spōk

2018 GUIDE:

HOW TO PROVE THE VALUE OF BUSINESS CONTINUITY

Does your hospital have the technology, resources, and a plan in place to meet today's business continuity requirements? A solid business continuity plan will help you avoid downtime in the face of security threats, natural disasters, and other adverse events.

Here's what every healthcare leader and IT professional should know about business continuity.

IS YOUR IT DEPARTMENT PREPARED TO RESPOND TO AND CONTROL A CRITICAL EVENT?

In a Spok survey of CHIME CIOs conducted in early 2018, we asked healthcare leaders how confident they are their organization could recover from a disaster scenario. Sixty-five percent of CIOs told us they're 'somewhat' or 'not very' confident, while five percent reported 'no confidence.' Ideally, every CIO should be highly confident, yet only thirty percent say they are.[1]

What's more, when asked about their top three business continuity concerns, CIOs said the inability to treat patients (73 percent), damage to their hospital's reputation and credibility (61 percent), and loss of revenue (58 percent) were top of the list.[2]

Think about the way your hospital handles business continuity and disaster recovery.

- Do your plans distinguish between business continuity and disaster recovery?
- Have you planned and invested in recovery for all systems and applications, or just those affecting patient care (such as the EHR)?
- Has your recovery budget increased or decreased and was that decision based on calculated costs of downtime (or other factors)?
- Does your plan address all types of risk and threats?
- Is your plan regularly reviewed and tested so it's ready when needed?
- Have you discussed business continuity with your vendors and business partners?

We gathered industry insights to help you answer these tough (but necessary) business continuity questions.

THE DIFFERENCE BETWEEN DISASTER RECOVERY AND BUSINESS CONTINUITY

Over a decade ago, business continuity started evolving at a rapid pace, moving beyond the tried-and-true disaster recovery methods developed during the 1960s and '70s.[3] IT departments developed redundancies to recover their systems and data from onsite data centers should a disaster render that technology unavailable. But as technology advances, and more applications and data move to the cloud, it's crucial that recovery priorities be reassessed and take on a broader view of business continuity. What was considered the norm a few years ago may not support new systems, threats and risks, or changing business goals. Healthcare organizations must look beyond disaster recovery to assess the larger picture of business continuity.

Disaster recovery is the process of getting all important IT infrastructure and operations up and running following a disruptive event or outage. It's a reactive recovery process that occurs when critical operations have been interrupted or stop completely.

> **Business continuity is more than just having redundant systems. It's a comprehensive approach that enables critical services to be delivered without interruption. Instead of focusing on how you'll resume business after operations have ceased (or recovery begins), business continuity is the plan by which you keep your hospital operational during and after a disaster.**

This includes your call center, mission critical systems and applications, and personnel. Business continuity often accounts for not only disaster scenarios, but other disruptions such as departure of key staff, partner/vendor/supplier problems, or any other number of challenges.

Despite these distinctions, the two terms are often used synonymously or lumped together under the acronym BC/DR because of their many common considerations. Therefore, it's important for healthcare leaders and IT departments to understand how business continuity differs from disaster recovery—managing a critical event is not the time to learn the difference, so we've outlined the basics of business continuity every healthcare leader and IT professional should know.

WHY PLANNING IS IMPORTANT, AND WHY INVESTMENT STRATEGIES ARE MORE IMPORTANT

For healthcare providers, a business continuity plan enables the continuance of business operations and patient care. Investing only in recovery systems for those systems impacting patient care, like the EHR, is not sufficient. Virtually every hospital IT system impacts care delivery. Consider a disaster scenario causing your clinical communications to fail. If that system doesn't have the appropriate recovery capabilities, your doctors, nurses, call center operators, and other staff will not be able to talk to one another as a care team.

Healthcare organizations must approach business continuity with a new mindset: focusing on overall business risks, not just IT systems. Knowing the cost of downtime for each of your systems and applications is crucial. This will help you determine recovery time objectives (the maximum length of time within which each business process must be restored). This is especially important for your mission critical applications. Once you've identified the systems requiring the most protection, you'll know how to prioritize your resources and where to invest in additional backup, disaster recovery as a service (DRaaS), fault-tolerance servers, etc.

