Strong Business Continuity Management Brings Resilience

At a Glance

Business continuity management (BCM) brings resilience to organizations as they transform digitally. For the greatest ROI from efforts towards resilience, CIOs should:

- Champion business requirements
- Consider the cloud as a way to build resilience
- Obtain buy-in from business leaders and steering committees
- Implement more disciplined validation and testing

Business disruptions happen every day and can cause companies to lose millions of dollars and suffer reputational damage. But these losses can be minimized. When astute executives, including CIOs, cheat disruption by focusing on business continuity management (BCM) programs that build resilience, interruption is conquered so that enterprise transformation can prosper.

CIOs should apply a business lens that informs how the business could be impacted (operationally, financially, legally, etc.) in the event of a disruption, and design solutions to minimize the impact. They must build resilience by analyzing the core operations driving the business and identifying critical business services. Understanding business requirements across the organization as they relate to resilience and remaining dynamic when business conditions change is key. As importantly, CIOs must account for the criticality and timing of each business process, from front-office processes such as sales and customer services to back-office processes such as human resources and finance.

Next-level organizations go a step further and use business continuity and resilience as a *competitive advantage*. Customers want to do business with organizations that do not miss a beat. Customers do not want to wait — they want what they want, when they want it, and that "when" is now. Companies that showcase resilience and build it into their value proposition gain a competitive advantage. But the issue of operational resilience expands beyond businesses. Supervisory authorities such as those in the financial services industry are bringing operational resilience into the limelight with discussion papers and proposals to enhance resilience.

Champion core business requirements

The CIO's customer is the business itself. As such, the business's needs must be understood. This is key to solution design. Proactivity also is a must. Asking the right questions for an understanding of the business's strategy and implementing architecture today that supports the technology of the future is fundamental. Similarly, CIOs and CISOs must anticipate technology needs to build an IT infrastructure that defends against cyberattacks. No longer a risk of tomorrow, cyberattacks are a real threat that BCM and IT leaders must be prepared for now. Understanding business requirements, from technology recovery requirements to data loss tolerance, enables a dynamic technology strategy that morphs with the changing needs of the business. To gain a strong business understanding, CIOs should evaluate:

- **Recovery time objective (RTO)** — The length of time a business process can be without key technology (e.g., business applications, data sets, devices)
- **Recovery point objective (RPO)** — The amount of critical data a process can afford to lose before there is intolerable impact — also known as data loss tolerance

Conducting a business impact analysis (BIA) is critical to identifying business requirements. BIAs enable an understanding of business activities and their outputs to position RTOs and RPOs as inputs into the transformation effort. However, completing a BIA is not enough — it must be maintained over time to allow for continued resilience as the environment changes.

Leverage cloud as a means to build resilience

The availability of robust, secure cloud solutions for disaster recovery represents a fundamental shift in disaster recovery planning. Cloud solutions can be more secure and provide better failover capabilities than businesses can accommodate with their own on-premise environments. For organizations that employ cloud technology for their production environments, resiliency and recovery are intrinsic to the platform, and disaster recovery capabilities are easily added. It is essential for these organizations to possess the expertise to govern and manage cloud implementations, keeping requirements of business process owners in the forefront. When businesses attend to these concerns, configuration of disaster recovery features in the cloud is reasonably straightforward.

Obtain buy-in from business leaders

The business continuity and resilience function cannot be performed in a silo. The CIO must ensure that technology solutions are designed and implemented with input and buy in from leaders across the enterprise, including C-level executives, operations, finance, legal, communications and HR, among others. Organizations should establish a steering committee composed of leaders across the organization who frequently collaborate on all issues related to BCM and resilience. Business leaders who are invested devote the time, people and resources needed for a successful BCM program.

Implement more disciplined validation and testing

CIOs must test against what could happen and stay disciplined in their validation and testing approach. A more disciplined methodology to validation and testing is essential to sidestepping shortfalls in meeting business expectations. If business leaders expect only 12 hours of downtime from a business interruption but technology workarounds require 48 hours, devastating consequences could ensue, including increased costs, reputational damage and other downstream effects. Testing and validation that back up technology assertions depended upon by stakeholders are elemental.

