RSA

WHITE PAPER

Key Principles of Integrated Business Resiliency

It's hard to find an organization not impacted by at least one natural, man-made or cyber disruption in 2017. From earthquakes in Mexico, to hurricanes in the U.S., to severe floods in China, Peru and India—global and regional organizations were more impacted than ever this year. In fact, in the U.S. alone, 2017 tied the record with the second greatest number of natural disasters since 1990. Impacts from these events included employee health and safety issues, supply chain disruption, loss of customers, reputational damage, increases in the cost of doing business and physical damages—and the financial impacts can be astronomical.

Of all the disruptions in 2017, cyber breaches impacted the most people and industries, including gaming, hospitality, healthcare, financial services, government and retail. Cyber breaches impact the bottom line and business value of organizations of all size, industry and location.

Business resiliency has become a corporate objective and board-level topic within many organizations due to the liability and loss they have experienced or the pain they have seen their peers go through. The nature, frequency and magnitude of disruptions have caused organizations to evaluate their abilities to properly identify threats, analyze the risk and then implement plans to avoid or recover from events. With the increasing frequency of events, it is impractical to rely on recovery alone. Resources are spread thin even with one disruption, let alone concurrent events that tax not only the resiliency team but also the rest of the organization. Resiliency has to be built into the very fabric of the organization—from its culture to how the company operates.

Business Resiliency

Business continuity management (BCM), including business continuity planning (BCP) and IT disaster recovery (ITDR), is an absolutely vital part of a strategy to be resilient in the face of disruptions. A related and critical discipline is incident management, which is the routine handling of small, business-as-usual events before they become a crisis. Having good incident management procedures in place can keep small events from getting out of hand. Finally, crisis management is the art of dealing with actual crisis events. This involves not only handling the event (e.g., impacts to the company from a flood) but the ancillary exposure that often accompanies a crisis event, such as reputational damage, product recalls or data loss that can cause additional crisis events by themselves.

Even though BCM, incident management and crisis management are the most common components of an organization's business resiliency program, they are often disconnected and performed by separate teams with different tools, communication methods and approaches. Disruptions and crises result in enough damage by themselves, but the disconnected state of these teams can add to the risk and exposure.

Integrating business resiliency functions, especially incident and crisis management, will better align the organization's processes to deal with disruptions with plans that are more fluid, practical and actionable, and thus reduce risk to the organization.

Four key principles for integrating resiliency functions are:

- Prioritization
- Alignment
- Preparation
- Visibility

Prioritization

Today's organization is a complicated tapestry of interconnected business processes, IT systems, locations, people, third parties, information and assets. This complex web is the engine the organization uses to provide its products and services to the end customer. However, the dilemma manifests in several layers of questions: Can we identify all of the moving parts and do we understand the interdependencies between them? How do we build resiliency in and where do we start if something is disrupted? What parts of this complicated picture are most important to protect and ensure they are resilient? The first step in answering these questions is prioritization.

The business impact analysis (BIA) process determines prioritization. BIA is used to identify criticality and recovery objectives of business processes and the systems, information, locations and other components that support them. However, this cannot be done in a vacuum, and a critical step that is often missing is the alignment of determined criticality and recovery objectives to the corporate objectives and strategies of the organization. This is important because those objectives and strategies are:
1) what drive the mission of the organization
2) subject to change. As they change, goals for resiliency planning must change too.

Equally important is how criticality and recovery objectives of this engine align with the products and services they support. For example, if the number one product a stock trading business provides is online trading, that service can only be down for minimal time before it starts to materially impact customers. The entire engine supporting online trading—from the people to the processes to the technology—must be prepared for minimal disruption.

The results of the BIA—criticality of the business process and what supports it—must drive prioritization of resiliency measures, recovery planning and testing, and the resources allocated to it. However, this same prioritization should extend to the

level of effort expended to other areas, like what third parties support them, how incidents are dealt with, or even how crises are handled based on what is being impacted. In a large organization there can be hundreds of departments, business processes and systems, and it's not feasible to touch them all. Prioritization brings clarity to what is truly important.

Finally, BR teams, resiliency programs, recovery planning and all that is associated are often thought of as cost centers, a necessary evil or a "check-the-box" activity to satisfy auditors or regulators. A more effective prioritization process aligned with the organization's objectives, strategies, products and services will go far in demonstrating to executives that the BR program focuses on protecting business value.