For most organizations, the major concern is the EHR system and electronic patient health information (ePHI), both requiring access on a 24/7 basis. As noted earlier, one of the top business continuity concerns for CIOs is the inability to treat patients (73 percent). Hospitals rely on the EHR because it's linked to many hospital functions, including admitting, billing, pharmacy, radiology and laboratory systems.[4]

> **Patient safety and quality of care is increasingly dependent on the EHR and other integrated technology, so the business continuity plan should outline a recovery time objective that can restore operations without seriously affecting the organization's ability to provide patient care.[5]**

When developing a business continuity plan, it's important for healthcare leaders to consider intangible losses, such as damage to hospital brand and reputation, loss of customers, impact to credit rating, or loss of contracts. Generally accepted standard financial measures and damage quantification methodologies can be used to estimate the financial impact.[6]

BUSINESS CONTINUITY BUDGETS

More CIOs say they're cutting costs than increasing investments[7]

61%
are cutting costs without adding risk

39%
increased their budget

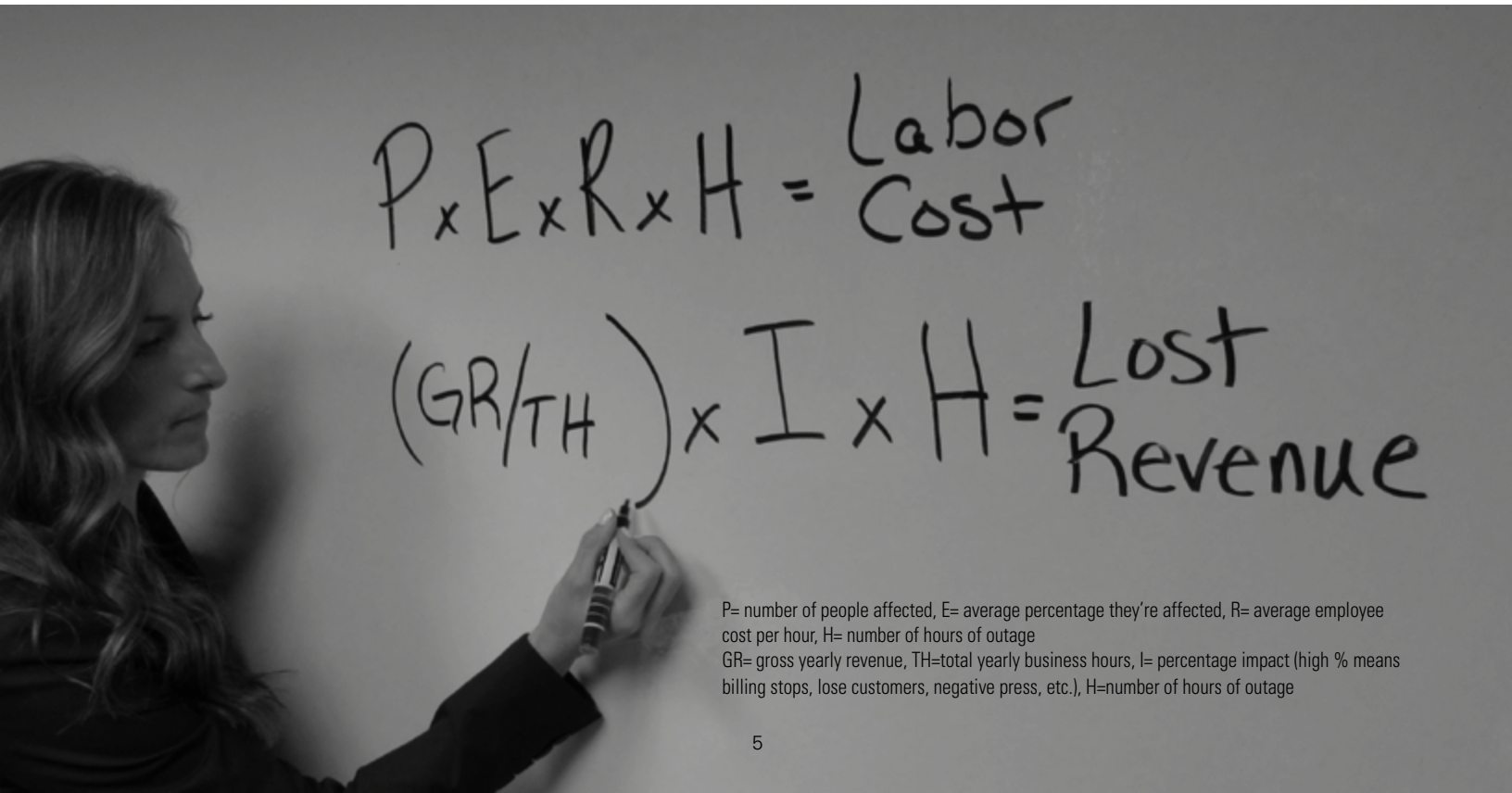
CALCULATING DOWNTIME

Every organization has a unique set of disaster recovery and business continuity requirements. Yet many are expected to have 99.999 percent availability, which equates to approximately 5 minutes of unscheduled downtime annually.[8] This expectation of near-zero downtime poses challenges when justifying IT budgets and the costs associated with ensuring this level of availability and/or recovery. According to a 2016 report from the Ponemon Institute, the total cost of a single, unplanned outage for healthcare organizations is $918,000.[9] Your budget might never be large enough to invest in resources and redundancy for every system and application, or to prevent every possible disaster.

Quantifying the cost of downtime is a good strategy to defend budgeting for these costs, especially for resources that you've prioritized for mission-critical applications. Here are a few cost factors to consider:

- Employee productivity:[10] The labor cost, including overtime (during downtime and recovery) for employees who would be impacted can be calculated as shown below (you can factor this at 50 percent if your employees could work on other tasks during downtime).
- Loss of business/revenue:[11] Some calculate this using average revenue per minute (ARPM), or as shown, by estimating the total annual cost of outage (multiplying lost revenue by the total expected annual hours of outage).
- IT recovery costs and restoring systems (out-of-warranty acquisition costs)
- Costs associated with potential compliance violations
- Outside vendor and consulting costs

Some hidden costs you may not have thought about include customer dissatisfaction, damage to your brand/reputation (including negative press), and lowered employee morale or turnover.[12]



P= number of people affected, E= average percentage they're affected, R= average employee cost per hour, H= number of hours of outage
GR= gross yearly revenue, TH=total yearly business hours, I= percentage impact (high % means billing stops, lose customers, negative press, etc.), H=number of hours of outage

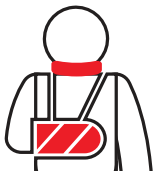
DEVELOPING A PLAN BY IDENTIFYING RISK

Every day hospital care teams respond to emergency situations requiring immediate action—often when a minute can mean the difference between life and death. As physicians, nurses, and caregivers respond to code calls and other important notifications, your hospital is most likely tracking response times, evaluating workflows and current technology, and identifying areas that could be improved. This type of analysis has allowed care teams to respond more efficiently and quickly to patient events, such as a code STEMI (ST-elevated myocardial infarction) for heart attack patients.

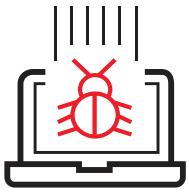
Each of these common code calls and alerts may be put at risk by events ranging from natural disaster, terror and security threats, power outages, and more. Every organization is vulnerable to potential disasters. Every organization should prepare their business continuity plan to be adaptable to a wide range of possible risks.