Collaboration is an all-way street

While technology is a driver for business resilience, it is not the *only* driver. People, processes and other factors must be considered. CIOs must understand the driving factors of C-suite members and, likewise, C-suite members must understand the driving factors of the CIO. Modern CIOs proactively collaborate to understand needs, and they ask questions that inform how IT staff can assist and what technology must do to fulfill business demands.

Impact on the C-suite

While the impact that disruption brings to each C-suite member can be industry specific, there are key considerations across all organizations regarding resilience.

- **Chief financial officer (CFO)** — Transaction processing delays cripple the CFO and the finance function by impeding the processing of financial information. With disruption, unplanned costs arise, most of which are the CFO's responsibility. Engaging the CFO and collaborating on planning for cost minimization are key.
- **Chief risk officer (CRO)** — Complying with regulatory guidelines may be challenging during times of disruption, especially in heavily regulated industries. Penalties for noncompliance — in addition to having to report such deficiencies to the organization's leadership — can be damaging. Designing resilient technology solutions enables compliance with regulatory requirements while also mitigating secondary fallout. Commercial insurance is another critical risk-mitigation tool used to reduce operational risks. Organizations may acquire insurance to protect the tangible assets (e.g., workers, equipment and buildings) of the organization and/or to defray the cost of unexpected liabilities (e.g., civil lawsuits, regulatory investigations).
- **Chief information security officer (CISO)** — The CISO develops the cybersecurity program for an organization and drives the IT security strategy and implementation while protecting the organization from cyber hacking and security threats. To ensure there are no gaps in IT and the cyber control environment, the CIO and CISO need to work closely together.
- **Chief audit executive (CAE)** — To optimize risk management, the CAE and the BCM function should work in unison to leverage technology for assessing and mitigating risk. BCM, enterprise risk management and internal audit must work together and apply uniform principles to their respective areas of responsibility.
- **Chief marketing officer (CMO)** — Understanding the impact of disruption — from viral pandemics to product delays — is key to a strong BCM program. Involving marketing in resilience efforts is extremely important to understanding which procedures are in place, how to supplement them and how to respond to a disruption event.
- **Chief operating officer (COO)** — Because COOs are responsible for operations that drive the organization, it is important to design technology solutions that can minimize disruption to those processes, which can vary by industry. Collaboration between the CIO and COO supports operational resilience by applying technology solutions that can minimize disruption and the subsequent impact to the organization.

What should companies do now?

A complete and deep understanding of the business is critical to mitigating disruption. To design solutions that minimize the impact of a business disruption, companies should assess their current BCM status. CIOs should inventory current efforts to maintain resilience and determine a desired BCM state and what they need to do to achieve it. It is important to eliminate or modify iterative technology to cut costs. However, while determinable costs are central, soft costs are just as important to mitigate. Idle personnel, employee morale and reputation costs that are not easily definable in dollars can bring down a business.

Organizations can optimize BCM ROI by continually understanding business requirements and designing complementary business and technology solutions that satisfy business objectives during enterprise transformation, inclusive of the following:

- Governance over resiliency efforts should be directed by a steering committee to assess and supplement policy standards, obtain C-suite buy-in and secure resources
- Key processes must be understood via the business-driven BIA, and the potential impacts of disruption must be addressed
- A strategic plan leveraging a BIA to minimize impact and plan for disruption is critical
- Implementing a disciplined methodology to validation and testing so that shortfalls in meeting business expectations can be avoided is imperative

Last, resilience is not a goal that is achieved. It is an ongoing effort earned over time. CIOs who cheat disruption by addressing resilience holistically support an organization's efforts to come back stronger in the face of adversity.

AUTHORS

MATT WATSON, Managing Director, Technology Strategy and Operations, Washington D.C.
DUGAN KRWAWICZ, Associate Director, Technology Strategy and Operations, Dallas
HIRUN TANTIRIGAMA, Director, Sydney

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, please contact us at TechnologyConsulting@protiviti.com.