healthcare informatics
CUSTOM MEDIA

Business Continuity and Disaster Recovery in Healthcare:

Risk and Technology Converge for Value-Based Care

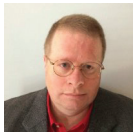
RESEARCH SUPPORTED BY

Zerto | Nth GENERATION

Contributing Executives

Trey Jones
Director, IT Infrastructure
Houston Methodist

Matt Johnson
Manager, Server Engineering
Houston Methodist



Shannon Snowden
Senior Technical Architect
Zerto

Jennifer Gill
Director, Global Product Marketing
Zerto

healthcare informatics
CUSTOM MEDIA

Introduction: Convergence

Change has always been a constant in healthcare, say veteran health-system executives, but today's convergence of healthcare reform—including the shift to accountable care, risk-sharing and population health—and the digital revolution—including mobile communications and consumerism—seems to be creating an unprecedented perfect storm of uncertainty.

Healthcare's "new normal" has many faces as it moves into a digital, value-based model, and surely one of them is cybersecurity, the daily threat to patient data that keeps CEOs and CIOs awake at night. Lost in the discussion of risk to patient privacy and security, however, is the need for new solutions for disaster recovery and business continuity. Health systems have become so dependent on information technology for patient care and operations that any outage to the IT infrastructure, network, data center or applications like the electronic health record (EHR) is a potential threat to patient care.

With increased HIT adoption, disaster preparedness and business continuity have become more crucial than ever. When Superstorm Sandy hit the northeastern United States in 2012 it delivered a wakeup call about the need for updated recovery and business continuity plans as many organizations lost not only their primary data centers but secondary data centers as well which were often many miles inland. Whether it's for natural disasters, bioterrorism, epidemics, human error causing unexpected downtime or cybersecurity threats, health-system senior leadership must plan for service interruptions to protect themselves and their patients. Fortunately, this era of clinical and digital transformation offers myriad enabling technologies for this mission, from virtualization, cloud computing and health information exchange to and mobile communications.

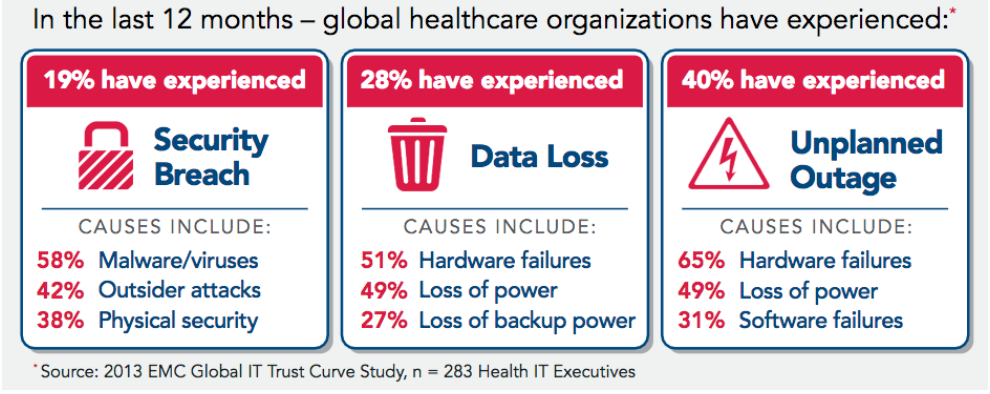
IT is realizing that data security, disaster recovery and business continuity are converging. Indeed, ransomware, arguably today's most frightening cyber threat, involves both cybersecurity and disaster recovery and business continuity. To plan for a cyberattack appropriately, organizations must focus on preventing breaches as well as the recovery plan if a breach should occur. Most organizations focus too much on the former and not enough on the latter.

When Superstorm Sandy hit the northeastern United States in 2012 it delivered a wakeup call about the need for updated recovery and business continuity plans as many organizations lost not only their primary data centers but secondary data centers as well which were often many miles inland.

