Business Resilience and Crisis Management

Overview

Over the last year of the COVID-19 pandemic, business resilience has been tested unlike ever before. As we inevitably move into the second year of this crisis, C-Suite level executives need to assume responsibility for ensuring that their organizations can mitigate risk factors and continue to operate through this unprecedented time. Reviewing the stability of a company's critical business processes and underlying systems can help companies determine whether proper safeguards are in place to mitigate common operational risks.

Business Resilience Strategy

Business resilience describes an organization's ability to operate during a major disruption or crisis, with minimal impact on critical business and operational processes. While every business and organization across the globe is currently assessing the impacts of COVID-19 on their operations, it is imperative for organizations to have a business resilience strategy. An effective strategy to manage the operational challenges caused by COVID-19 comprises of several resilience disciplines including <u>Incident Management, Emergency Management, Crisis Management, Business Continuity Management, and IT Disaster Recovery</u>:

- **Incident Management:** Escalation and management of events which fall outside existing processes and/or systems. They are also considered by the organization as warranting special management attention.

- **Emergency Management:** Immediate response to an incident to manage time-critical threats to the lives and safety of individuals, the protection of assets under threat, and the risks of broader environmental impacts.

- **Crisis Management:** Management of strategic impacts of incidents, such as severe financial losses, reputational damage, and/or compromise to the organization's ability to achieve its strategic objectives or fulfill its mission.

- **Business Continuity Management:** Capability of the organization to continue delivery of products or services at acceptable, predefined levels – despite disruptive incidents – and to recover these services to a "business as usual" position.

- **IT Disaster Recovery/IT Service Continuity:** Response and recovery of IT systems and assets from significant outages, failures, or degraded service.

While the above disciplines are crucial for companies to implement, there are certain key focus areas which management must consider when developing its Business Resilience Strategy. Building an effective strategy that allows for an organization to respond to critical challenges can be significantly easier if the following factors are in place and working in unison:

Priorities

Priorities for managing incidents vary significantly from organization to organization. It is important that, wherever possible, your organization's priorities are documented and agreed to by the management team. For example, a company may state based on its company values, "We prioritize our staff safety and wellbeing." This means that the initial step in all responses is to account for staff whereabouts, with operational impacts only being addressed once an appropriate response has been initiated to support those affected.

Flexible Working Arrangements

Flexible working arrangements and technology supporting these practices provide organizations with a unique opportunity to distribute technology loads – minimizing peak demand on hardware, reducing the impact of site or transport disruptions, and providing staff with the space and time to manage other responsibilities related to family and community commitments. These practices cannot be implemented overnight and retaining productivity through the transition takes both planning and careful change management. Business leaders can initiate a conversation around how remote working would be used if required with your technology, risk, human resources, and operations team ahead of time to understand the likely challenges and opportunities.

The Right Team Crisis Management

The Right Team Crisis Management is a discipline that teams must learn and practice to enact a smooth and coordinated response. A response to a crisis often requires managers and executives to lead with multiple styles, concurrently. For example, operational functions may require a high degree of decisiveness, whereas strategic decisions may warrant broad stakeholder consultation and nuanced communication. Many leaders take time to adjust to this change. If possible, companies should invest in the training and development of several potential leaders who may be able to guide and/or support the function of a management team if required. If the organization lacks the ability to do this, companies may appoint different leaders to manage operational and strategic impacts – while ensuring regular communication and collaboration between both groups takes place. This will assist in ensuring each level of the response receives the appropriate focus where required.

Is Your Organization Equipped to Handle the Next Crisis?

While society is amid the COVID-19 crisis, business leaders need to take proactive steps to ensure they are prepared to mitigate risk and manage potential crises both efficiently and effectively. The initial step in being prepared to face a future crisis is building a Readiness Checklist.

1. **Be clear on management roles and responsibilities**

   Understanding key management and support roles for Crisis Management is central to an efficient and effective response. Business leaders should identify which key staff will lead response efforts, each supported by an appropriately qualified and experienced alternate/back-up wherever possible. Organizations need to consider:

- Who will lead the Crisis Management Team? Note: Ideally, CEOs (or equivalents) should not chair or coordinate meetings due to common, competing demands during the incident (i.e., public representation, liaison with key stakeholders, regulators, etc.)

- Are all critical functions represented in the team? For example: Legal, Technology, Operations, Finance, Insurance/Risk, Communications, Human Resources

2. **Agree on your organizational priorities and which key competencies must be maintained**

Crises must be managed in-line with an organization's values – being true to these is an important part of a response, particularly within internal and external communications. Beyond prioritizing people, many organizations face challenges in defining priorities for a response while experiencing the pressures of a crisis. Organizations need to consider:

- Is reliably poor service more important than an unreliable service?
- Could operating without typical resources jeopardize quality or safety, or create unintended consequences which are worse than the incident itself (unmanageable backlogs or excessive credit risk)?

