explains:

We make backups every four hours for this client so we went back to the image from the previous four hours, mounted the image, grabbed the actual database, and put it into their existing server. We were able to get the system up and going with a relatively short amount of wait time.

In fact, the total downtime for that pediatrics firm—from the time they notified Speros—was three hours. Instead of losing months of data entry work, and two weeks of business waiting for the PMS vendor to unlock the database, the practice only had to re-create two hours of lost work.
**RX #2: REGULAR CHECKUPS SAVE BUSINESSES**

*Not testing your backups is like flying on a trapeze.*

So says David Spire, President and CEO of United Systems Computer Group.

You can see the net beneath you, but you’ve never tested it to see if it will support your weight.

David speaks from personal experience. His company gained their largest client as the result of an untested backup from another provider.

They lost an Exchange server and waited two days to get it back from the cloud. That’s when they found out their backup was corrupt. We now back up 11 servers for them.

Every 30 to 45 days, depending on the client, they generate a service ticket for a test restore.

It’s automatically generated for each client. We only get one chance to get it right if they’ve had a failure.

Regular backups and backup testing help United Systems sell their managed services.

Having good backups in place is the #1 thing we lead with in our sales efforts. We talk backup before everything, because if you don’t have your data, you don’t have your business.

In most cases, they don’t have to convince customers. They spend time looking at what the client already has in place, then describe what a good backup solution looks like.

We say, “here are the six pieces of the ideal solution—how many do you have in place today?” I’ve never found anybody that has all six.

Because of the data retention and security requirements in healthcare, one of the most popular services he sells to his medical clients is a “forever backup.”

From the day we capture the base backup, we keep making incremental backups until the end of time, or until they cancel our service. The data transfer is through an AES-encrypted tunnel to make sure remote backups are secure.

Though each client feels its needs are unique, David follows the same guidelines for all clients.

We follow best practices. Most of our healthcare and other clients are set up similarly, using best practices and standards. We’re pretty consistent in deploying our solutions. General infrastructure, backup, and security are the same across the board.

**SIX PIECES**

According to David Spire of United Systems Computer Group, the ideal backup and disaster recovery solution is made up of six pieces:

- Onsite and offsite copies
- Incremental backups
- Backups on a rotating basis
- Automated backups ("so you don’t have to trust humans")
- Verifiable backups (tested on a frequent basis)
- Restore tests every 30 to 45 days
More than 90% of CompuTech City’s clients are in the medical community and Dave Patel, COO, believes in preventive medicine for his clients:

We use a proactive care approach to managed systems. CompuTech City relies on an image-based backup and disaster recovery solution along with monitoring agents to make sure backups happen every day—and every hour. Once a month, they mount the backup images and verify that they’re restorable. While that may seem overly cautious to some, in the healthcare sector, it’s essential.

In healthcare it’s very important to have backups. The value of their medical and financial data is far more important than the cost of their hardware or software. The average physician we support bills out millions of dollars in a year.

Also important are uptime and data retention.

The healthcare industry is very diverse and complicated, with a lot of moving parts and complicated applications. Uptime requirements are very high. You can’t see patients, order prescriptions, or do anything without your electronic records.

Federal regulations require certain medical records to be preserved for seven years.

A server shelf life is three to five years. A lot of software and hardware can change during those seven years. You have to make sure the backups you take can easily convert from physical to virtual, or to a new server, so you can keep that server “alive” for seven years.

Hardware failure and software corruption aren’t the only threats to server data. One of Dave’s clients lost its only server to theft.

It was a medical practice 130 miles from our office. Thieves broke in over the weekend and when they didn’t find drugs they grabbed the most expensive item—the server—and left. Monday morning the client contacted us. As soon as the insurance and FBI finished their investigation, we overnighted a server and restored them from backup.

Because of regular backups, the client only lost a half-day of work.

Without the backups, the medical office would’ve lost all of their clinical data and their billing data forever. They would’ve lost a lot of money.

Threats

One of the basic steps of every disaster recovery plan is a threat assessment.

Of course, there are threats that endanger every business, like server failure or natural disaster, but each industry has its own specific problems as well and they may not always be obvious.