Business Continuity and Disaster Recovery for Healthcare

As the most highly regulated information on the planet, patient and healthcare information must be available anytime and anywhere to healthcare providers to deliver safe, effective and quality care. The shift to value-based care with its emphasis on coordinated team care and population-health management is only accelerating the demand for 24x7 data access from anywhere the patient and provider happen to be. The risk to data remains high from cyber threats and other outages.

According to one study nearly 40 percent of healthcare organizations across the globe have experienced a costly unplanned outage in the past 12 months. On average these incidents cost $432,000, and once an emergency has passed, only half of those organizations surveyed are confident in their ability to restore 100 percent of the data required by service level agreements (SLAs).[1] This doesn't even factor in the threat to patient care should the data center and network crash and eliminate access to patient information in the EHR.



40%

According to one study the percentage of healthcare organizations across the globe that experienced a costly unplanned outage in the page 12 months.

$432,000

Average cost of an unplanned outage.

However, advancing cybersecurity threats have also heightened the need for a new look at disaster recovery and business continuity as have enhanced regulatory requirements like HIPAA, technology advances such as mobility, virtualization and the cloud, and a rapidly consolidating healthcare delivery environment with more disparate IT systems. Highlights of some of these factors follow.

1. http://www.meritalk.com/rx

Health Insurance Portability and Accountability Act

Among the many components of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect the privacy and confidentiality of patient data is a requirement that healthcare organizations must be able to recover from a natural disaster. While it doesn't specify the exact process, any failure to adequately recover from a disaster would likely be defined as non-compliance that would cost senior officers severe financial penalties or even jail time.

An overall guide to HIPAA can be found at https://www.hhs.gov/hipaa/index.html.

Here are some key points related to disaster recovery and business continuity in the HIPAA Security Final Rule:

- The requirement is non-negotiable. Under HIPAA all hospitals and health systems, including medical practices musty securely back up "retrievable exact copies of electronic protected health information."
- Health systems must be able to recover their data, be able to fully "restore any loss of data." The process is to failover the information to a target site where there is standby equipment. A disaster recovery process must then be executed to build the applications with the associated data so that it is fully usable to deliver patient care.
- Data must be moved off-site in case of a disaster.
- Health systems must back up their data regularly. Many organization do this nightly to comply with regulations.
- Once in recovery mode, health systems must still maintain safeguards.
- Both the 2009 HITECH Act and the HIPAA Security Rule require health systems to encrypt or destroy data.
- Health systems must have written documentation of policies and procedures for data recovery plans, many of which can take days or hours.
- Recovery testing is mandatory. The law requires health systems to "Implement procedures for periodic testing and revision of contingency plans." Because testing of traditional tape-based or disk-based disaster recovery is burdensome and time-consuming, most health systems organizations rarely do it.
- Health systems will pay severe non-compliance penalties in the millions of dollars.
- Health systems will be audited for compliance with the Rule: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/

Virtualization

Virtualization has become widely accepted due to its cost-savings combined with increased flexibility and portability of applications. Data is not growing in healthcare, it is exploding with the simplification of medical processes. X-rays and other tests are not the complex, time-consuming procedures they were in the past, and can be completed quickly and easily. Due to the exploding growth of data, organizations cannot remain on physical systems as the costs to manage, power, cool and maintain this environment becomes astronomical.

Virtualization enables IT to logically carve out resources on a physical server and assign them to a specific application and its associated data. Instead of running one application on a server, IT can logically separate the server's resources and run several applications on one server. This consolidation reduces power and cooling costs while reducing the complexity of management.

Virtualization allows health systems to use less hardware, power and cooling for a data center and fewer FTEs for management and maintenance. Like the move to cloud computing, healthcare organizations have been late adopters of virtualization, however they are embracing the strategy because of its economy and flexibility. Virtualization has become a key component in the IT platform of the future because of the explosion of data for value-based, accountable care and population health. Risk and cost management converge as bulwarks of safe and quality care.

"The move to virtualization in healthcare is a matter of becoming comfortable with it," says Trey Jones, director of IT infrastructure at Houston Methodist, an eight-hospital health system in Texas. "Prior to 2014, we weren't comfortable with virtualization. Today we're comfortable with virtualizing our largest systems."