Here are some common code calls, disaster events, and other disruptions that a business continuity plan should address:

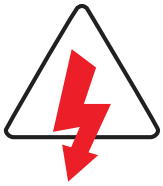
Natural disasters



Accidents



Cyberattacks, malware, denial of service (DNS) attack

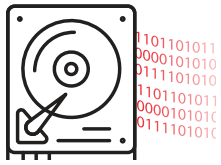


Power failures/ energy disruptions

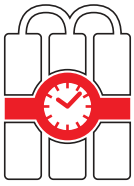
Environmental disasters

Communications, transportation, safety and service sector failure

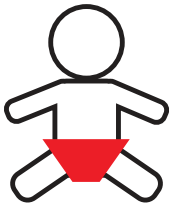
Thefts and vandalism



Loss of data center, data corruption



Bomb threats



Infant/child abduction

Loss of key staff members

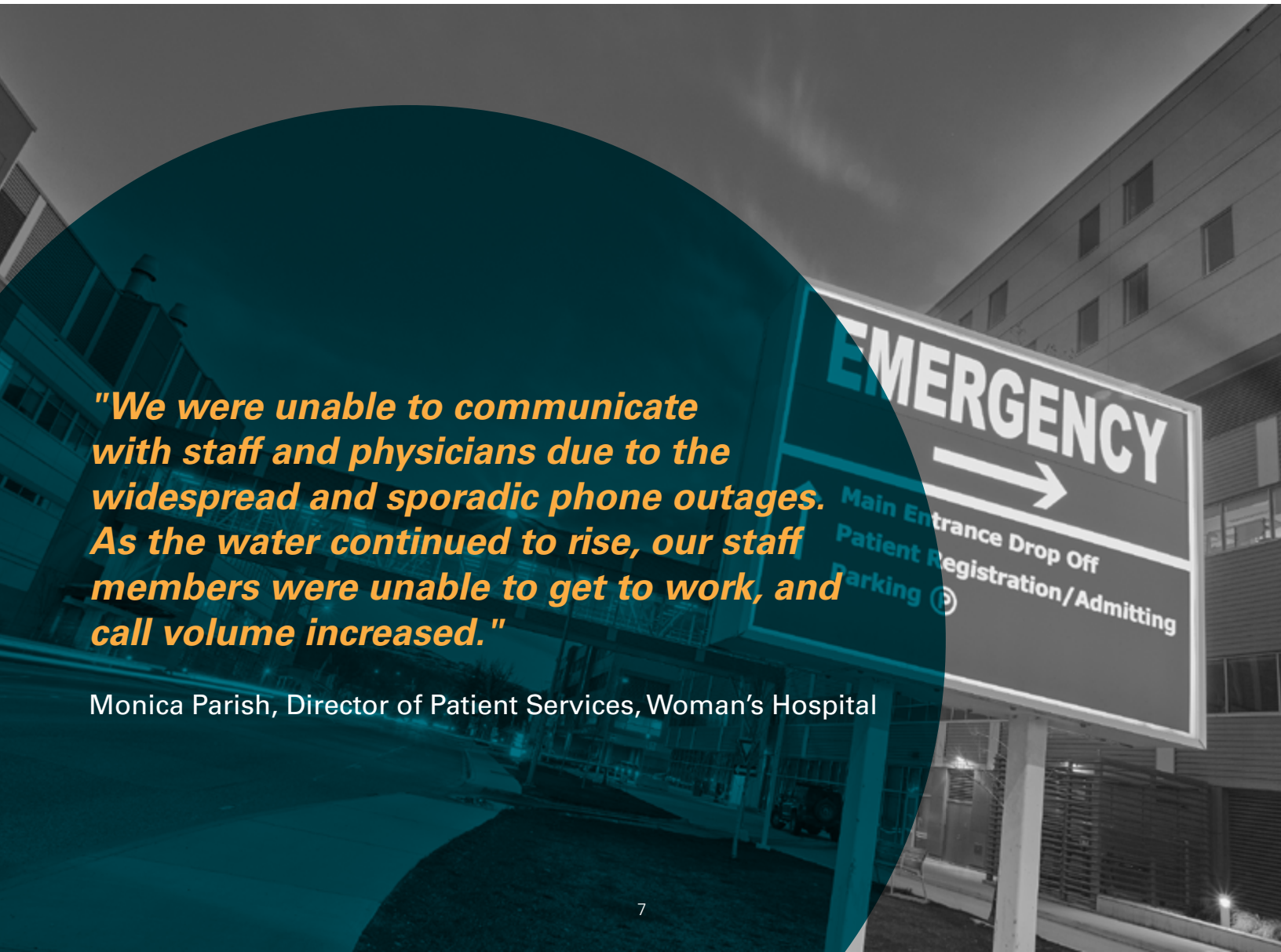
EHR vendor or other vendor failure

In addition, outcomes from some of these events can lead to loss of access to your physical building, medical equipment, paper or electronic health records (including billing, scheduling, and patient charts); unavailable staff members; and third-party data breach.

Developing your plan is the first step to successful business continuity. The second step involves testing your plan.

Woman's Hospital confronted a disaster scenario in early August 2016, when Louisiana faced a severe weather system resulting in record-level flooding.

Read how Woman's Hospital put their communication infrastructure to the test »



