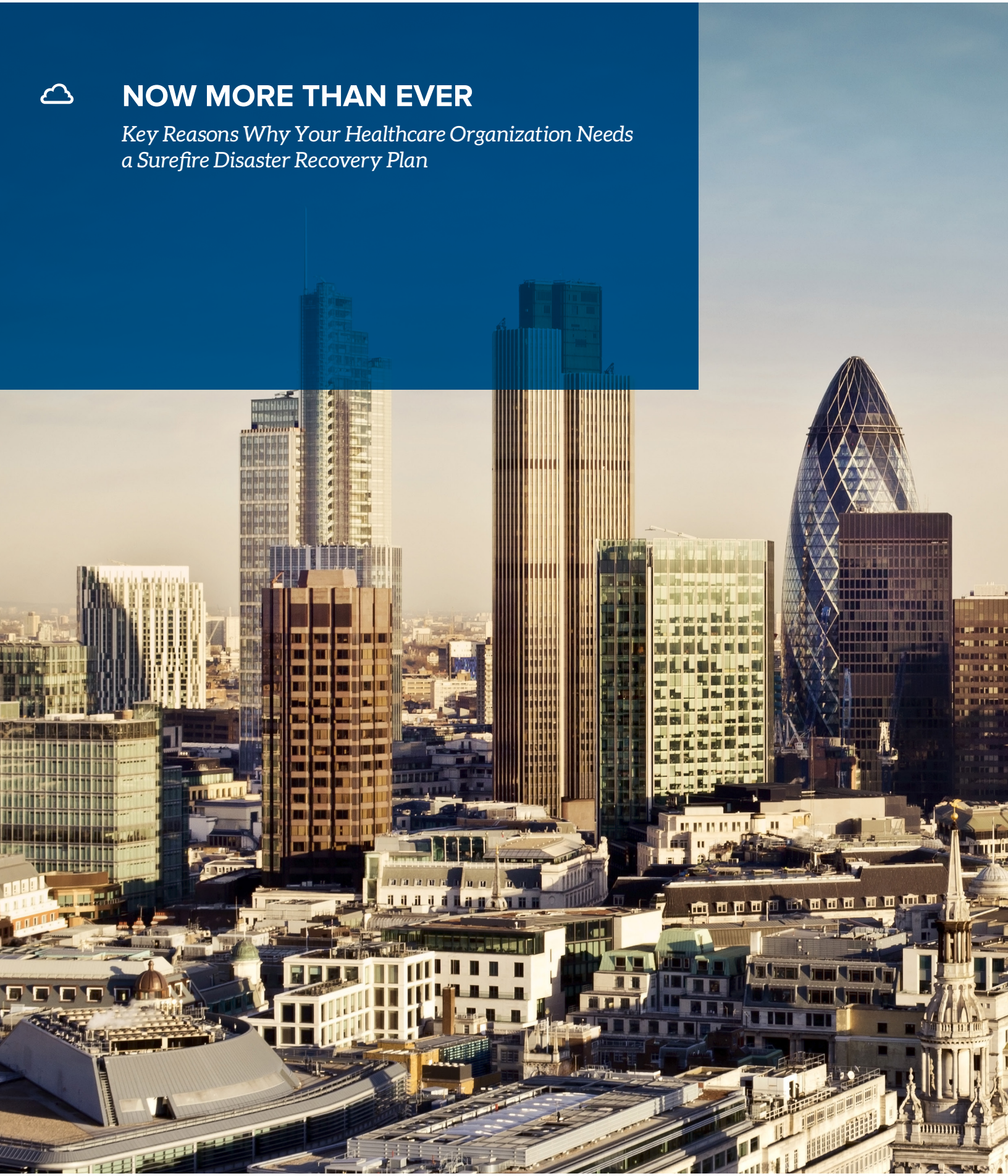
NOW MORE THAN EVER

Key Reasons Why Your Healthcare Organization Needs a Surefire Disaster Recovery Plan



INTRODUCTION

The potential loss of data for any reason is always present, and so is the possibility of a natural disaster. This threat is especially concerning when dealing with patient data. So, what happens if that hundreds or thousands of patient data is lost? What plan do you have in place?