That means updating disaster recovery and business continuity plans and technology to match the new IT environment.

As healthcare moves to virtualization and the Cloud, the new technology model for disaster and business continuity is virtual replication and orchestration, which has been pioneered by Zerto, a firm that provides virtual replication and orchestration solutions for disaster recovery and business continuity. Zerto Virtual Replication protects healthcare data in the hypervisor. When combined with a fully configured and automated recovery process, Zerto Virtual Replication delivers stability for business continuity. Zerto's well-engineered virtual replication can be integrated seamlessly into a hospital's or health system's IT infrastructure without requiring any hardware or software reconfiguration.

Instead of running one application on a server, IT can logically separate the server's resources and run several applications on one server. This consolidation reduces power and cooling costs while reducing the complexity of management.

The combination of Zerto Virtual Replication and orchestration of the recovery plan enables hospitals and health systems to quickly recover from any time of disruption or disaster. Unique to Zerto is its non-disruptive disaster-recovery testing which can unequivocally demonstrate to compliance officers that a recovery plan is in place to quickly recover both applications and data. Upon completion of the test, a documented test plan is produced which satisfies many compliance requirements including HIPAA. While the organization must still document that critical personnel and communications are in place, having Zerto Virtual Replication solves the most daunting issue of all: access to patient records.

"Virtualization is a no-brainer for health systems scrambling for funds to invest in the most efficient, secure and easy to use IT," says Shannon Snowden, senior technical architect at Zerto. "Zerto Virtual Replication is the natural next step for ensuring their EHR is always up and running."

While the organization must still document that critical personnel and communications are in place, having Zerto Virtual Replication solves the most daunting issue of all: access to patient records.

Ransomware

In the past few years we've witnessed the increasing trend of hackers trying to extort money from private users, businesses and health systems using ransomware "Trojans," malicious software designed to access and encrypt data by generating a private-public pair of keys. The objective: make it impossible to decrypt your own data without the private key, typically stored on the attacker's server until the ransom is paid. Too often—even if the ransom is paid—the attackers fail to provide the decryption key, which leaves victims without their money or their files.

A recent article in Forbes cited a "staggering" increase in ransomware attacks in 2016 to 638 million compared to 3.8 million in 2015—more than 167 times the previous year![2]

While ransomware has been around for years, recent advances in encryption technology and hackers' increased ability to disguise their identities have resulted in a dramatic increase in ransomware attacks, which are dangerous for several reasons:

- Hackers use sophisticated techniques to circumvent security software, including creation of "Zero-Day Malware" that makes the Trojan invisible to security experts and security software.
- Security experts consider encrypted data to be unrecoverable. Because many victims say the decryption key is not provided even if the ransom is paid, experts recommend not giving in to hacker demands from the start.
- Through the use of the Tor network and virtual currencies such as Bitcoin, hackers are largely untraceable by security agencies.
- Ransomware attacks are mostly directed at users in more affluent countries; in 2015, half of a major ransomware-type's attacks occurred in the U.S. and more than a third in Europe.
- In late 2014 a ransomware threat specifically targeted mass-storage and network attached storage (NAS) disks. This trend of targeting "high-value" victims is increasing.
- Ensuring you have suitable anti-virus and security software—that is kept up-to-date—is the obvious starting point. User-education is also key, as many Trojans gain initial access to systems through links contained in—often very official-looking—phishing emails. Human error can and does happen though, so extra layers of protection are still required.

3.8 M

According to Forbes, the number of ransomware attacks in 2015.

638 M

According to Forbes, the number of ransomware attacks in 2016.

167x

The increase in ransomware attacks from 2015 to 2016, according to Forbes.

2. http://www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/#61230ed23468

Backing up your data is crucial, but many businesses either do not have a backup program in place, or have such infrequent backups that should their systems become infected they'll potentially stand to lose a significant amount of data.

"Most ransomware attacks can be avoided through good cyber hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed. Our recommendation is that businesses need to be proactive because the decryption keys are not always provided when ransoms are paid and being proactive is often easier and less costly than a reactive approach," says Raj Samani, CTO for Europe at Intel Security.