In the case of Dave Patel and his client, for example, theft was a problem and in hindsight, it makes sense. It’s probably a risk for many healthcare providers.

Because of the perception that doctors always have drugs on hand, criminals may be more likely to break into a doctor’s office than some other kind of business.

A threat assessment is not something you gloss over. In order to be truly prepared, take the time to honestly assess your own or your client’s risks and then make a plan to prevent or mitigate those risks.
Most of Information Technology Group’s healthcare clients are multi-site medical practices with anywhere from 50 to 300 endpoints.

Physicians see patients at different locations throughout the day and according to Vice President Steven Saslow, they’re generally centralized systems, with satellite offices that don’t have much hardware. All of the spokes rely on connections to the hub office.

At the hub offices and server farms where clients’ infrastructure runs, then, fault tolerance is mandatory.

Crisis scenarios don’t happen often. In the 23 years I’ve been doing this, it’s only happened twice.

Information Technology Group specializes in planning to prevent failure and implementing solutions that can be successful in case of site disaster or significant failure.

That’s why they use an image-based backup and disaster recovery solution.

Image-based is all we do. There’s no compelling reason to do file-based backups anymore. When we started to become aware of the limitations of file-based backups, we started looking at emerging technologies. Now 90% of our customers have converted to image-based.

For example, a few months ago a pediatric clinic’s primary Hyper-V host server failed.

The host had four or five virtual machines running inside of it. Their entire infrastructure was encapsulated in that one server. Because of image-based backup, we recovered the Hyper-V host in a few hours. To rebuild those virtual machines with a file-based recovery would’ve taken two days.
Federal and state regulations require healthcare clients to have backup and disaster recovery plans—as well as privacy protection—for patient information.

This makes backup and disaster recovery services an “easy sell” to the healthcare field.

But managed service providers Van, Dave, David, and Steven offer more than backup and disaster recovery services. They offer disaster resistance to their clients. Proactive planning, monitoring, and testing make their clients resistant to disasters that could destroy their data and disrupt their businesses.

Disaster resistance means their clients can sleep well at night, without worrying about their data.


At StorageCraft®, the goal of complete disaster recovery drives everything we do. Our StorageCraft® Recover-Ability™ solution is an end-to-end, best-in-class backup and disaster recovery solution that is both fast and reliable.

STORAGECRAFT RECOVER-ABILITY

It starts with a good backup. Our award-winning StorageCraft® ShadowProtect® takes complete, pristine images of your machines, including all your operating systems, applications, services, and settings. It then records changes at the sector level, so you always have an up-to-date copy of every machine in your IT environment, whether it's a critical server or an employee laptop, physical or virtual. We even work with specialized database servers, like SQL, SharePoint, or Exchange. You can get granular recovery in Exchange with ShadowProtect Granular Recovery for Exchange.

You have complete control over the frequency of your backups and you can set rules for consolidation and retention to manage your precious storage space using StorageCraft® ImageManager.

Plus, with StorageCraft® ShadowControl® CMD™ you can monitor the machines in your backup environment from a single interface and get alerts when a machine is running out of space, when a backup doesn't happen, or when any of a variety of conditions you specify is met.

We also give you tools to test your backups using StorageCraft® VirtualBoot™ and StorageCraft® Image-Ready™ technologies, which gives you confidence that your data is safe and that a disaster won't shut you down or hold you up.

Then we make it easy to replicate your backup images with StorageCraft® Cloud Services or to our cloud or to your own offsite location so you can always have your data close when you need it and at a good safe distance when a disaster comes.

When it does, you can launch your backups as virtual machines with VirtualBoot or mount them as drives for complete, granular access to your data.

Or you can pre-stage the recovery of a backup image in a virtual machine with our patented StorageCraft® HeadStart Restore® technology, so if your main server blows up, you can be up and running in minutes. You can even virtualize your data in our cloud so even Mother Nature can't keep you down.

Then, you can rebuild your infrastructure and recover to all kinds of machines, physical or virtual, using our StorageCraft Hardware® Independent Restore™ technology or ShadowProtect IT Edition.

You can't be sure what kind of disaster will strike you next, but with the StorageCraft Recover-Ability solution, you can be sure it doesn't matter. You'll be just fine.