The increasing number of high-profile healthcare data breaches serve as a warning of the importance of having a robust disaster recover plan. Consider these facts:

- The average cost associated with an interruption in health information technology systems is $7,900 per minute, or almost $500,00 per hour, which translates to over $11 million for one 24-hour day.
- 56 percent of healthcare professionals reported that disaster recovery was a top priority, but only 26 percent said they had a “robust, tried-and-tested” plan in place.
- As of May 18th, 2015, HHS had published the names of 1,223 healthcare organizations that suffered a breach of 500 or more individuals since October 2009.

As seen above, while healthcare organizations understand the importance of having a DR plan, there is more that they must do to implement and ensure the effectiveness of those plans. The failure to act in the event of a catastrophe will not only cost you millions, but your organization’s reputation would be on the line. This paper takes a look at essential steps to safeguarding against a natural disaster as well as an inside look into how Grady Memorial has established a robust DR system to support all their operations and patient care. Finally, we will walk through the eight must-have requirements for your DR plan.

CONTENTS

WHY PROVIDERS NEED DISASTER RECOVERY PLANS

Even the most reliable information systems will crash at some time. Healthcare consultants point out that no system will run smoothly 24 hours a day, seven days a week and 365 days a year without failing. Experts estimate that the highest uptime rate is about 99.5 percent, which means that even the best system will fail 0.5 percent of the time.[1] Therefore, every healthcare organization needs a Disaster Recovery (DR) plan.

Another critical concern is that with many of the hospitals and healthcare organizations that have DR plans, their IT departments do not conduct routine testing of their plans.[2] When a disaster strikes, the IT staff should be confident that their DR plan will prevent data loss and downtime.

"Although healthcare administrators understand that no system is foolproof, things will go wrong and many times they are not prepared for a system failure when it happens. The question is: How do they prepare for that 0.5 percent of the time when systems fail?" says Gina J. Haylett, a Trusted Advisor for healthcare accounts for QTS data centers in Atlanta.

Healthcare organizations know that they should have DR and business continuity (BC) plans in place but most do not. She adds, most hospitals are in two positions. They either don't have a disaster recovery program in place or they have one at a facility just down the street. In contrast, there are providers with more reliable DR programs in place. These organizations have decided to invest in their DR plans after weighing the impact of the alternative, which is the risk of losing thousands and potentially millions of dollars if an outage occurs.

They are also challenged with shrinking budgets for IT projects. In this time of declining reimbursements for healthcare services, CIOs are controlling spending by seeking alternatives with technology partners that help turn capital expenses into operational expenses," Haylett explains. "They can do so through managed hosting or cloud services. This model provides healthcare organizations with the ability to budget and track infrastructure costs more efficiently when compared with having to find the costly capital upfront to do it on their own.

These systems give IT professionals the peace of mind that comes with knowing their critical systems are in a highly reliable data center and ready to respond in any disaster.

CIOs are controlling spending by seeking alternatives with technology partners that help turn capital expenses into operational expenses. They can do so through managed hosting or cloud services.

"Here's another benefit that CIOs value: These DR services give IT professionals the peace of mind that comes with knowing their critical systems are in a highly reliable data center that is supported by best practice processes with 24x7 monitoring and support that is ready to respond in any disaster," Haylett explains.

"The cloud and managed services model also increases the staffing of the IT department since the technology partner becomes an extension of the IT staff. Provider organizations should

WHY PROVIDERS NEED DISASTER RECOVERY PLANS

consider contracting with a vendor partner who has a team of in-house engineers skilled in various parts of the infrastructure so they can work side by side with a provider's IT department," she says. "These engineering partners can work closely with the IT staff to provide insight on growth initiatives and direction on new infrastructure as the environment changes, which may involve leveraging other services to enhance an existing disaster recovery solution."

