Advisory Board | Health Care IT Advisor

The best practices are the ones that work for you.℠

Briefing

IT Disaster Recovery: Three Critical Areas to Consider for Effective and Strategic Recovery Planning

Today's IT-enabled health care clinical and business processes require CIOs[1] to deftly manage risk and create highly resilient organizations. When IT systems—such as EHRs,[2] clinical communications, analytic capabilities, and billing systems—falter or are unavailable, it significantly disrupts routine practices and impacts patient care.

Testing Remains an Issue

While nearly 40% of organizations have had to enact their disaster recovery (DR) plan in the past two years due to some sort of service disruption, less than a third of IT departments actually test their DR plans more than once a year.[3] This is a risk health care providers can no longer afford to take. A robust and well-tested DR plan can help HCOs[4] withstand various forms of service disruptions including cyber incidents, human error, hardware and software malfunctions, and natural disasters.

Halifax Health Case Study

Hurricane Matthew in 2016 provides a clear reason why it is important to develop a thorough DR plan and test it regularly. **Halifax Health**[5] (located in Daytona Beach, Florida) is in hurricane territory, so they must be particularly alert and prepared for disaster recovery. Fortunately, hurricanes, unlike most other natural disasters, give those in their paths a few days of warning. Expected to be a Category 4 or Category 5 storm upon impact, Hurricane Matthew took direct aim at Daytona Beach, Florida in October 2016. Despite all their preparation efforts, Halifax Health still experienced some unforeseen problems and had to do some quick thinking to overcome them.

Key Takeaways

- Plan to have an overnight space large enough to house staff
- Welcome family members of all sorts
- Plan for continuous food service

As the storm approached, the organization's IT department initiated their A and B disaster recovery teams. Per the plan, these teams would stay on site until the storm passed, working 12-hour rotations. Team members were encouraged to bring their family members—and even pets—to campus. Team members and their families stayed in facility floor space that had not been built out for patient care yet; pets were housed in large rooms in the environmental services area. The cafeteria remained open and offered a limited menu throughout the storm. The IT disaster recovery teams worked in conjunction with a hospital-wide disaster recovery command center led by the Administrator on Call.

Key Takeaways

- Consider your physical surroundings and be prepared to make alterations
- Prioritize key clinical communications and data platforms

Halifax Health's data strategy includes data redundancy inside the facility along with a second warm site located several hundred miles away in the event they needed true disaster data restoration. At the time, the organization was moving to MEDITECH 6.1 and was one of the first customers to implement a partial cluster to make their system more highly available; luckily this meant they had an extra SAN[6] on hand. Within 24 hours, the technical services team replicated their MEDITECH data, moved over VMware hosts and their critical communications platforms (including Exchange and

[1] CIO = Chief information officer.
[2] EHR = Electronic health record.
[3] 2015 Cost of Data Breach Study: Impact of Business Continuity Management," Ponemon Institute, June 2015.
[4] HCOs = Health care organizations.
[5] Halifax Health provides a continuum of health care services to the Daytona Beach, Florida community. Their network includes a tertiary hospital, a community hospital, psychiatric services, four cancer treatment centers, a large hospice organization, and a preferred provider organization (PPO).
[6] SAN = Storage area network.

Author: Allyson Vicars | July 2017

Vocera), and relocated the extra SAN to a temporary site at the core of a hurricane-rated building on campus, which was already outfitted with fiber and power. This makeshift secondary data center was created in case of a catastrophic event that damaged or eliminated the primary data center, but the hurricane-rated building remained intact—and ultimately would provide a much faster restoration time.

Other key preparation efforts include:

- Senior leadership is well aware of RPOs[7] and RTOs[8] thanks to biannual board updates. This sets expectations for what the CIO can deliver upon the need for data recovery.
- Business continuity plans for core information systems are tested regularly (once every other month) as part of server patching maintenance.
- Clear lines of emergency situation authority have been established, discussed, and defined—they follow the Hospital Emergency Incident Command System (HEICS) model—which allows for quick decision making in the moment. The IT command center reports to the hospital-wide command center. They provide updates, ask for permission when needed, and submit requests for resources.
- The information security team communicated with staff about the heightened cybersecurity risk for the organization (hackers may take advantage of their situation). The IT department stressed the importance for staff not to share their credentials with family members who may be staying in the facilities and encouraged increased vigilance with both personal and work email accounts following the storm.