"We were unable to communicate with staff and physicians due to the widespread and sporadic phone outages. As the water continued to rise, our staff members were unable to get to work, and call volume increased."

Monica Parish, Director of Patient Services, Woman's Hospital

TESTING YOUR PLAN

The principle of Murphy's Law states that, 'if it's possible for something to go wrong, it will go wrong.' This adage reminds us of the importance and need for business continuity, and that however much we invest and plan, we never completely identify and prevent all risk.

Developing your business continuity plan may have been an overwhelming task: Practicing how to respond to adverse events isn't any easier. Every crisis is different—unexpected and unpredictable circumstances will arise. Testing your plan and repeatedly practicing your response will help your organization, employees, and patients be more resilient.

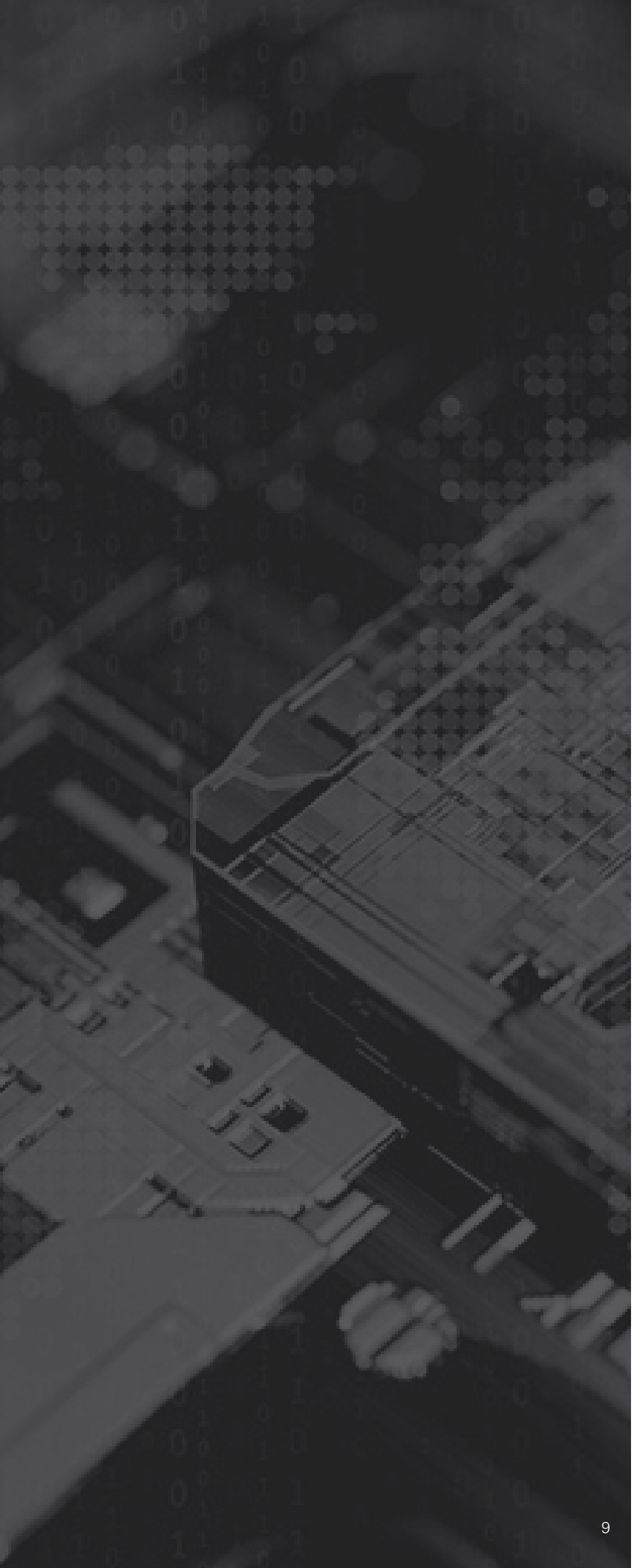
When asking hospital CIOs how often their organization tests its business-continuity plan, 56 percent test annually, 10 percent quarterly, and 10 percent test on an ongoing basis. Alarmingly, 10 percent were not sure how often their organization tested its plan, and 14 percent said they never test.[13] What's the corrent answer?