Lessons Data Professionals Can Learn From Disaster Recovery

When health information technology systems fail, the average cost is $7,900 per minute, or almost $500,000 per hour, which is well over $11 million for one 24-hour day, according to a report from the Ponemon Institute.[3] It will come as no surprise, then, that when costs run this high for one data system failure, it's likely that at least one high-ranking executive will resign or be fired. All of these factors point to one unmistakable conclusion: Every provider organization needs a comprehensive DR plan. This need has never been greater. The potential loss of data for any reason is always present and so is the possibility of catastrophe, including natural disasters, such as a flood, hurricane or tornado.

While research shows CIOs emphasize the importance of DR plans, few hospitals are working to protect their data in the event of a disaster. Based on a study of healthcare professionals, 54.6 percent reported that the need to address disaster recovery was a top priority, but only 26 percent said they had a "robust, tried-and-tested" data recovery plan in place, according to The BridgeHead Software 2011 International Healthcare Data Management Survey.[4] In the same survey, two thirds of the executives said data volume had increased in the past year and 64 percent said they had disaster recovery plans in place. But only 38 percent of this group had tested those plans.

CIO's have been warned for years that they should have a robust disaster recovery plan in the event of a disaster.

Failure to prepare adequately for a disaster has been costly to health systems. In 2005, thousands of paper health records were lost in New Orleans after Hurricane Katrina. In 2012, Hurricane Sandy caused a significant loss of health records and data systems in New Jersey and New York.[5] A category 5 hurricane ripped through Joplin, Missouri, in 2013, knocking out power to Mercy Memorial Hospital, leading to an evacuation of all patients. A disaster recovery plan would have improved patient care for those patients, according to published reports.[6]

In 2012, dozens of hospitals lost access to their electronic health records (EHR) systems when human error led to a widespread computer failure. The result was providers had no access to electronic records for most of one day.[7] Earlier this year, the EHR at Boston Children's Hospital crashed and was not operable for five days, according to The Boston Globe. Physicians resorted to using paper records.[8]

Given that disasters are common and costly, hospitals and other healthcare organizations can develop more effective disaster

WHY PROVIDERS NEED DISASTER RECOVERY PLANS

recovery plans by investing in a hospital incident command system (HICS). HICS implementation is a strategy that healthcare organizations use when planning for and responding to disasters. A HICS supports providers in creating DR and BC plans.

The DR plan usually consists of a strategy designed to quickly get the information system up and running while minimizing downtime as much as possible. In order to do so, a failover system must be established offsite so that when a hospital's system crashes, operations will run on or fail over to the DR site with minimal disruption.

A BC plan is one that outlines the steps a provider would take when a disaster strikes yet allows the facility to continue to operate with almost no interruption.

Protect Your Healthcare Organization's Reputation

CIOs have been warned for years that they should have a robust DR plan in the event of a disaster.[9] In fact, the Association for Data Center Management has been warning since 2009 that organizations operating data centers have not done enough to prepare for disaster recovery, according to Information Security magazine.[10]

Today, of course, most healthcare administrators are well aware of the need to have a robust DR and BC plan in place. But, recent reports show that when Premera, a large health insurer in the Pacific Northwest, was hacked in 2014, it had already been cited in a federal audit for failing to have an adequate plan, according to the Seattle Times.[11]

Premera is likely to pay a steep price in terms of penalties and claims from members, not to mention its loss of prestige as a business.[12] Unfortunately, it is likely to find its name on the Wall of Shame, which is what the federal Department of Health and Human Services (HHS) uses to publicize the names of hospitals and other healthcare providers that have experienced a data breach resulting in the loss of records of 500 or more individuals.[13]

As of May 18, 2015, HHS had published the names of 1,223 healthcare organizations that suffered a breach of 500 or more individuals since October 2009. According to Health Data Management, "The HHS Wall of Shame clearly illustrates that a number of healthcare organizations still need to step up their security game and DR plan, which is a bit shocking when you consider the HIPAA security compliance deadline was set in April 2005."[14]

WHY PROVIDERS NEED DISASTER RECOVERY PLANS

DR and BC Planning

The question, then, for IT professionals is how to increase your hospital or healthcare organization's reputation.