Alignment

The individual functions of resiliency management—business continuity, IT disaster recovery, incident management and crisis management—can actually get in their own way and be an impediment in developing business resiliency. Often, these functions are within separate groups with misaligned processes and different tools. The BIA helps establish common business criticalities and recovery priorities; however, the way these groups work, the metrics they track, the reporting they provide, the communication mechanisms they use and how they address issues are often very different.

In recent years, the industry tide has turned to the need to build resiliency into the organization versus only thinking about recovery after an event. The term business resiliency denotes a more holistic approach to ensure the organization can bend and not break. This cannot effectively occur when the functions at its very heart are disconnected.

A consolidated, automated system that is used by all of these groups is absolutely vital to bridge the gaps. Common and integrated workflows, reporting, handoffs and issue resolution are just some of the capabilities that produce benefits of quicker response, better resource utilization and reduced losses. This system should also help to align business resiliency functions with others that are concerned about evaluating risk, such as an operational risk management function or a compliance group tasked to ensure measures are in place to adhere to laws and regulations. Automation can also help drive the necessary steps to better align incident and crisis management teams and their capability to more efficiently handle small events that turn into larger ones.

Preparation

The complex nature of business resiliency requires planning and practice. One example is recovery plan testing or exercising. Business resiliency takes this to new heights because the goal is for an organization to not only be able to recover after a disruption but to build resiliency into the very fabric of the organization's operations. This requires more than testing—it also takes process improvement.

Over the past few decades, various models have emerged for process improvement. Dr. W. Edwards Deming popularized a four-step process, the Plan, Do, Check, Act (PDCA) cycle, which has been widely adopted in business resiliency and crisis management approaches and standards. The steps are:

- Plan: Define the plan to improve a process.
- Do: Implement the plan and measure its performance.
- Check: Assess whether the desired results are being achieved.

Act: Decide on changes to improve the process, and then start the whole cycle again.

BCM teams are typically well-versed at exercising recovery plans. However, a critical gap is testing how plans merge together during real-life events. Cracks in the plans are evident—at the worse time—when dealing with an event that crosses individual teams. For example, a scenario where a chemical spill (incident) causes an evacuation of an entire facility (crisis event), and the company has to recover their business processes and systems that reside in that facility elsewhere (BC and IT DR planning), requires coordination across multiple teams. If that type of scenario is not fully tested, the execution when it counts will typically suffer. Another area that needs improving in most organizations is testing a wide variety of scenarios and "what could go wrong" in terms of not only internal company operations but what could happen on social media, with legal or regulatory authorities, third parties and other external dependencies. Finally, within any organization, resiliency cannot be the responsibility of a small group of people—everyone must have a role in building and practicing resiliency.

Visibility

Visibility is absolutely vital in building resiliency, especially across incident and crisis management. Getting the right information to the people who need it in real time, using dashboards, reports and information directly targeted to each actor, is a critical success factor. This includes putting the best measures and reporting in place so progress can be objectively evaluated and improved—both before and during an event. Information is critical in the middle of a crisis because decisions are being made quickly and decision-makers need the best information available to them.

Visibility has to be holistic—meaning information is communicated across BC, DR, incident and crisis teams, and provides decision-makers with information in business value terms they can do something about. For example, an executive must consider financial impacts of a potential disruption (risk) compared to insurance coverage. Further, aligning business resiliency to the objectives and strategies of the organization makes it much easier for executives to tie to the priorities of the organization and substantiate funding to continue to drive resiliency initiatives. Evaluating lessons learned after an event and acting on gaps not only go a long way toward process improvement but also bring crisis teams together as they come to understand the challenges that don't necessarily affect their immediate roles.

Visibility also includes association to other related disciplines, such as risk management and compliance, and a demonstration of how BR reduces risks to acceptable levels or strengthens compliance with laws and regulations. The tracking and reporting of metrics in real business value terms is what gets attention.

Summary

The nature, pace and complexity of impacts to organizations will not be slowing down anytime soon if the last few years, especially 2017, are any indication. Organizations that focus on building better prioritization, alignment, preparation and visibility into their business resiliency programs will have a much better chance of not only enduring in the face of these disruptions but also finding that they can use their ability to "bend but not break" as a competitive advantage.

Learn more about RSA Archer® solutions for business resiliency at rsa.com/grc.