RSA

WHITE PAPER

Produced in partnership with:

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

STRATEGIES FOR MANAGING BUSINESS DISRUPTIONS

Organizations strive to maintain business continuity to ensure continued productivity and efficiency in the face of disruptions.

However, unexpected business disruptions can occur, from technological to natural to manmade. And organizations that are not prepared to handle an array of disruptions are left to scramble, risking employee and patient health in the process.

No organization can be prepared for every possible disruption. Even those most prepared to respond to the current crisis did not anticipate it being as long or severe as it would be.

Business continuity plans need to be sufficiently prescriptive to provide organizations direction during uncertain times but likewise flexible to adapt to ever-changing circumstances.

To understand how organizations were managing business continuity during disruptions such as the pandemic, RSA commissioned Xtelligent Healthcare Media to conduct a survey of healthcare industry leaders about their thoughts on decision-making during the current crisis and its impact on future strategies.

Results highlight three common challenges facing organizations during the current crisis that they are likely to encounter again in the future: 1) managing a remote workforce, 2) managing third-party partnerships, and 3) continuing digital transformation. Two survey respondents also completed qualitative follow-up interviews to discuss the survey findings further and highlight key strategies to success in these areas at their organization.

CURRENT BUSINESS CONTINUITY PLANS

Business continuity planning is not new to the healthcare industry. Hospitals, health systems, and provider clinics must always be prepared to handle the unexpected while continuing operations and providing patient care. But the pandemic presented new challenges to the industry as it has persisted well beyond initial expectations.

“Our business continuity plan did not cover the extent of the situation or the length of time that this has been going on for,” said a security director of an academic medical center (AMC). “We had to adapt pretty quickly.”

Perhaps the most significant component of this response is that IT infrastructure was called on to support a remote workforce and leverage telehealth solutions.

"Most large independent practices (organizations) have robust recovery capabilities. (For example) If the main data center were to get wiped out, there are strong recovery capabilities," a clinically integrated network (CIN) director pointed out. "The bigger challenge around business continuity is usually not so much the computing systems if you have a disaster recovery capability in place. It is really the ability for people to be able to continue doing their work. It is more about support."

This sentiment echoed that of survey respondents who indicated that the biggest challenge to resiliency during disruptions was maintaining continuity of patient care. Managing the crisis event and scaling to meet increased demand for patient care were next on the list of priorities.

From an IT resource and backup capability perspective, organizations were less concerned. What mattered most was people.

"We designed the business continuity plan not so much based on how to continue to keep a computer system running but actually focusing on alternative work locations and accommodations people need to work from home," the director continued.

Due to the pandemic, part of ensuring employees are taken care of is providing resources to support remote work, including protecting them. Thirty-nine percent of survey respondents said their organization had IT security in place to enable and protect their remote workers.

A security director of an academic medical center (AMC) confirmed this by saying, "We were uniquely prepared to move to an online environment pretty quickly. A lot of the systems that we had were already in the cloud. And we already had a plan."

Once the infrastructure was in place to promote a remote environment, organizations felt confident in their ability to support staff, provider, and patient needs.

STRATEGIES TO MANAGING A REMOTE WORKFORCE

Shifting to a remote work environment can be a challenge for many. Staff members are accustomed to being in an office environment and walking to a coworker's desk to ask a question at any time. And providers and patients are used to meeting in person.

"Overall engagement is the biggest challenge. People are used to being in an office and being able to chat face-to-face. Now everybody's remote," reported the security director.

The greatest challenge to managing a remote workforce was providing employees with necessary IT tools (62%). The second-toughest challenge was enabling employees to be productive, according to 52% of respondents. Both highlight the difficulties of supporting a productive work environment as if the employee were sitting in the office.

"As far as our technology infrastructure and our work support capabilities, including controls from a policy point of view and human resources, to what's supported by IT, those were all flexible to allow people to shift to telework," the CIN director emphasized. "We had a pretty complete set of capabilities to continue working as if we were sitting in our normal office."

Making the transition to remote work relatively seamless can be credited to robust technological capabilities. Eighty-one percent of respondents identified this as a strategy they were already employing to manage employees who worked remotely. Telemedicine capabilities, security controls to protect remote online work, and flexible work hours were also critical ongoing strategies according to 70%, 67%, and 63% of respondents, respectively.

These plans promote flexibility and ensure employees, providers, and patients can maintain some level of continuity during a chaotic time.

"It's been demonstrated that people can work from home, be productive, and still help organizations meet their goals," reported the AMC security director. "So, a lot of departments are now rethinking work from home policies."

STRATEGIES TO MANAGING THIRD-PARTY PARTNERS

Third-party organizations play a unique role in maintaining business operations. They can fill critical gaps and help organizations achieve their objectives.