Cybersecurity, risk-management and disaster-recovery experts agree that 100-percent prevention isn't always possible, but mitigating threats is possible by creating a flexible and resilient response strategy that includes a virtual replication-based disaster recovery and business continuity strategy. Zerto Virtual Replication enables health systems to recover from ransomware and other malware by being able to:

- Rewind their information systems to the last point-in-time before the infection struck, to within a matter of seconds leveraging continuous data protection (CDP).
- Recover their critical systems within the space of a few minutes, with only a few clicks of a button through automated orchestration.
- Not only restore entire sites, applications and databases with consistency, but to do so with the granularity to restore VMs that are part of an application or individual file.
- Perform non-disruptive failover tests at any time, assuring senior leadership they can bring the business back online whenever needed—and document completed tests to meet regulatory requirements.
- Create off-site backups for longer-term data retention in addition to receiving Continuous Data Protection for up to 30 days.

"Most ransomware attacks can be avoided through good cyber hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed. Our recommendation is that businesses need to be proactive because the decryption keys are not always provided when ransoms are paid and being proactive is often easier and less costly than a reactive approach."

—Raj Samani

Case Studies

Leading health systems and provider organizations are implementing Zerto Virtual Replication as a key component of their disaster-recovery and business-continuity strategies with positive results.

- Houston Methodist
- Yakima Valley Farm Workers Clinic
- Liverpool Heart and Chest Hospital

HOUSTON METHODIST

Comprising a leading academic medical center located in the renowned Texas Medical Center as well as seven community hospitals serving the Houston metro area, Houston Methodist can truly say it is one of the emerging academic health systems. It balances the teaching and research excellence of an urban academic medical center with the burgeoning and diverse patient populations of high-growth suburban communities.

Like many health systems, Houston Methodist is migrating from a heterogeneous EHR environment with both Eclipsys and Epic to a single Epic platform. It also uses Microsoft SQL Server as its primary data base. So when Microsoft recommended virtualization of its data servers as a way to achieve efficiency and flexibility, Houston Methodist listened. “We were able to change our licensing structure and save $1 million in the first year,” says Matt Johnson, manager of server engineering at the health system.

The move opened the door to Zerto Virtual Replication as a disaster recovery and business continuity solution. “When it came to disaster testing in the past,” says Trey Jones, director of IT infrastructure for Houston Methodist, “we found ourselves flying up to Philadelphia twice a year to the DR vendor’s site, boots on the ground, having them issue us servers. It was very time-consuming and we decided it wasn’t good for business. We found ourselves looking at point solutions to automate disaster testing of SQL Server, VMware and physical databases. Zerto kept rising to the top as a comprehensive solution.”

When Houston Methodist did a proof of concept it was impressed by Zerto’s short deployment time and even shorter testing time. “Everything clicked. It was like magic,” recalls Jones. Adds Johnson: “When we did a disaster recovery test last year for the first time to do cross failover, it took only minutes to do what previously took four to six hours.”

That’s important given that hurricanes pose the primary disaster threat to Houston Methodist. “It’s one of those slow punches you can see coming,” says Jones. “Zerto allows us to leave ourselves in a production environment until the last minute. We can designate a single person to watch the weather chart and alert us and then we failover. It only takes a few minutes for hospital downtime. That’s the real benefit.”

YAKIMA VALLEY FARM WORKERS CLINIC

For all the handwringing about how to manage the health of populations, sometimes models are right before us. That's the case with the Yakima Valley Farm Workers Clinic, a nonprofit clinic that provides comprehensive medical, dental and social services for more than 141,000 people throughout the Pacific Northwest. Toppenish, Wash.-based Yakima Valley Farm Workers Clinic employs about 2,000 full-time and part-time employees at 31 medical and dental clinics and 50 programs in the states of Washington and Oregon.

Delivering health services to this population would be impossible without the organization's electronic health record (EHR) from Epic. Given their experience with data-center outages Yakima Valley Farm Workers Clinic management knew they needed the best disaster recovery solution available for Epic, which involves highly complex, time-consuming and staff-intensive processes.

