FLIRTING WITH DISASTER: BUSINESS CONTINUITY AND DATA PROTECTION IN TODAY’S HEALTHCARE WORLD
Contributing Executives

Kurt Hildebrand  
Director, Data Center Practice Group  
Connection

David Kendrick, MD, MPH, FACP  
CEO & Principal Investigator  
MyHealth Access Network

Trey Jones  
Director, IT Infrastructure Services  
Houston Methodist
Introduction

Is your healthcare organization ready for when disaster strikes?

The use of the word “when” in that sentence is intentional. Because between the severe storms, earthquakes, floods, and wildfires Mother Nature too often provides—as well as the myriad issues caused by the deliberate or negligent actions on the part of humans—hospitals and other healthcare organizations need to be ready to respond to all manner of calamity. They need to expect the unexpected—and prepare for the worst. And, they need to have a comprehensive business continuity and data protection plan in place so they are able to quickly and agilely react to whatever threats may cross their path—and still provide the highest quality of care to their patient populations.

The need for such a plan is clear. As noted in Gartner’s Top Predictions for IT Organizations and Users, 2011 and Beyond: IT’s Growing Transparency, being unable to prevent lost data and downtime is extremely costly—every second counts. In fact, 40% of companies that experience a major disaster—regardless of whether it is of the natural or manmade variety—will go out of business if they are unable to regain access to their data within a 24-hour period. Kurt Hildebrand, Director, Data Center Practice for Connection’s Technology Solutions Group, says unexpected downtime may be even more costly for healthcare organizations.

“Healthcare organizations aren’t necessarily exposed to types of disasters that are unique only to that vertical,” he explains. “But with healthcare, what we see is that data really is mission critical—beyond just from the business perspective. Today, there are so many technology systems that are responsible for providing life-sustaining or life-providing care – and if those go down, the whole operation is put at serious risk.”
Hildebrand is not just discussing traditional life support systems you find on the hospital floor. Hospitals also rely on critical data streams and other online healthcare information technology (IT) systems to provide safe, effective care to patients. As such, data center downtime can be devastating for healthcare organizations. And this goes beyond those debilitating interruptions to patient care. The inability to adequately respond to a data center disaster can also result in significant lost revenue, weakened community trust, various government, legal, and industry penalties, and the substantial costs associated with system recovery and repair.²

“You need a plan and a process in place. The ability for information technology to remain online and operational for healthcare organizations is crucial to surviving in today’s healthcare landscape,” says Hildebrand. “You need to be ready.”

Trey Jones, Director of IT Infrastructure Services at Houston Methodist Hospital in Houston, Texas, agrees. “These days, with so many organizations moving to electronic medical records, you can render a hospital pretty much useless just by knocking out their Internet,” he says. “Organizations need to have strong business continuity plans in place so they can maintain a presence even if network communications are down. Houston Methodist, for example, has a pretty heavy daily run rate. If you knock out our ability to get to our data, you’re talking about millions of dollars in losses per day. We need the ability to get back up and running pretty much immediately in the face of disaster so we can provide our patients the care they need.”

“Organizations need to have strong business continuity plans in place so they can maintain a presence even if network communications are down.”
Challenges to Readiness

There are many benefits to strong business continuity management in the business world. The recent IBM-sponsored Ponemon Institute: 2016 Cost of Data Breach Study uncovered that having business continuity management processes in place significantly reduced the time required to identify and contain data breaches—as well as the average total cost of such incidents. Furthermore, this industry-wide global study reported that 76% of companies surveyed without business continuity plans said they experienced material disruption to their business operations in the face of data breaches.

With the patient care mission, one can see why business continuity may be even more important to the healthcare industry. Yet, despite the benefits outlined by the Ponemon report, Hildebrand says that too many healthcare organizations are leaving their data centers vulnerable to disaster.

"Unfortunately, what we see is only about 40% of organizations today have what we would consider a fully viable disaster recovery strategy," he says. "The other 60% fall on some spectrum of partial coverage. And, in doing so, they really are leaving themselves exposed to some serious risk."

Why do so few organizations implement a full disaster recovery strategy? David Kendrick, MD, MPH, FACP, CEO and Principal Investigator of Oklahoma’s MyHealth Access Network, says one of the greatest challenges is that so many healthcare organizations are running on “very old” data systems and system architectures.
“You have these newer electronic health record systems running off code that was written in the late 80’s or, if we’re being generous, the early 90’s. Almost all major health organizations use these older platforms,” Kendrick says. “That older architecture not only involves a lot of overhead to maintain, it also has a lot of points of failure that need to be monitored—with so many systems in play, you’re really doubling, at the very least, your vulnerability points. It can be difficult to keep up with them all.”