Two of the most important steps a hospital can take are:

- Establish a data center DR plan. This step is critically important because with a DR plan, the hospital's IT system can be up and running again while IT staff conducts an audit of the system.
- Conduct a thorough BC assessment. This assessment would include a detailed analysis of compliance with federal laws and regulations.

Those laws include the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology Act (HITECH) of 2009 and the regulations include those from the Federal Risk and Authorization Management Program (FedRAMP).

Compliance with these laws and regulations will not guarantee that a hospital or healthcare organization will never suffer any data loss from a disaster, but full compliance will help to mitigate the consequences.

The best in class compliance vendors will implement a strong control environment and provide all necessary reports so that hospitals and other healthcare organizations can demonstrate that they are meeting industry DR standards.

IT professionals should consider hiring independent third-party consulting firms with expertise in the areas of healthcare data loss and DR to assess risk. Taking these and other steps to help ensure data protection will be costly, but it is possible—and in fact probable—that the investment in DR will be less than the expense of paying for losses and fines as well as damage to the hospital's reputation.

Consider that after health insurer Anthem's incident in February 2015, which caused the loss of 80 million health records, legal experts reported that the insurer was facing more than 50 class-action lawsuits in just the first month. And, there is a possibility that it could face a number of civil suits as well, according to Modern Healthcare.[15] Ask yourself: is this worth your hospital or healthcare organization's reputation?

Case Study: Grady Memorial Hospital Relies on IT Systems for All Operations

For Grady Memorial Hospital in Atlanta, GA, DR has been a high priority for many years, according to Ben McKeeby, Senior Vice President and Chief Information Officer.

About five years ago, the administration identified the need to remove and replace the previous DR system so that the 950-bed hospital could install new infrastructure that would allow the facility to run a highly reliable system that also offered redundant backup, he says.

"At the time, we wanted a physical location that could accommodate a more robust data system and that was better suited as a DR solution," McKeeby explained. "Our previous DR system was directly across the street, and being that close is less than ideal if you're trying to protect against a disaster that could affect an entire area." Grady works closely with QTS, a data

WHY PROVIDERS NEED DISASTER RECOVERY PLANS

center and information systems solutions company with operations nationwide.

Now that the DR system is in place, Grady Memorial, part of the Grady Health System, can rely on the DR system to support all operations and patient care, McKeeby says.

"When you think about it, even in the IT department, the heart of the mission of the hospital is to deliver the best patient care possible," he adds. "The biggest impact we have may not be directly on the patient but, instead, on the systems that serve our patients. For example, we support our EHR system, Epic, that all the physicians and clinicians rely on to help deliver better care more efficiently.

"Of course, we're also supporting the back office operations, which not many people think about, but it is as critically important to ensuring the operations of the hospital," McKeeby continues. "Our job is to support every aspect of operations from patient care right through to the business side of the operation, which means ensuring the security of all aspects of patient data from billing information to clinical data."

Every hospital IT department understands the need for continual vigilance, he says.

"That's why we try to build security into everything we do. We understand our vulnerabilities, whether from a natural disaster or some other unforeseen event," McKeeby explains. "But what is worrisome is the event that no one can predict." CIOs try to imagine every possible scenario that might affect a facility's data systems, McKeeby says. "As such, we have a challenge to manage risk at the appropriate level," he comments.

"We know technology will break. That's a given with any system," he explains. "Our job is to make sure our design is fault tolerant and then when it does break down, we need to get the system back up quickly and efficiently. To do these things well requires effective planning, the proper design and the best systems. We think we have all three of those components in place.

Our job is to support every aspect of operations from patient care right through to the business side of the operation, which means ensuring the security of all aspects of patient data from billing information to clinical data.

