CXO FOCUS

EXECUTIVE BRIEFING – BUSINESS AT RISK

BUSINESS CONTINUATION AND DISASTER RECOVERY

Nutanix Americas Healthcare CTO, Cheryl Rodenfels, shares insights from the front lines

One of the best ways that IT executives can keep up in the rapidly changing world of IT is through in-person interactions—to discuss and review use cases with peers, consultants, and vendors. Over the last couple of years, we've hosted a series of face-to-face sessions that allow senior IT leaders to interact, engage, and share insights and concerns about relevant topics. Recently, we held sessions on Business Continuation and Disaster Recovery (BCDR).
Below is a synthesis of these well-attended sessions by dozens of leading senior IT professionals.

A shift in focus: it's no longer just a line item for IT

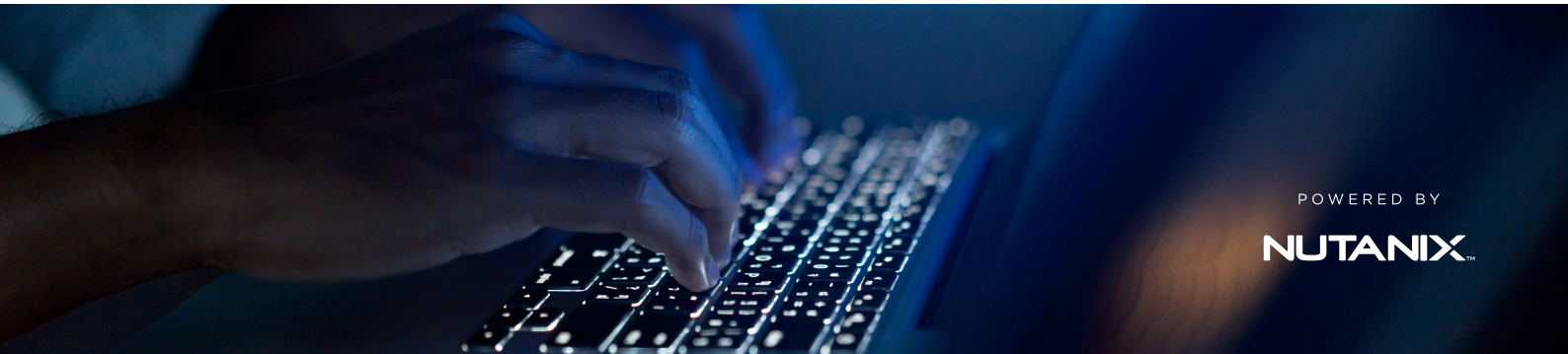
Every organization experiences a disaster recovery incident that impacts their operations. It truly is a matter of "when" not "if." From a simple application outage to a more complex weather or facility event, no one is immune to service disruptions. What is essential is how prepared they are to support the continuation of business functions when disaster strikes.

For IT leaders, the risk is real—and they are accountable for mitigating risk.

Traditionally, disaster recovery involved duplicating IT infrastructure and software systems in the event of a failure in the primary environment. All of the leaders we've listened to have shifted their focus from providing system availability to ensuring business continuation. They commented, "We can buy inexpensive hardware; we have duplicate services available through technology like backup data centers, hosted software, and [the] cloud; but we have to understand the business processes and priorities in order to provide the right solutions."

Senior IT leaders have become better partners with the organizations they support. They perform research on the many potential threats (technical, environmental, cyber); they understand the negative impact of such events to the business, the customers, the investors, and the community; and they raise awareness of the necessity to create response plans that can be executed quickly and effectively.

According to these leaders, "The investment in business continuation is constant. It's no longer just an IT line item. It's an organizational investment in time and planning, developing real-time processes with contingencies, creating multi-step communication strategies, and performing pre-disaster exercises."



A range of approaches with some common themes

While approaches to BCDR vary by organization type or market segment, there are some broad characteristics that define the two groups of organizations with whom we met:

1. **State, Local, and Education (SLED)** organizations mentioned being mission-oriented, and keeping the organization running is an expectation of their jobs. Two county CIOs and CISOs discussed the "all-hands-on-deck" approach, activating their plans and testing them against the new challenges introduced in California.