But partnerships require a level of trust between the organization and the third-party vendor. To effectively manage these partnerships, 45% of survey respondents said they performed risk assessment to identify areas of third-party risk.

At the academic medical center, there is a third-party review process in which employees must submit a request to leverage new commercial technology. "We basically look at things like: What kind of data the application is storing? Is it storing patient data or employee data? If the answer is no to any of these questions, the process is a lot more straightforward and very simple to follow," he explained. "If the answer is yes to any of those questions, then we have a longer process and more teams involved who assist in decision-making to ensure the data is secure."

Understanding third-party risk can be a complex undertaking. Twenty one percent of survey respondents said that just tracking these organizations was difficult. Forty-eight percent reported that understanding and managing the security risks of third-party vendors was one of their most significant challenges to managing these relationships. Another 33% indicated truly assessing a third party's overall risk to be a challenge. Twenty seven percent of organizations also noted that getting third parties to reduce their own risk was an additional challenge. With uncertainty having become the new normal, organizations may have even more difficulty assessing and monitoring these partnerships.

As a result, many organizations turn to a hybrid vendor model, managing some resources in-house and others exclusively with their vendor.

Partnerships between vendors and in-house IT can increase ease of use and efficiency. At the academic medical center, this occurred in the area of cloud management.

"We rely on a lot of third-party vendors that are already on the cloud for things like our learning management system to our EHR. All those systems are hosted elsewhere," the AMC security director noted.

Diversifying vendors is also a strategy that organizations are leveraging to manage third parties, according to 11% of all respondents.

The CIN director highlighted the importance of this strategy. Before the COVID-19 pandemic, his organization was using a variety of video-communication vendors.

"In some parts of the organization, we were using all of them," he explained. "That wasn't necessarily efficient, but we had experience with all of them. So, when we had a shift to a mode where it was absolutely critical to communicate this way, we had all these options available."

When one of these platforms was updating or slowed because of increased demand, the organization was able to transition seamlessly to another provider.

"We got lucky because we probably overbought by having multiple vendors that were under contract," he said. "Having an excess set of redundant tools helped us during this time."

In normal times, this strategy is untenable as it does not promote cost-efficiency, but diversifying its vendor selection enabled the clinically-integrated network to maintain standard operations. When one system failed, another available filled the gap and business continuity remained intact.

DIGITAL TRANSFORMATION AND PLANNING FOR THE FUTURE

Since the pandemic introduced unprecedented business disruption, many organizations are reimagining their continuity plans to incorporate best practices learned from the pandemic into future strategies.

A key element in organizations' response was a robust IT infrastructure that allowed employees and care visits to occur virtually. In fact, 55% of respondents believe that business disruptions, such as the pandemic, have accelerated digital transformation.

Twenty-eight percent said digital transformation at their organization has remained the same amidst the disruption, and only 3% reported a decline in digital transformation.

At the academic medical center, the current disruption gave the organization the necessary push to make changes that were put off for years, the representative from an academic medical center pointed out. "Before the pandemic, we were slowly looking at consolidating tools and workflows. We have a pretty siloed IT department," the AMC security director explained. "There have always been plans to merge those. From a transformation perspective, the pandemic has brought on an acceleration of this effort."

There is also agreement across organizations that their IT infrastructure was adequately prepared for this business disruption: 51% of respondents agreed with the statement and 23% strongly agreed.

"From a technical perspective, having already been relying on the cloud for our main systems was key," the security director continued. The academic medical center already had in place infrastructure to enable operations to continue as normal when a disruption occurred.

In order to ensure organizations are adequately prepared for the next disruption to business continuity, respondents reported several strategies their organizations are promoting:

- Bolstering IT infrastructure to support new digital solutions (42%)
- Improved risk management abilities (36%)
- Increased security protocols (32%)
- Redesigned business recovery plans (24%)

The current disruption has laid bare the strengths and weaknesses of business recovery planning. Given the importance of systems and data, IT must play a central role. Moving forward, organizations must take these lessons learned and work them into new, improved resiliency measures.

"IT is a silent partner that was engaged, but a lot of the time, there's not a lot of recognition," the security director for an academic medical center emphasized. "But we have received a lot of recognition for our ability to quickly help the organization move to a remote work environment, (and) be able to quickly pivot to use different tools or deploy computers to people who need to work remotely."

The survey results highlight some of the challenges organizations face to maintaining business continuity in the face of disruptions. No plan can account for every situation, but the right strategic approach will allow organizations to grow and adapt their plans, reshaping their strategies to prepare for threats to business continuity in the future.

PRODUCED BY

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

ABOUT RSA

RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, visit rsa.com.