We know that systems will break down. Our job is to make sure our design is fault tolerant and then when it does break down, we need to get the system back up quickly and efficiently.

"Technology is key to the future of healthcare," he comments. "That's why we have a system that is 'always on.' That alone means it needs to be highly reliable.

"We recognize that there's an expectation about IT in a hospital that the information systems should not break down often. That's why our goal is to ensure reliability and to put in the processes and procedures so that when things go wrong, we can get them running again quickly. This is an important point of emphasis in any hospital IT department: keep all systems running and if they do break down, make sure that you can switch over to a backup system quickly and easily," he explains.

"IT is such a vital part of

WHY PROVIDERS NEED DISASTER RECOVERY PLANS

Grady, it's important that we partner and work closely with every department, including administration, clinicians, service lines, and emergency management, among others. All of our organizational imperatives require some level of technology to enable improvements, and consistently meeting or exceeding our goals leads to the ability to reinvest in continually improving patient care."

Technology is key to the future of healthcare. That's why we have a system that is 'always on.' That alone means it needs to be highly reliable.

EIGHT MUST-HAVE REQUIREMENTS FOR YOUR DISASTER RECOVERY PLAN

When CIOs and other IT professionals are evaluating the need for a more robust disaster recovery system, Gina J. Haylett, a Trusted Advisor for healthcare accounts at QTS data centers in Atlanta, suggests they ask themselves these questions.

1 **CAN THE DR PLAN SUPPORT YOUR CRITICAL APPLICATIONS?**

"If your DR infrastructure cannot support your most important applications, then it's not a fully functioning DR solution," she says. In addition to ensuring that it supports all mission-critical applications, make sure it can replicate an application spread across many different virtual machines. And, discuss the recovery time objective (RTO) and the recovery point objective (RPO) to ensure that they meet the expectations of your organization's plan.

2 **IS THE DR SYSTEM VIRTUAL READY?**

"Many applications today run on virtual machines or on virtual disks. Therefore, the best DR systems are ready to do so as well," she explains. "Failing to get a DR solution that is virtual ready could eliminate the benefits your hospital or care center gets from virtualization and double your overhead. This can mean that many of the benefits you've achieved through virtualization of the rest of your infrastructure may be lost."

3 **IS YOUR DR SYSTEM VENDOR AGNOSTIC?**

Some DR solution providers have particular hardware requirements in their systems. Therefore, IT organizations should try to avoid vendor lock-in whenever possible. "True vendor heterogeneity will enable you to replicate from high-end storage to a lower tier of storage at a secondary site without changing your environment or driving up costs to establish the DR site," Haylett explains. "Having a DR solution that will work in any environment increases your DR system flexibility and thus keeps costs down."

4 **IS THE DR SOLUTION HARDWARE-AGNOSTIC?**

Any DR system needs to accommodate replication and mobility among different vendors and among different storage technologies.

5 **IS IT SCALABLE?**

Even though the ability to scale any system is critical today, this feature is often overlooked, which could be costly. "Scalability has two components: deployment and management. As your virtual infrastructure grows, you need your DR to grow with it seamlessly

EIGHT MUST-HAVE REQUIREMENTS FOR YOUR DISASTER RECOVERY PLAN

without the need to purchase, install, and configure additional proprietary hardware. Otherwise, costs will rise dramatically every time you need new technology," she says.

6 WILL YOUR DR SYSTEM IMPROVE PERFORMANCE?

"It seems strange, but some DR solutions designed to replicate data and/or systems often have adverse effects on production application performance and can even interrupt service at times," Haylett explains. "Therefore, the best in class DR solutions should have little to no negative impact on production."

7 IS YOUR DR SYSTEM CLOUD-READY?

"Today, many cloud-based DR systems operate as disaster recovery as a service (or DRaaS), which helps to reduce costs and eliminate barriers to data replication which is a best practice that might not have been feasible before," she says. "Also, DRaaS is an excellent option for enterprises that want to test the cloud for the first time."