> **Organizations should test their plans periodically, as needed to ensure their plan is complete, effective, and allows staff to get hands-on practice executing it.**

Testing may be initiated after updates are made to the business continuity plan, following organizational changes, or to validate the operability of a single IT system and application, often those deemed mission critical. Therefore, testing exercises take many forms:[14]

- **Component testing:** Tests individual software or hardware components considered mission critical.
- **System testing:** Tests complete systems, such as the EHR, which evaluate the systems' compliance with specified requirements.
- **Comprehensive testing:** Tests all systems and components and is considered extensive in scope, such as testing data backup sites in the event of power outages.

Once you have selected the level of testing you want to perform, you need to determine the best format of testing for your organization. As many systems within a healthcare organization are mission critical and require 24/7/365 operations, it may not be practical to perform a disruptive test. The following are typical testing formats:



- **Paper test:** Individuals read and annotate recovery plans.
- **Walk-through test:** Groups walk through plans to identify issues and changes.
- **Simulation or tabletop test:** Groups go through a simulated disaster to identify whether emergency response plans are adequate.
- **Parallel test:** Recovery systems are built/set up and tested to see if they can perform actual business transactions to support key processes. Primary systems still carry the full production workload.
- **Cutover test:** Recovery systems are built/set up to assume the full production workload. You disconnect primary systems.

Every organization has unique requirements, which means frequency and formats of business continuity testing is different for everyone. To help establish and document a testing regime that fits your organization, a testing schedule may prove beneficial.[15]

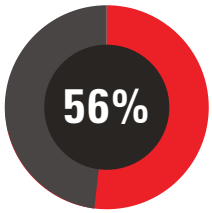
A test schedule outlines when tests are performed, what systems are tested, and how they are tested, including testing mandated by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule 164.308 (a) (7) (i) under administrative safeguards.[16]

DISCUSS BUSINESS CONTINUITY WITH VENDORS AND PARTNERS

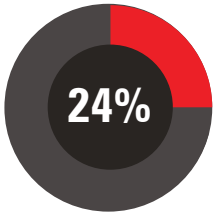
How many vendors and business partners does your organization use for basic services or supply chain—and who has access to your network? A Ponemon Institute survey found that data breaches caused by third parties are on the rise: Fifty-six percent of respondents experienced a breach caused by a third party, and only 57 percent had a complete list of all the third-party companies they did business with.[17]

The healthcare industry relies on a vast number of systems, applications, and technologies, including the EHR. Many of those systems are outsourced to business partners. It's important to know the specifics of your vendor's plan, but remember vendor continuity doesn't negate the need for your own disaster recovery systems.