And that older IT infrastructure becomes a larger issue when you consider a second challenge: that most hospital organizations, as Hildebrand puts it, are “grounded.” Not only might open and working healthcare facilities be desperately needed in the event of a natural disaster—but, even in the case of man-made problems, most hospitals and other care facilities are simply not built to move in response to a crisis.

“A hospital can’t just pick up in the event of a disaster and just move to some alternate work location. The equipment and the IT systems are very much attached to that facility,” he explains. “Some healthcare organizations are more mobile, like a mobile clinician’s office, but often they, too, are tethered to the larger organization or health system. What that means is that, specifically to healthcare, the ability for information technology to remain online with minimal disruption, or even zero down-time, is a requirement for many different types of healthcare organizations. And that requirement can make developing the right plan seem quite overwhelming.”

“Specifically to healthcare, the ability for information technology to remain online with minimal disruption, or even zero down-time, is a requirement for many different types of healthcare organizations.”
With so many potential threats in play, it can be difficult to know which require the most investment of resources. In terms of natural disasters, many organizations focus on the type of events that occur most in their area. For example, as a hospital that lives in Houston’s so-called “underwater zone,” Jones says Houston Methodist spends a lot of time thinking about hurricanes and flooding.

“Power was out for 23 days during Hurricane Allison in 2001. But the hospital still had a lot of paper processes in place then so they were able to continue even with hampered local services,” he says. “It’s the tropical storm that can really mess things up for us—the water and the wind can just rapidly decimate the power grid. So, we think a lot about that, and how we can mitigate those issues, when we think about our business continuity and disaster recovery plans.”

Other hospitals, depending on their geographic region, might have more of a focus on tornadoes, earthquakes, or other natural disasters.

But man-made disasters can be just as devastating. Today, many healthcare systems are also putting significant resources into protecting themselves against ransomware attacks. And for good reason. Healthcare organizations are known for being a “perfect mark” for ransomware attempts due to their need for immediate access to patient data and lack of cybersecurity awareness. In fact, the Federal Bureau of Investigation (FBI) went so far as to issue a specific warning to healthcare organizations in 2014 regarding hacks, including ransomware attacks, suggesting that health data was far more valuable than credit card numbers. With such warnings, as well as high profile attacks like the WannaCry ransomware threat in 2017, many organizations are making hacks the focus on their disaster recovery efforts.

“Hackers are always upping their game, and we have to be able to meet that,” says Kendrick. “With so many different systems and platforms in place, we often bring events from one platform to another, and, if we aren’t careful, some unexpected events can come across with the wanted events and cause problems.”
But ransomware doesn’t have to be considered in a vacuum. A comprehensive disaster recovery plan will help protect your organization from any hacking threats, ransomware or otherwise, Hildebrand says.

“Certainly, the success of ransomware attacks recently showcases the great need for disaster recovery plans. These attacks show just how practical and useful having a disaster recovery plan in place can be—because organizations that have them in place are able to ignore the ransomware. They can just say, ‘We got compromised, delete that system, restore the data, no problem,’” and not even think about having to pay the ransom. But you need to be sure that your plan, that same plan that can help protect your organization from ransomware, can help you stay up and running during other types of disasters as well.”

Which can include simple human error. Jones says that another grave concern for many organizations is the one that struck Amazon Web Services’ servers in May 2017: the “fat-fingered server engineer.”

“It’s one of the most dangerous scenarios—because people make mistakes,” he says. “And server engineers have so many rights, so much capability to impact the back end of your IT environment, a single mistake can take hours and hours of recovery time. You need to be prepared to deal with that.”

According to Netwrix’s 2017 IT Risks Survey, human error was one of the most common causes of security incidents—with 29% of respondents saying that incorrect user activity led to significant downtime for their data centers.

A strong, comprehensive business continuity and data protection strategy will consider all these scenarios—and more. “You have to assume that the worst can and will happen. And you need to have a back-up plan for each of those scenarios,” says Kendrick. “You almost have to think like a dystopic futurist to prepare yourself. And then you have to weigh the costs of protecting yourself against all those events with your other operating costs. It’s a difficult balancing act—but it’s one we need to get better at doing in healthcare.”
Process Over Technology

Too many organizations may feel that they are protected because they have back-up systems and other security technologies in place. And while Jones will be the first to tell you there is no substitute for a good back-up solution, it should not be the only shield in your disaster recovery arsenal. Kendrick agrees.

