ARCHER

WHITE PAPER

Navigating Uncertainty:
Strategies for Building Business Resiliency

Most, if not all, organizations have been impacted by disruptions including the pandemic, natural disasters, geopolitical events, cyberattacks, fraud, human error, or a combination of causes. These types of events impact consumer demand, employee health and safety, supply chains, cause physical damage, loss of customers and reputational damage, and exponentially increase the cost of doing business. Resources within the organization are spread thin even with one disruption, let alone concurrent and ongoing events that occur more frequently and tax not only the resilience team but also the rest of the organization.

The nature, frequency and magnitude of disruptions have caused organizations to evaluate their ability to recover from events – but even more the state of their business resilience. Business resilience has become a strategic imperative in addition to a regulatory, corporate, and board-level topic within many organizations across virtually every industry.

Organizations of all industries, size and location are discovering that they must build on their recovery capabilities and become resilient.

A survey by the Business Continuity Institute (BCI) found that 65% of organizations experienced at least one disruption in the past year that impacted their operations.

(Source: BCI impact of an attack)

Business Resilience

Business resilience is the ability of an organization to foresee changes, risks and disruptions and adapt in an evolving environment, and continue to deliver their objectives.

Business resilience includes, but is more than, business recovery; it is a change in mindset, culture and approach that drives resilient measures and practices throughout the business.

The maturation from recovery to resilience requires a cultural change starting at the top of the organization and cannot only be the responsibility of a small team – it requires focus throughout the entire organization.

Building a resilient organization requires a shift from a reactive to a proactive posture. Resilience must be built into the very fabric of the organization—from its culture to the business model to how the company operates both internally and across the extended third-party ecosystem.

Business resilience requires not only focusing on the recovery of internal processes and systems but developing the ability of the organization to be able to continue to execute their strategic and business objectives, including providing their important products and services to external parties, regardless of the length or type of disruption. There are six key focus areas that should be considered in building business resilience that includes:

1. Prioritize what is most important to make resilient.
2. Identify threats and mitigate the risks.
3. Test your resilience.
4. Build resilience both inside and out.
5. Inspire ownership across the organization.
6. Evolve from recovery to resilience.

Prioritize What is Most Important to Make Resilient

Every organization has a core mission and strategic objectives that likely include providing products and services to customers, revenue-generating activities, or other objectives that provide purpose for the company.

Building a resilient is complex and can be costly in terms of time and money, so it's impossible to make everything resilient at once. Organizations must define what is most important to make resilient. This is done by identifying their most important activities, products and services, or business processes. Because organizations are complex ecosystems this must include identifying the interrelated business processes, systems, people, assets, data, facilities, and external partners that all contribute. This is best done by performing business impact analyses (BIAs).

The BIA not only helps identify what is most important to make resilient, but also define metrics that describe "being resilient" or "not resilient enough". These metrics are traditionally recovery time objective (RTO), recovery point objective (RPO), and other related, time-bound metrics that are used to measure the organization's ability to recover after a disruption.

Progressive organizations are adding to these metrics by identifying and measuring other metrics that are tied to financial or business metrics – they are called impact tolerances. Impact tolerances are resilience metrics that define the point (in time, dollars, or other impacts) at which a disruption becomes intolerable. For example, impact tolerance could include the amount of revenue or customers the company is prepared to lose, or transactions that could go unfulfilled because of a disruption. For an airline, an impact tolerance might be cancelled flights. For a healthcare entity the impact tolerance might be unfulfilled prescriptions or untreated patients. It's up to each organization to determine the impacts they can tolerate from a disruption. Recovery and resilience strategies, plans, controls, and other measures should all be evaluated against their associated resilience metrics.

A study by the Disaster Recovery Preparedness (DRP) Council found that 73% of organizations worldwide are not properly prepared for a disaster or business disruption.

(Source: DRP Council)

Identify Threats and Mitigate the Risks

The other side to identifying what is most important to make resilient within (and without) the organization is to identify what could disrupt it. Each organization must assume that at some point a disruption will occur that will interrupt their ability to achieve their objectives. Therefore, the organization must identify the individual threats and combination of threats, or disruptive scenarios, that could impact the organization – specifically those that would cause them to exceed their resilience metrics and impact tolerances discussed above.

Scenario analysis is the art and science of identifying 'what could go wrong' including the potential threats, risks and disruptive scenarios that could disrupt the organization and then evaluate the organization's ability to be resilient enough to mitigate the intolerable effects.

The key to properly identifying and treating the threats is to take a holistic view of risk management across the organization. A challenge is many risk functions are in silos and primarily focus on their types of risk – operational, financial, third-party, etc. Therefore it is vital to take an integrated approach to risk management across these functions. One of the most important steps to risk management is to mitigate the effects of risks within your impact tolerances. For example, if the airline mentioned above is disrupted because of bad weather and has to cancel thousands of flights, is that tolerable? If not, they need to mitigate that risk by other means. This could include implementing other business measures, controls or plans to reduce the number of cancelled flights to within their impact tolerance.

Building resilience across an organization takes a coordinated approach and integrated risk management is fundamental.

Test your Resilience

Since it is not best to wait for a real disruption to see how well the organization responds, it is vital way to test the business measures, controls and plans the organization has put in place to prepare for and respond to particular threats or disruptive scenarios. The traditional way is to test recovery plans that have been developed. Most often these plans are tested via "tabletop tests" or simple walkthroughs. Although this is a good step, it is not enough. These measures and plans must be tested as fully as possible to determine how the organization really responds and what the real impacts could be. Only when this is done does the organization get a real picture of how resilient they are to the identified threats and disruptive scenarios.