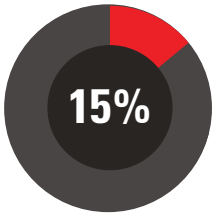
A Spok survey of CHIME CIOs asked respondents if they know which vendors have recovery plans in place to support their hospital's operations in a disaster scenario, and whether their support is part of their business continuity plan?[18] Here's how CIOs responded:



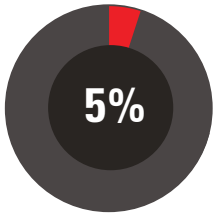
Yes, and vendor support is a key requirement of our plan



No, but we would use their support



Yes, but vendor support is not part of our plan



No, we would NOT use their support

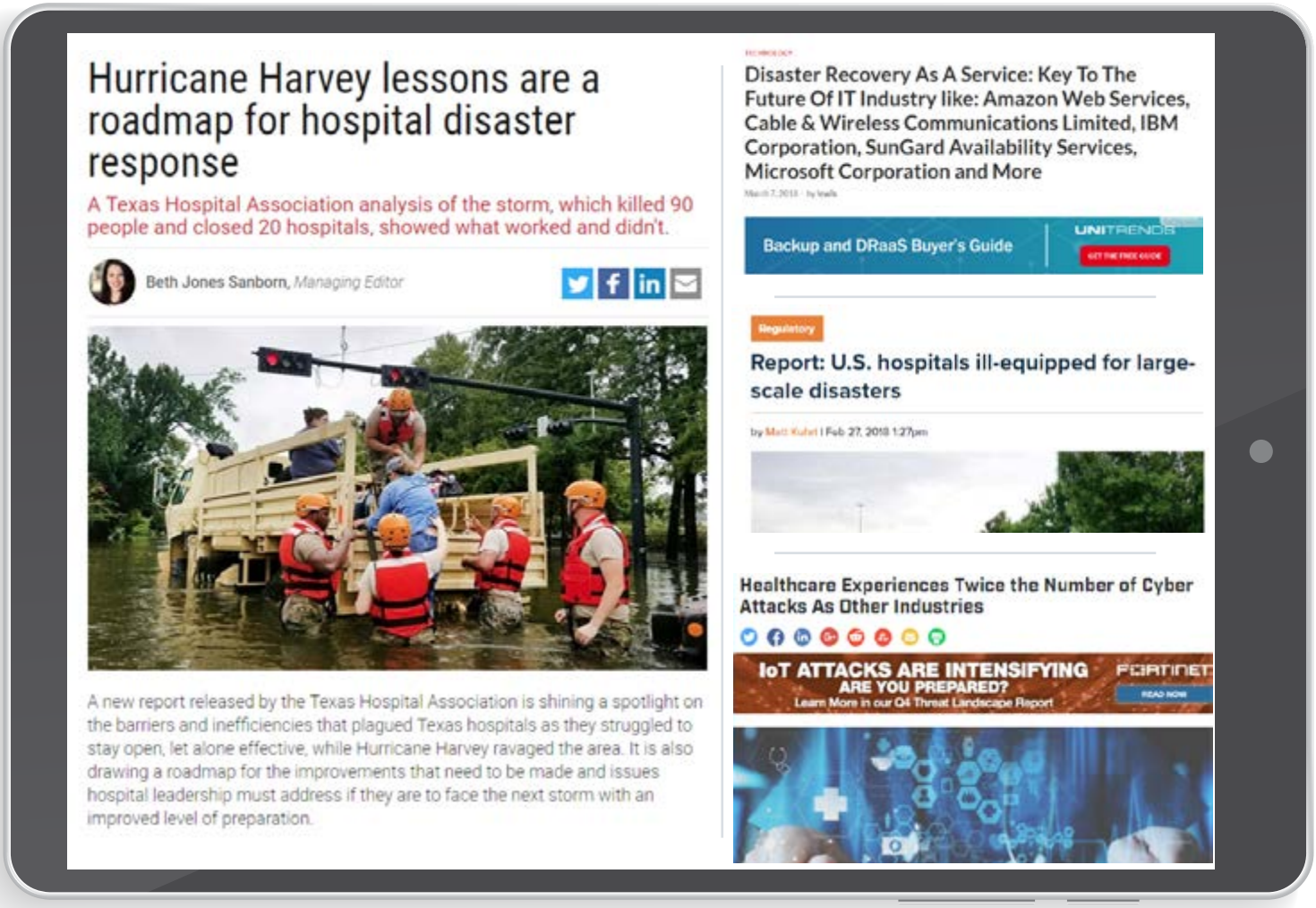
Just over half of healthcare organizations say they're using vendor expertise and services to assist in business continuity planning.