“Back-up and recovery is important. But you use the back-up and recovery after the bad event has already happened and you are trying to recover from it,” he explains. “A good disaster recovery plan is going to have a lot of prevention in it. You are going to have a plan in place to prevent these issues from happening—and that plan needs to be in play all day, every day. It’s the difference between getting a vaccine to prevent measles or giving someone a drug to treat the disease later in life. You want to do everything you can to prevent the bad stuff from happening.”

And that comes down to having strong processes in place to support your business continuity and data protection efforts.

“A disaster is like a big giant square. And you are only able to shoot circles at it. And you never have any circles that are as big as the square,” says Jones. “So you have to make sure you know what those circles are and that they have them at the ready so you can just keep plugging and throwing more and more circles at it so you can avoid the disaster altogether or have a short recovery window.”

And that’s where having a trusted advisor can help you. Kendrick says having the right advisors can help you develop a unique, workable disaster recovery plan—to find that balance he spoke of in terms of results and resources.

“A rare small percentage of disaster recovery is the software,” he says. “If you have the people and the process in place to keep you blocking and tackling, each and every day, you’ll find that you’ll catch issues earlier, or even avoid problems altogether, even if there are the occasional lapses in the software. This goes beyond just reviewing and checking all the boxes regarding security the federal government puts in front of you. It’s about knowing your organization’s needs, identifying potential gaps, and putting a plan in place that will help you stay up and running no matter what occurs.”

But any plan worth its salt has to be tested regularly. Hildebrand says that too many organizations drop the ball when it comes to disaster recovery efforts because they don’t conduct regular testing.
“This has to be part of your process. It doesn’t matter how good or expensive your technology is—or what it does in theory—if you don’t test it to make sure,” he says.

Jones agrees. “Delivery on day 1 is easy. Delivery on day 300 is harder. And delivery on day 1000 is even more difficult. You need to keep working and testing and making sure the processes and systems you put in place are doing the job you set them out to do,” he says. “You need to test the system—think outside production. And think about how you can get what you need up and running somewhere else rapidly. You can’t know all the potential pitfalls, and all the potential gaps, unless you are constantly testing.”

“You need to test the system—think outside production. And think about how you can get what you need up and running somewhere else rapidly. You can’t know all the potential pitfalls, and all the potential gaps, unless you are constantly testing.”

— Trey Jones
Beyond Theory into Practice

Disaster recovery, by its very nature, is challenging. Today’s healthcare organizations need to protect themselves from a wide variety of threats and still continue their mission of quality patient care. With limited resources, it can be difficult to know where to begin. But Jones says that it starts with making business continuity an intrinsic part of an organization’s overall IT strategy.

“This needs to be part of your traditional IT strategy. There should be disaster recovery milestones as part of every project they run,” he says. “An organization’s Chief Information Officer (CIO) should be the flag carrier. And if you don’t have the talent in shop to handle some of these efforts, bring people in. Because you need to be able to answer questions about how you’ll get this application up and running from another place, how you’ll get to this data, how you’ll handle this problem or that problem if we get hit by a hurricane or by some other issue.”

Hildebrand doesn’t downplay the potential challenges of putting a strong strategy in place. Yet, he says the investment in that upfront planning and regular testing to meet your organization’s business requirements will pay off in the long run.

“A lot of times, disaster recovery will come from the top down. Someone in the C-suite decides you need a good strategy in place,” he says. “But once you have the strategy, you need to drive the implementation of that disaster recovery strategy from the bottom up. You need to ask yourself what you really need in order to continue day-to-day business operations, what happens if you are down more than four hours, what applications need to be available in real-time, and so on. You need to start this process at the business level and then give those business requirements to your IT organization or to a trusted advisor outside your organization so they can design a technology solution that works the way you need it to. And, over time, in doing so, you’ll find that strategy, and the accompanying solution, can help your organization stay up and running no matter what is thrown your way.”

To learn more about how your healthcare organization can develop and implement a comprehensive business continuity and data protection plan to help mitigate issues caused by disasters both natural and man-made, visit the experts at Connection.
Additional Sources