8 IS YOUR DR SYSTEM SIMPLE TO DEPLOY?

"Among the most important keys to successful adoption of any enterprise tool are ease of installation and implementation," Haylett comments. "A best-in- class DR solution should be easy to install and configure with the existing infrastructure without disruption."

Asking these questions and working in partnership with an experienced and knowledgeable IT and data center vendor will help ensure that your data will be secure for many years regardless of what unforeseen disasters may strike.

ABOUT QTS | 877.QTS.DATA | QTSDATACENTERS.COM

QTS Realty Trust, Inc. (NYSE: QTS) is a leading provider of secure, compliant data center, hybrid cloud and managed services. QTS features the nation's only fully integrated technology services platform providing flexible, scalable solutions for the federal government, financial services, healthcare and high tech industries. QTS owns, operates or manages more than 5 million square feet of data center space and supports more than 1,100 customers in North America, Europe and Asia Pacific. In addition, QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for third-party data center owners and operators. For more information, please visit www.qtsdatacenters.com, call toll-free 877.QTS.DATA or follow us on Twitter @DataCenters_QTS.

SOURCES

1 HALL, SD, "DATA CENTER DOWNTIME COST AVERAGES $7,900 A MINUTE," FIERCEHEALTHIT, DEC. 5, 2013. ACCESSED MAY 18, 2015: KEY REASONS WHY YOUR HEALTHCARE ORGANIZATION HTTP://WWW.FIERCEHEALTHIT.COM/STORY/DATA-CENTER-DOWNTIME-COST-AVERAGES-7900-MINUTE/2013-12-05

2 HOROWITZ, BT, "DISASTER RECOVERY PLANS LACKING AT A MAJORITY OF HOSPITALS: REPORT," EWEEK, JUNE 29, 2012. ACCESSED MAY 18, 2015: HTTP://WWW.EWEEK.COM/C/A/HEALTH-CARE-IT/DISASTER-RECOVERY-PLANS-LACKING-AT-A-MAJORITY-OF-HOSPITALS-REPORT-321899

3 PONEMON INSTITUTE, 2013 COST OF DATA CENTER OUTAGES, DECEMBER 2013. ACCESSED MAY 18, 2015: HTTP://WWW.EMERSONNETWORKPOWER.COM/DOCUMENTATION/EN-US/BRANDS/LIEBERT/DOCUMENTS/WHITE%20PAPERS/2013_EMERSON_DATA _CENTER_COST_DOWNTIME_SL-24680.PDF

4 BRIDGEHEAD SOFTWARE, THE BRIDGEHEAD SOFTWARE 2011 INTERNATIONAL HEALTHCARE DATA MANAGEMENT SURVEY. JUNE 2012. ACCESSED MAY 18, 2015: HTTP://WWW.BRIDGEHEADSOFTWARE.COM/COMPANY/PRESS_RELEASES/BRIDGEHEAD_SURVEY_FINDS_MAJORITY_OF_HOSPITALS_LACK_ROBUST_ DISASTER_RECOVERY/

5 CHAPMAN, S, "WHEN DISASTER STRIKES," FOR THE RECORD, MAY 2013, VOL. 25 NO. 8 P. 22. ACCESSED MAY 18, 2015: HTTP://WWW.FORTHERECORDMAG.COM/ARCHIVES/0513P22.SHTML

6 BERNHARD, B, "LOST MEDICAL RECORDS COMPLICATE JOPLIN HOSPITAL'S TORNADO RECOVERY", ST. LOUIS POST-DISPATCH, JUNE 2, 2011. ACCESSED MAY 18, 2015: HTTP://WWW.STLTODAY.COM/LIFESTYLES/HEALTH-MED-FIT/FITNESS/LOST-MEDICAL-RECORDS-COMPLICATE-JOPLIN-HOSPITAL-S-TORNADO-RECOVERY/ ARTICLE_84C76336-172F-5EB9-A88A-90647F5FF443.HTML