As the storm travelled along the coast of Florida, Hurricane Matthew slowed down off of Miami and took a more northerly path; this lessened the intensity of the storm to Category 3 and the eye wall remained about 30 miles out to sea.

The brunt of the storm brought some unexpected problems the IT team had not anticipated: the primary data center lost two cooling units in the span of 10 minutes. The temperature in the data center quickly rose from 70 to 84 degrees within 15 minutes and continued to rise. Adding pressure, the SANs automatically shut off at 90 degrees to preserve data integrity.

Halifax Health kept emergency cooling units on hand and immediately called the facilities department to bring them in. While waiting for them to arrive, the technical and application services team immediately began to shut down about 160 test and non-production servers (of about 700 total) and two older SANS used for miscellaneous storage. The room was still too hot, so the IT and Facilities departments creatively repurposed a large HEPA[9] filter to funnel cold air from inside the ice cold UPS[10] room to the server environment. Together, the temporary cooling units from facilities, the shutdown of several test and non-production servers, and the cold air from the UPS room were able to reduce and maintain the temperature at 70 degrees.

The following day after the storm passed, Halifax Health was the only emergency department open within 50 miles and unexpectedly saw a surge in patients approximately three times their typical volume. The State of Florida provided some resources including supplemental physicians and nurses and set up large tents in the parking lots to triage and treat less acute patients.

Key Takeaways

- Be prepared to think quickly, get creative, and react to events you did not predict or practice
- Keep extra cooling units on hand to use in case of unexpected rising temperatures within the data center
- Consider shutting down nonessential servers so the only heat generated in the data center is that from critical servers

Key Takeaways

- Recognize that recovery challenges may not end when the main incident or storm does
- Expect to accommodate a patient surge after a natural disaster

[7] RPOs = Recovery point objectives.
[8] RTOs = Recovery time objectives.
[9] HEPA = High-efficiency particulate air.
[10] UPS = Uninterruptible power supply.

Author: Allyson Vicars | July 2017

Key Takeaways

- Prepare to provide clinical services in places you did not expect
- Prioritize clinical communications
- Hold a "lessons learned" session after the incident or storm to identify pain points to determine how to improve response for next time

The technical services team needed to extend the hospital network and power to the parking lot to enable critical communications, workstations on wheels, and set up of printers for the supplemental clinicians. They provided wireless access points (APs) facilitated through point-to-point radios to enable communication back to the hospital. They also ran hardwire Ethernet to a small industrial switch inside one of the tents and distributed connections for telephones and access points. Staff was able to register patients from one of the tents.

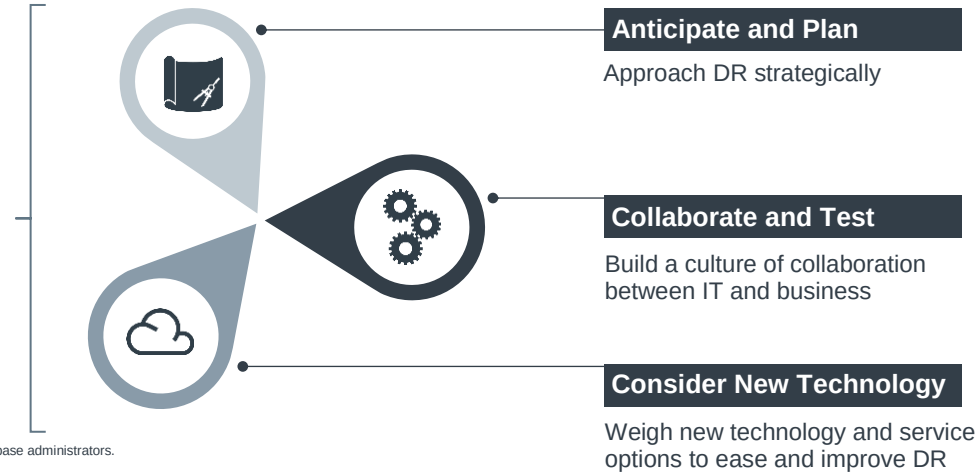
After operations returned to normal, Halifax Health held a meeting to reflect on lessons learned to improve their response in the event of another, similar incident. Key learnings included:

- Ensure all critical staff (e.g., SQL DBAs,[11] storage engineers) will be readily available and preferably on site.
- Overestimate how many service desk technicians you will need. Your need will likely increase during immediate preparation efforts and throughout a storm or incident.
- Anticipate a huge demand for cable television. Employees and families on site will want to stay updated on the progress of storms, other natural disasters, or emergency events.
- Reserve a team of individuals who can provide immediate relief support for teams that weathered the brunt of the storm or incident.
- Maintain spare cooling units available and ready in the Data Center prior to storms.
- Consider shutting down non-critical (test, non-production, non-business-hours) systems in your data center before a storm, if you have time to prepare.
- Consider a permanent secondary data center on campus, if not already available.
- Consider having the Service Desk proactively round to stay aware of what is happening in the facilities and to avoid small issues from growing.
- Review access to the backup facility prior to a disaster to ensure the right people can get to equipment at the facility, if needed.

Action Items

Below is a three-part framework and accompanying action items to approach IT disaster recovery effectively. HCOs should **anticipate and plan** appropriately for a variety of scenarios that may trigger the DR plan, **collaborate and test** the plan thoroughly with end users from across the organization, and **consider new technologies** that may improve DR response.

Areas of Consideration for Disaster Recovery



[11] SQL DBAs = SQL (structured query language) database administrators.

Author: Allyson Vicars | July 2017

Anticipate and Plan: Approach DR Strategically

- **Take an enterprise-wide view for DR planning and build a roadmap of critical assets and their interdependencies.** Today's IT systems are highly interconnected, so it is imperative to account for these broader interdependencies when you prioritize IT systems and assets to bring back online first.
- **Involve senior leadership and board.** Be transparent about the how and why of your system prioritization and even include their input during the prioritization process. Ensure they understand the ramifications of prioritizing systems in a certain way. Give clear, ROI[12]-based reasons for investment in additional DR resources that you deem critical or highly valuable.
- **Set clear expectations for your RPO and RTO.** Without this, senior leadership will likely expect you to deliver something you cannot. The middle of an incident or natural disaster is not the time when you want to explain to senior leadership that your restore point is from three days ago, a week ago, a month ago, etc.
- **Incorporate risks from a variety of sources and conduct scenario analysis to prepare for several possible situations.** System outages and downtime can come from several sources: cybersecurity incidents, such as debilitating ransomware and denial of service attacks; natural disasters, which are less frequent, but potentially physically devastating to facility infrastructure and business operations; and hardware and software malfunctions and human error. While the top cause of system unplanned downtime is human error,[13] natural and other man-made disasters still require significant and thorough advanced planning and preparation in order to recover quickly and still care for and protect patients
- **Establish clear lines of authority in advance.** Understand who has the power to make decisions in the moment, clarify the limits of your own authority, and know how you will get ahold of the decision maker during a crisis.
- **Be flexible and creative in the face of unforeseen circumstances.** Your scenario analyses and preparation cannot account for all eventualities. Particularly with natural disasters, be prepared to think on your feet, come up with quick solutions, and make do with what you have in the event additional resources take longer than anticipated to arrive or are unavailable.
- **Consider building a "clinic in a can" starter pack.** Include all the minimal equipment necessary to bring up a location quickly.

Collaborate and Test: Build a Strong Culture of Collaboration Between IT and Business Units

- **Test, practice, and assess.** Annual testing is an absolute minimum; mature organizations and other technology-dependent industries test multiple times a year and even as frequently as monthly or weekly on a rolling basis.[14] While some natural disasters, like hurricanes, can provide some lead time to prepare, this is not the case with most other sources of disruption. Identify processes that do not function smoothly in practice and provide further education to parties who need it to improve response.