CONCLUSION

Last year, healthcare was the most targeted industry for malware attacks, accounting for 40 percent of all security incidents in the third quarter,[19] and the U.S. experienced 15 natural disasters with losses exceeding $1 billion each.[20]

> **The headlines in 2018 indicate these adverse events will continue, which has experts warning "it's not a question of if, it's a question of when" an organization will experience a threat to business operations.**

Murphy's Law reminds us that however much we invest in and prepare our business continuity plan—we never eliminate all risk. Emergent cybersecurity risks, and the increasing complexity of hospital IT systems have raised the alarm among healthcare IT leaders, who can no longer leave management of business continuity to IT departments alone. Disruptive and adverse events are no longer events of chance, and healthcare leaders must face the changing needs of business continuity.



References

[1, 2] Spok Survey of CHIME CIOs. (2018, January). Business Continuity in 2018 [survey].

[3] Yeager, D. (2012, June). Split Decisions—Separate Disaster Recovery and Business Continuity Plans Make Sense [journal].

[4, 5] Rozek et al. (2008, March). Business continuity planning. Health Management Technology [article].

[6] Deloitte. (2016). Beneath the Surface of Cyberattack [report].

[7] Spok Survey of CHIME CIOs. (2018, January). Business Continuity in 2018 [survey].

[8] Duffy, C. (2014, June 27). Qualifying and Quantifying the Cost of Disaster Recovery (DR) / BCP [article].

[9] Ponemon Institute. (2016, January). Cost of Data Center Outages [pdf].

[10, 11] CoreSpace. (2016, February 20). Downtime and Outages – Understanding Their True Costs [article].

[12] Duffy, C. (2014, June 27). Qualifying and Quantifying the Cost of Disaster Recovery (DR) / BCP [article].

[13] Spok Survey of CHIME CIOs. (2018, January). Business Continuity in 2018 [survey].

[14, 15] U.S. Department of Commerce. (2006, September 21). Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities [report].

[16] Supremus Group LLC. (2016). HIPAA Security Contingency Plan Consulting [website].

[17] Ponemon Institute. (2017). Ponemon 2017 Third Party Data Risk Study Your Organization Can't Afford To Ignore [report].

[18] Spok Survey of CHIME CIOs. (2018, January). Business Continuity in 2018 [survey].

[19] McAfee. (2017, December). McAfee Labs Threat Report [pdf].

[20] NOAA National Centers for Environmental Information (NCEI). (2018). U.S. Billion-Dollar Weather and Climate Disasters [website].

[21] Adefala, L, (2018, March 6). Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries [article].

[22] Sanborn, B. (2018, February 9). Hurricane Harvey lessons are a roadmap for hospital disaster response [article].

[23] Kuhrt, M., (2018, February 27). Report: U.S. hospitals ill-equipped for large-scale disasters [article].

[24] Thomas, K. (2018, March 7). Disaster recovery as a service: key to the future of IT industry. Business Services [article].

spōk℠

ABOUT SPOK, INC.

Spok, Inc., a wholly owned subsidiary of Spok Holdings, Inc. (NASDAQ: SPOK), headquartered in Springfield, Virginia, is proud to be the global leader in healthcare communications. We deliver clinical information to care teams when and where it matters most to improve patient outcomes. Top hospitals rely on the Spok Care Connect® platform to enhance workflows for clinicians, support administrative compliance, and provide a better experience for patients. Our customers send over 100 million messages each month through their Spok® solutions. When seconds count, count on Spok.

spok.com

/Spoktweets

Rev: 3/18