After one particularly onerous data outage, senior management began searching for a top-notch business continuity and disaster recovery solution that was neither complex nor costly. "We have limited staff and we're not in an urban area," said Todd Pappas, the organization's system engineer. At the same time, "We just did not have a robust enough disaster recovery solution to bring all the services back up quickly.

In 2013, Yakima Valley Farm Workers Clinic discovered Zerto and was able to quickly implement Zerto Virtual Replication, delivering aggressive recovery point objectives (RPOs) and recovery time objectives (RTOs). "When you are dealing with legacy replication systems," said Pappas, "it drives up your RTO, because it's not like Zerto, where you have four or five clicks and you're failed over. It's very cumbersome when you're in the midst of a disaster and you're trying to fail over using a legacy system. We needed something simple and the Zerto solution was a great fit for us."

LIVERPOOL HEART AND CHEST HOSPITAL

As one of the largest integrated cardiothoracic-care providers in the United Kingdom, Liverpool Heart and Chest Hospital delivers cardiology, respiratory medicine and cardiothoracic surgery to more than 115,000 patients a year in its hospital and clinics. It couldn't do that without seamless information sharing among its clinicians, staff and patients—enabled by a significant investment in its Allscripts EHR.

Because its virtualized EHR has become indispensable to the quality of care Liverpool Heart and Chest Hospital delivers to its patients, business continuity and disaster recovery was a top priority. However, most market solutions were piecemeal, focused on just replication—the ability to back up the data and make it accessible to everyone—or just orchestration—the ability to redeploy the EHR and its workflows without disruption in case of an outage. Given the need for uninterrupted patient care processes, non-disruptive testing of the disaster recovery and business continuity system was also critical.

James Crowther, IT Operations Manager for Liverpool Heart and Chest Hospital, found that Zerto Virtual Replication was the solution to extend the benefits of virtualization to the organization's disaster recovery and business continuity strategy, a complete disaster-recovery product combining both replication and orchestration.

"When we migrated from paper files to all-electronic files, robust disaster recovery capabilities quickly rose to the top of our priority list. Our goal is to ensure that a patient's experience is not impacted in any way regardless of data losses or interruptions. To ensure that we adopted Allscripts as our electronic patient record system and implemented Zerto Virtual Replication to protect it. Zerto Virtual Replication delivers aggressive service levels, lets us test our disaster recovery plan with no impact and 'future proofs' our environment with no hardware dependencies. It is ideally suited to protect our healthcare environment."

Conclusion

Disaster recovery and business continuity should be an integral component of any health system's risk-management strategy that addresses notorious cybersecurity threats and like interruptions. As convergence occurs on many levels in healthcare's transformation to a value-based, accountable care model that is absolutely dependent on digital technology, the need for new solutions for disaster recovery and business continuity increases.

Like other industries, healthcare is already moving to new IT platforms like virtualization, mobile technology and the cloud. Zerto offers healthcare organizations a solution for disaster recovery and business continuity that matches the speed and ease of use of these new platforms.

Testing of disaster recovery systems, required by law, takes only a few minutes compared to previous solutions that took days because they were reliant on backup tapes. Zerto allows a health system to test daily without disruption to the production environment. When it comes to ransomware attacks, Zerto enables an organization to roll back to a point just seconds before it was hit. In the event of a data center outage, recovery plans can be executed quickly with data and applications available in minutes.

Some organizations are using disaster recovery as a use case to evaluate the cloud. Organizations can test a failover with no impact at any time and see how the application performs in the cloud. Once the team gets comfortable with the performance, Zerto Virtual Replication easily migrates workloads to the cloud with minimal impact.

"When we talk to hospital and health system administrators about their EHR and data center," says Zerto's senior technical architect Snowden, "they all say, 'I just want it up and running.'" Virtual replication like Zerto's has sold itself, he says, because of its reliability, efficiency and ease of management. "It's all about the ultimate up time for the cost."

For more information visit http://www.zerto.com