[12] ROI = Return-on-investment.
[13] The 2016 Disaster Recovery Report, CloudEndure, February 2016.
[14] Masters of disaster recovery: How highly resilient organizations excel, IBM, January 2016.

Author: Allyson Vicars | July 2017

- **Include stakeholders from across the organization as well as key partners and service providers in your preparation efforts**. For key external partners and service providers, include testing requirements as part of service-level agreements.
- **Test business continuity plans in conjunction with your disaster recovery plan.** One tricky aspect of downtime recovery is that the business continuity plan, back-ups, and DR plan must all work well together. Staff needs to be trained on business continuity procedures so they know what to do when the DR plan is initiated. Ensure you do not consistently test with the same end users—all shifts, all employees must know the appropriate procedures as downtime, cyber-attacks, and natural disasters can happen at any time. Work out any issues before an event by testing all three separately and together.
- **Recognize that high system availability can work against you since your clinicians will not have experience or practice using downtime procedures.** An operational dependence on IT lends an "always on" expectation for electronic systems that many high-performing IT departments are able to deliver. Clinicians often cite patient safety at the mention of scheduled downtime, but patient safety is at risk when there is an unexpected system outage and clinical staff is unfamiliar with appropriate downtime procedures.
- **Update your DR plan regularly.** Account for changes in organizational strategies, critical systems, stakeholders, and facilities within your responsibilities.
- **Continuously update your mass communication tools and have an alternate ready.** Ensure you send updates to all staff who need to get them. Prepare for and train on an alternate communication pathway in the event the primary pathway is unavailable.

Consider Technology: Weigh New Offerings to Ease and Improve DR

- **Consider new technologies and services.** Disaster Recovery-as-a-Service (DRaaS) vendors now offer a wide range of services including virtual machine replication and activation, exercise management, customer disaster declaration service, hosting, Infrastructure-as-a-Service (IaaS), cloud-based recovery, backup-as-a-service (BaaS), cloud-based archival, and virtual desktop and unified communications recovery. Weigh whether outsourcing this would be worthwhile for your organization to free up time for your IT staff to fulfill other requirements.
- **If external technologies and services are right for your organization, develop trusted partnerships with vendors of choice.** Leverage third-party experts for disaster recovery assessments and evaluations. Include testing requirements as part of service-level agreements with vendors.

Sample Disaster Recovery-as-a-Service Vendors

- Acronis
- Axcient
- Bluelock
- C&W Business
- Carbonite
- Datto
- Evolve IP
- IBM
- iland
- Infrascale
- Microsoft
- NTT Communications
- Peak 10
- Recovery Point
- TierPoint
- Unitrends
- Verizon
- VMWare

Author: Allyson Vicars | July 2017

Appendix: CMS Final Rule on Emergency Preparedness

In September 2016, the Centers for Medicare & Medicaid Services (CMS) issued the final rule for Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers, which sets national requirements for adequate planning for natural and man-made disasters. All affected entities must comply with and implement the rule's regulations by **November 16, 2017**.

CMS's Four Core Elements of Emergency Preparedness

Risk Assessment and Emergency Preparedness	Communication Plan	Policies and Procedures	Training and Testing
• Hazards likely in geographic area • Care-related emergencies • Equipment and power failures • Interruption in communications, including cyberattacks • Loss of all/portion of facility • Loss of all/portion of supplies • Plan is to be reviewed and updated at least annually	• Complies with federal and state laws • System to contact staff, including patients' physicians, other necessary persons • Well-coordinated within the facility, across health care providers, and with state and local public health departments and emergency management agencies	• Complies with federal and state laws	• Complies with federal and state laws • Maintain and at a minimum update annually

The rule also outlines several facility-related elements including: having alternative sources of energy for basic operations; provisions for sewage and waste disposal; a system to track staff and patient location during and after emergencies; resources for safe evacuations; and space to shelter in place.

Author: Allyson Vicars | July 2017