- "This year was different than other years. The threats were the same with the fires we experience, but the utility company began a series of rolling power outages. While we pay the telecom companies for priority service, that only helped us for a few hours. We had moved several of our systems to the cloud, but there was no internet available to access it. Additionally, our people lost power at home and had no way to access systems."
- "We found flaws in our communications plans as employee cell phones lost power and most of our team members no longer have landlines. There were worse traffic issues as the signal lights were out, so even the people we were able to contact had a difficult time getting onsite."
- "Everyone is expected to be available, and Public Safety is our number one goal. We will have to revisit several parts of our plan and adjust based on what we experienced."

2. **Private sector** CIOs were mixed in their approaches. One described their culture as having a "best efforts" approach to keep operations moving, and others had strong product and operational safety risks associated with power outages.

- A financial services CIO said, "We knew our systems were up and our processes were running. We only had a few critical people involved in managing the business. Everyone else was told to focus on their families and making sure everyone was safe."
- The CIO of a national poultry operation had major concerns and challenges. "We have an extensive investment in backup generators and water supplies to keep the animals healthy. We are able to pause processing if the power situation continues for extended periods of time. But our biggest concerns are trucking and refrigeration for processed chickens. We have USDA standards that must be followed and safe handling procedures. Anything that interrupts that can cause harm to our products and cause danger to consumers. We could lose entire shipments at great financial loss if we do not have appropriate safeguards in place."

> "If we cannot guarantee smooth operations, customers will lose trust with us."
>
> CIO - Global shipping organization

- The CIO for an extensive shipping operation described the impact of interruptions to their organization: "Our biggest concern is safety. We move tons of goods through daily. There are vessels and trucks coming and going. Everyone needs to know what is happening, where people are, ensure safe and effective loading and unloading, and track activities throughout the property. Corporations pay to have their goods shipped through us. If we cannot guarantee smooth operations, customers will lose trust with us and send their shipments to Canada or Mexico. We rely on continual operation to keep us in business. We have operations centers that run 24/7 to keep disruptions to a minimum."

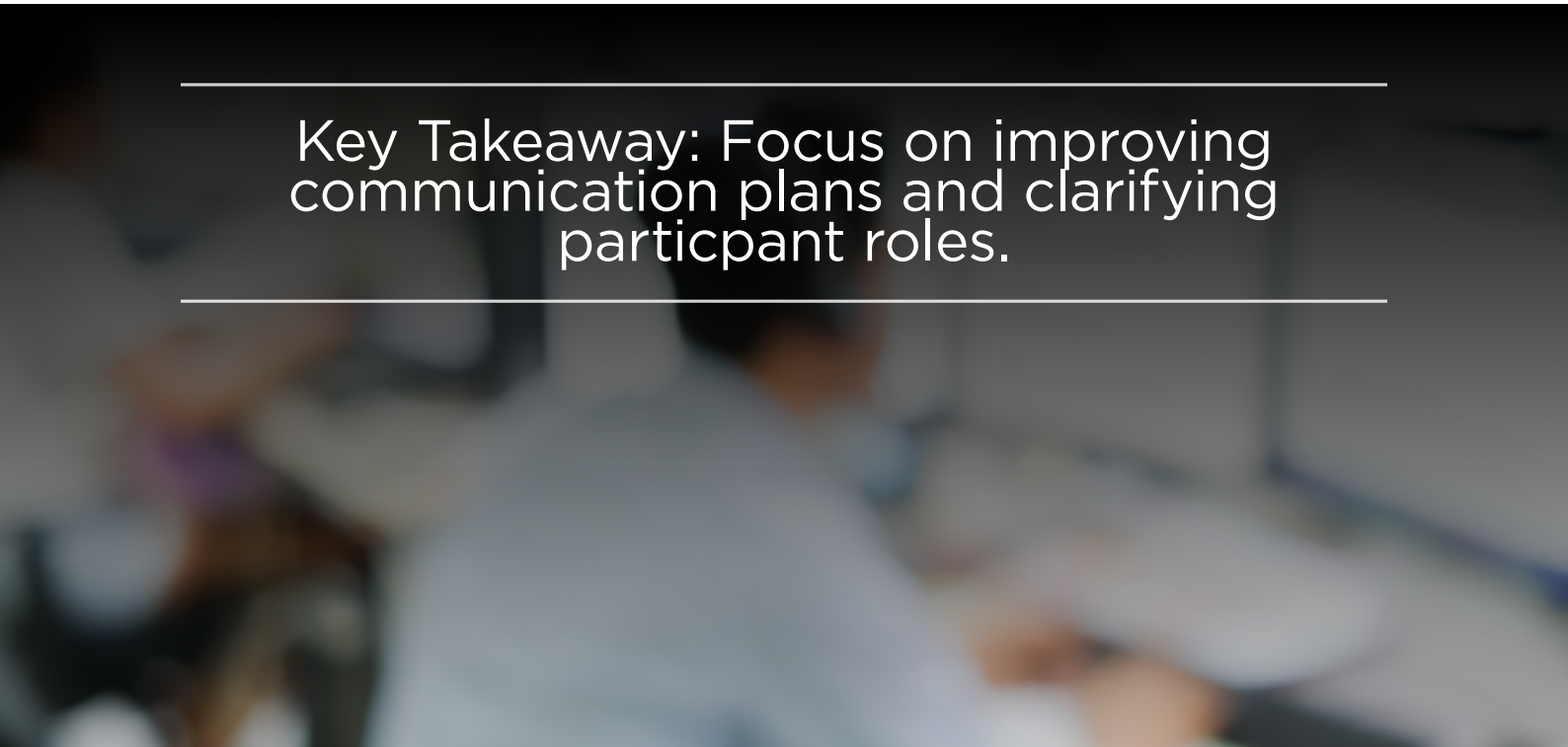
3. **Common themes** emerged, spanning both segments:

- All senior IT leaders agreed that cyber threats are increasingly seen as a BCDR incident. From small phishing attempts to large ransomware events, each of the organizations have had to create a cyber response plan.
- Even the most prepared organizations did not anticipate the impact of the rolling power outages.
- Their communications plans all needed some adjustment. They must align with their business peers to create effective response plans.

Key takeaways for IT leaders

Revisit BCDR plans and focus on improving communication plans and clarifying participant roles during events.

1. Many communication plans are developed in best-case scenarios. Have a Plan B and C ready for when new threats are introduced.
2. Most CIOs were looking into/had already invested in satellite phones for senior executives.
3. Know where your employees and participants live. Distribute responsibilities across your organization's geography to have a better chance at maintaining operations. ("All of our execs lived in one area of the county. They were responsible for leading the efforts and were least able to.")



Re-evaluate staffing plans.

1. A command center must be established.
2. Determine primary, secondary, and tertiary assignments to cover each role. You never know who will be available during any particular event.
3. Participants must be flexible and able to perform in any capacity.

Be mindful of all the ways your business is dependent on and integrated with digital technology. For example:

1. Public cloud. In previous business cycles, it may have been enough to have a redundant power source and replicated backup systems in place. Now, what happens to your applications, infrastructure, and/or public cloud when service providers are down? What are your "downtime" procedures?
2. Mobile phones. Batteries have a finite capacity. What alternatives and redundancies do you need and/or have?
3. Electronic BCDR plans. What happens when you can't access them electronically? Do you have a hard copy?

Business Continuation and Disaster Recovery continues to be a major topic in risk management, and today CIOs are responsible for mitigating both IT and business risks. While IT leaders may have a plan in place, these plans require continuous improvement and updates, given new variables like the recent public power outages and evolving cyber threats. As shown, the investment required is not just for IT services but also for the overall planning, testing, and awareness of the entire organization and its business functions. To paraphrase an old saying, when it comes to BCDR, use more than just an ounce of prevention to mitigate a pound of potential cure. Your business may depend on it.

AUTHOR 'S BIO:

Cheryl is a seasoned technology executive, having worked extensively across the client, consultant, and solution provider landscape. As CTO for Americas Healthcare at Nutanix, Cheryl's responsibilities include identifying and developing market opportunities, creating industry-specific training and documentation, enabling sales, and improving technology adoption and solution delivery. You can find her thought leadership across many leading organizations including HIMSS, CHIME, NCHICA, IDG, and Nutanix CXO Focus.