Build Resilience Both Inside and Out

Third parties, external partners, supply chains and others are an extension of your organization and in some cases perform very critical functions for you. Your organization and these third-party organizations are often very closely intertwined in the achievement of your objectives, and if one is disrupted, the other may be impacted at the same time. Therefore, it is vital to ensure that your external ecosystem is as resilient as you need them to be. Myriad issues must be considered as your organization strives to build business resilience across your unique third-party ecosystem.

Third-party ecosystems are becoming more complex and specialized which complicates building resilience. For example, organizations may become dependent on a small number of outsourced or third-party service providers who are very difficult or impossible to substitute, which could, over time, give rise to systemic concentration risks. A major disruption, outage, or failure at one of these service providers could create a single point of failure with potential adverse consequences on your own financial stability, compliance capabilities, or reputation. This can be especially true of cloud service providers or outsourced data centers. In addition, sub-outsourcing to a third party's third parties (nth parties) can amplify certain risks in outsourcing arrangements, such as data security, or limit your organization's ability to manage them—particularly where large, complex chains of service providers are involved.

Third-party resilience is complicated to achieve because most of the control and responsibility lies with the external party. However, there are ways to build toward better resilience of your third parties. For example, during onboarding of a third party, service-level agreements and clauses can be included in contracts that stipulate the third party will take steps such as performing risk management and reporting findings or maintaining and testing their recovery plans. These agreements should cover how the third party will maintain business resilience under normal conditions and in the event of a disruption. Your organization can also monitor the third party on an ongoing basis through performance and resilience metrics, perform joint tests of recovery plans, and normalize procedures to align the resilience of the third party with your own over time. Agreement should be made that the third party will do the same for their third parties.

Third-party resilience is best achieved through a combination of upfront agreements and ongoing efforts that build resilience between your organization and the third party together.

An effective business continuity management (BCM) program is a vital part of the foundation to begin to shift focus on building resilience across the organization.

Inspire Ownership Across the Organization

Building business resilience cannot only be the responsibility of the resilience or recovery team but must be owned across the business—by each business unit and department, including IT, sales, public relations and more. Building business resilience may start with business recovery but it will not thrive without proactive participation across the business in building resilience into the way the organization operates, including its culture, business model, systems, and practices. Performance and reward systems should motive everyone to look for ways to make the organization more resilient.

A critical component is ownership of business resilience at the executive level. Executive ownership, such as by the chief operating officer (COO), chief risk officer (CRO), chief compliance officer (CCO), or chief information officer (CIO), provides the importance, sponsorship, and visibility to make and sustain progress against other business priorities.

Boards of Directors are asking more questions about the organization's resilience and this should be leveraged into action. Risk committees should be discussing the organization's resilience and risks that could impact it.

Evolve from Recovery to Resilience

An effective business continuity management (BCM) program is a vital part of the foundation to begin to shift focus on building resilience across the organization. A BCM program includes business continuity planning (BCP); IT disaster recovery (ITDR); incident management, which is the routine handling of small, business-as-usual events before they become a crisis; and crisis management, which is dealing with escalating crisis events. BCM teams are used to performing BIAs and understand the concept of business criticality and how that should drive priorities.

One challenge to overcome is the sometimes-disconnected nature of these functions. They are often separate teams with different tools, objectives, and approaches. Disruptions and crises result in enough damage by themselves, but the disconnected state of these teams can add to the risk, reduce speed to respond and result in more negative impacts. Integrating these functions builds business resilience by better aligning the organizations that deal with disruptions, using approaches that are more agile, practical, actionable, and tested—and reduce impact to the organization.

These teams should be the "tip of the spear" in helping the organization evolve from primarily focused on reactive measures and recovery to building resilience into the way the organization operates. This takes leadership, agreement by these teams that building resilience is a requirement and taking steps to make it happen.

Summary

Risks that threaten the resilience of your organization come in many forms—health crises, cyber threats, competition, business model changes, business incidents and supply chain disruptions. In fact, risks impacting an organization can often cause a domino effect. For example, weak security controls in a third party may result in a cyber breach to your organization. The breach may result in an exposure of your customer data (a compliance violation) and result in a disruption of systems that require IT disaster recovery, or financial losses and reputation damage. The interconnected nature of risks illustrated in this example demonstrates that building resilience isn't a siloed activity and resilience and risk management must be integrated across the organization.

As organizations mature their business resilience approaches, they must look holistically and proactively for ways to build resilience into the fabric of the organization. Concepts like redundancy, diversification and adaptability are important. It is just as important to build upon the BCM program, ensure executive ownership, align resilience and business risk, and build a resilient third-party ecosystem. Taking action in these areas will significantly enable the organization to build business resilience.

Discover More

Archer is a leading provider of integrated risk management (IRM) solutions that enable customers to improve strategic decision-making and operational resilience with a modern technology platform that supports qualitative and quantitative analysis driven by both business and IT impacts. As true pioneers in GRC software, Archer remains solely dedicated to helping customers manage risk and compliance domains, from traditional operational risk to emerging issues such as ESG. With over 20 years in the risk management industry, the Archer customer base represents one of the largest pure risk management communities globally, with more than 1,200 customers including more than 50% of the Fortune 500.

Visit www.ArcherIRM.com.