7 RONEY, K, "5 GUIDELINES FOR HOSPITAL DATA RECOVERY PLANS," BECKER'S HOSPITAL REVIEW, AUG. 15, 2012. ACCESSED MAY 18, 2015: HTTP://WWW.BECKERSHOSPITALREVIEW.COM/HEALTHCARE-INFORMATION-TECHNOLOGY/5-GUIDELINES-FOR-HOSPITAL-DATA-RECOVERY-PLANS.HTML

8 FREYER, F, "BOSTON CHILDREN'S EMERGES FROM ELECTRONIC RECORDS SHUTDOWN," THE BOSTON GLOBE, MARCH 25, 2015. ACCESSED MAY 18, 2015: HTTP://WWW.BOSTONGLOBE.COM/METRO/2015/03/25/BOSTON-CHILDREN-EMERGES-FROM-DAY-SHUTDOWN-ELECTRONIC-MEDICAL-RECORDS/Q6SE7HRM4CXFEMEDYWP8IK/STORY.HTML

9 HENDERSON, N, "AFCOM REPORT FINDS DATA CENTERS LACK BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS," THE WHIR, SEPT. 13, 2011. ACCESSED MAY 18, 2015: HTTP://WWW.THEWHIR.COM/WEB-HOSTING-NEWS/AFCOM-REPORT-FINDS-DATA-CENTERS-LACK-BUSINESS-CONTINUITY-AND- DISASTER-RECOVERY-PLANS

10 MORTMAN, D, "DISASTER RECOVERY RISK ASSESSMENT FOR CYBERTERRORISM ATTACKS," INFORMATION SECURITY, NOVEMBER 2009. ACCESSED MAY 18, 2015: HTTP://SEARCHSECURITY.TECHTARGET.COM/ANSWER/DISASTER-RECOVERY-RISK-ASSESSMENT-FOR-CYBERTERRORISM-ATTACKS

11 BAKER, M, "FEDS WARNED PREMERA ABOUT SECURITY FLAWS BEFORE BREACH," THE SEATTLE TIMES, MARCH 18, 2015, (AND UPDATED APRIL 2, 2015). ACCESSED MAY 18, 2015: HTTP://WWW.SEATTLETIMES.COM/SEATTLE-NEWS/FEDS-WARNED-PREMERA-ABOUT-SECURITY-FLAWS-BEFORE-BREACH/

12 GARNICK, C, "PREMERA NEGLIGENT IN DATA BREACH, 5 LAWSUITS CLAIM," THE SEATTLE TIMES, MARCH 27, 2015. ACCESSED MAY 18, 2015: HTTP://WWW.SEATTLETIMES.COM/SEATTLE-NEWS/PREMERA-NEGLIGENT-IN-DATA-BREACH-5-LAWSUITS-CLAIM/

13 KOLBASUK MCGEE, M, "ANTHEM HACK NOW TOPS 'WALL OF SHAME,' FEDERAL BREACH TALLY TO SOON INCLUDE MORE HACKER ATTACKS," DATA BREACH TODAY, MARCH 17, 2015. ACCESSED MAY 18. 2015: HTTP://WWW.DATABREACHTODAY.COM/ANTHEM-HACK-NOW-TOPS-WALL-SHAME-A-8025

14 EVANS, B, "FOUR 2015 HIT SECURITY PREDICTIONS," HEALTH DATA MANAGEMENT, DEC. 16, 2014. ACCESSED MAY 18, 2015: HTTP://WWW.HEALTHDATAMANAGEMENT.COM/BLOGS/FOUR-2015-HIT-SECURITY-PREDICTIONS-49443-1.HTML

15 CONN, J, "LEGAL LIABILITIES IN RECENT DATA BREACH EXTEND FAR BEYOND ANTHEM," MODERN HEALTHCARE, FEB. 23, 2015. ACCESSED MAY 18. 2015: HTTP://WWW.MODERNHEALTHCARE.COM/ARTICLE/20150223/NEWS/302239977