Business Continuity and Disaster Recovery in Healthcare

As health IT continues to explode, disaster preparedness and business continuity have become more crucial than ever

PROVIDED BY

healthcare innovation
PEOPLE. PROCESS. TECHNOLOGY TRANSFORMATION.

IN COLLABORATION WITH

Zerto

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" faces challenges 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 business continuity and disaster recovery (BC/DR). Health systems have become so dependent on health information technology (HIT) 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 also their secondary data centers which were often many miles inland. Whether it's for natural disasters, bioterrorism, epidemics, human error causing unexpected downtime or cybersecurity threats, health systems' senior leadership must plan for service interruptions to protect their organizations and their patients. Fortunately, this era of clinical and digital transformation offers a myriad of enabling technologies for this mission, from virtualization, cloud computing and health information exchange to mobile communications.

IT professionals are 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 to enable business continuity. To plan for a cyberattack appropriately, organizations must focus on preventing breaches, but more importantly plan for disaster recovery if a breach should occur. Most organizations focus too much on the former, which may be near impossible with multiple cyber-attack variants and methods, and not enough on the latter to recover quickly to restore systems and data.

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 arguably 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 care teams 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 the 2019 Ponemon Institute Study, an annual study of more than 500 global organizations that have experienced a data breach in the past year, the healthcare industry has lost more money because of data breaches than any other industry for the ninth year in a row. Data breaches caused the healthcare industry to lose $6.5 million, which is over 60% more than all other industries (who lost, on average, about $3.9 million). $6.5 million translates to $429 per patient record that was lost or stolen, which is three times more per record than all other industries (about $150 per record).

Also, for the first time, this year's study included the longtail financial impact of a data breach. The effects of a data breach last for years, and the healthcare industry had higher longtail costs in the second and third years after a data breach than other industries. Researchers found that some of these higher costs are related to the higher level of regulation of healthcare organizations.

Another interesting finding is that, after 14 years of research, the Ponemon Institute discovered that the greatest impact on the overall cost of the breach is how quickly and efficiently a company can respond to a data breach. In fact, the following components were two of the most influential for lowering the costs of data breaches:

- Having an incident response team in place
- Conducting extensive testing on the incident response plan

In other words, incident response directly correlates to the overall costs of a data breach. The study shows that organizations who detect and contain a breach in fewer than 200 days spent about $1.2 million less on the breach. That is to say, disaster recovery and business continuity are critical factors in lowering the cost of data disruptions—and being prepared for data breaches is essential to BC/DR. What's more, researchers discovered that businesses that utilized security automation technologies for data breaches lost about half as much money (an average of $2.65 million) as those who did not utilize these technologies (an average of $5.16 million).

In addition, the study shows that cyberattacks continue to be a greater and greater threat to digital data. The Ponemon Institute found that, from 2014 to 2019, criminal cyberattacks have increased across all industries by 21% and also caused the most data breaches (51%) last year. Even worse, the cost of recovery of a malicious cyberattack was 25% higher than breaches caused by system or human error.

Not only have advancing cybersecurity threats heightened a need for a new look at BC/DR, the impact of BC/DR has on lowering the cost of data breaches has highlighted the importance for enhanced

regulatory requirements (such as HIPAA), technology advances (such as mobility, virtualization, and the cloud), and a rapidly consolidating healthcare-delivery environment with more disparate IT systems.

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.

The overall guide to HIPAA.

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 this Rule.

Achieving IT Resilience in Healthcare

We know that the healthcare industry has become an attractive target for cyberattacks, but that doesn't necessarily mean procedures and treatments need to be postponed when downtime occurs,

whether due to a breach or disaster. Indeed, with resilient IT infrastructure, systems can be back up-and-running in hours instead of days, with all primary infrastructure intact and functional.

However, it's undeniable that the resilience of businesses' IT is under constant pressure. According to IDC's 2019 multi-industry "The State of IT Resilience Survey and Report," which collected insight and data from 500 C-level executives and IT professionals on the state and maturity of IT resilience as the cornerstone of wider business resilience:

- 100 percent of respondents believe cloud will play a role in their organization's DR or data protection plans.
- The average cost of downtime for all industries and organizational sites is $250,000 per hour. The long-term impact on an organization's reputation and customer goodwill may add significantly to this total.
- Many unrecoverable data events were the result of avoidable causes, such as data loss during the gap between backups, backup/recovery system failure, and lost or damaged tapes.
- 57.8% of respondents believe their data protection requirements will be more complex in the coming years.

IT resilience accelerates digital transformation and innovation by seamlessly adapting to new technology, while protecting the business and customers from disruptions. Zerto's IT Resilience Platform™, for example, accelerates healthcare IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions, Zerto converges disaster recovery, backup and cloud mobility solutions into a single, simple, scalable IT Resilience Platform™ to protect, recover and move applications freely across hybrid and multi-clouds. Zerto delivers continuous availability for an always-on patient and provider experience that addresses use cases faced by healthcare organizations undergoing transformation. Medical applications are carefully configured so re-architecting them for any reason is challenging and could invalidate support agreements. However, Zerto installs seamlessly into the existing infrastructure with no hardware or software reconfigurations required.

The nondisruptive disaster recovery testing clearly demonstrates to compliance officers that a recovery plan is in place that enables fast recovery of applications and data. This doesn't satisfy the complete DR plan, as critical personnel and communications must also be documented. However, the most critical piece, ensuring access to patient records, is solved with Zerto.

Ransomware

In the past several 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.

Indeed, ransomware attacks have become a huge cause for concern for hospitals all over the world. As a result, patient care organizations have had to deal with severe delays and costs to healthcare organizations, patients left untreated, and appointments canceled.

A recent report from cybersecurity company Comparitech analyzed data from ransomware attacks affecting healthcare organizations since 2016, including both the large breaches, impacting more than 500 people, published by the U.S. Department of Health Services (HHS), as well as the attacks impacting fewer people, but that still became public by making the news. The researchers then applied data from studies on the cost of downtime to estimate a range for the likely cost of ransomware attacks to healthcare organizations.

Some of the team's key findings include:

- 172 individual ransomware attacks on healthcare organizations
- 1,446 hospitals, clinics, and organizations affected
- 6,649,713 patients affected
- Ransomware amounts vary from $1,600 to $14,000,000
- Downtime caused varies from hours to weeks and even months
- Hackers have demanded ransoms totaling more than $16.48 million since 2016
- Hackers have received at least $640,000 since 2016
- The overall cost of these attacks is estimated at $157 million

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.
- 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.

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 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 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 migrated 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 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 throughout the Pacific Northwest. The Toppenish, Wash.-based Yakima Valley Farm Workers Clinic offers dozens of 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 120,000 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 to protect it."

"Zerto 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 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 Shannon Snowden, "they all say, 'I just want it up and running.'"

Virtual replication like Zerto's has sold itself because of its reliability, efficiency and ease of management. "It's all about the ultimate up time for the cost."

For more information visit Zerto's website.