3. **Know your exposure, and how impacts may manifest in your organization**

Many organizations do not have visibility of their most time-critical processes, key resources/inputs, interdependencies, or their tolerances for disruptions to these. Additionally, many organizations are unsure how a severe disruption may manifest for them. At a minimum, executive groups should agree on a prioritized sequence for resource and process restoration following a disruption. This includes a review of the company's Business Continuity Plan as noted in one of the sections below.

4. **Understand impacts during an economic downtown**

Let's say a large manufacturing firm is suffering from the effects of a recession. What happens to this firm will likely happen to other big businesses as the recession runs its course.

As sales revenues and profits decline, the manufacturer will cut back on hiring new employees, or freeze hiring entirely. In an effort to cut costs and improve the bottom line, the manufacturer may cut back on research and development, stop buying new equipment, and stop new product rollouts (a factor in the growth of revenue and market share). Expenditures for marketing and advertising may also be reduced. These cost-cutting efforts will impact other businesses, both big and small, which provide the goods and services used by the big manufacturer.

5. **Update your plans, strategies, and contact lists**

While management decision-making is a central part of any response, prepared resources serve to expedite responses and provide critical inputs to the process – namely, situational awareness and business intelligence. These inputs can assist with the sequencing, prioritization, and delegation of response actions in a timely manner – as well as the rapid analysis of impacts, including the identification of affected stakeholders. Consider the following when developing and/or reviewing your organization's plan:

- Is your organization clear on the timing of when your plan will be activated?
- What is your company's threshold for activation or tolerance for impact?
- How will your company assemble the right people and resources to facilitate a response?
- Which communication mechanisms will be utilized and how will you communicate with stakeholders?
- How do you intend to communicate in the early stages of your response? (i.e., town halls, key messages, frequency of communications)

6. **Plan to contact your staff quickly, and through multiple channels**

During a crisis, organizations may need to rapidly alert staff of safety-critical issues or distribute messages and instructions to teams across the organization as part of a response. This requires careful planning and rehearsal for all businesses, particularly where communication is reliant on personal information. When an intermediary is involved (such as call trees), complexity in the delivery of the communications, and the opportunity for introducing risks of inconsistent messaging across key staff is greatly heightened. If possible, use of a multichannel rapid notification system capable of SMS, automated phone calls, and email is best practice. At a minimum, key managers across the business should be able to rapidly contact their teams when required.

7. **Test your arrangements**

One of the most effective measures an organization can take to prepare for a crisis is to rehearse their response. This can involve management discussing a severe, yet plausible scenario, and applying the resources expected to be used in the event of a crisis – such as business continuity and disaster recovery plans. These tests must include individuals with identified roles in the response, and ideally their backups. The scenarios selected should be ones which create impacts to technology, third parties, people, and critical assets (i.e., buildings, plant, and specialist equipment), facilitating discussion of:

- How the crisis may impact the organization and its key stakeholders
- How the crisis should be identified and escalated to management
- What external support is available, and how to access it if required

- How to manage communications and engagement with key stakeholders
- How to manage operational impacts, especially disruptions and/or service degradations

A lack of a rehearsed response can also potentially have negative impacts on recovery. For example, backups are essential to be performed on a regular basis; however, if an organization does not perform restoration tests on a periodic basis, such backups may not be able to be relied on during a crisis.

Final Thoughts

The COVID-19 epidemic has had and will continue to have a significant and pervasive impact on business operations. Companies should consider these items above, and any other known impacts of the virus, on their operations when preparing and implementing their Business Resilience Plans and associated crisis management activities. Roles and responsibilities should be clearly defined, and companies should focus on their go-to-market priorities, especially during a time of economic unrest. Organizations should maintain a more frequent level of communication with their employees during such times. Additionally, business continuity and/or disaster recovery tests should be regularly performed prior to a crisis occurring to determine preparedness and understand if any additional precautions are warranted.

****

Please look for future updates on other risk management matters at www.fidatopartners.com

Contact
Justin DiGaetano, CRMA, CISA | Managing Principal, Risk Management

1001 Old Cassatt Road | Suite 200 | Berwyn, PA 19312
Two Commerce Square | 2001 Market Street | Suite 3230 | Philadelphia, PA 19103
jdigaetano@fidatopartners.com | 609 315 7186 (c)

www.fidatopartners.com
https://www.linkedin.com/in/justin-digaetano-08a953/

About Fidato Partners, LLC

Fidato Partners is the leading service provider of consulting and recruiting in accounting, risk management, and information technology in the Mid-Atlantic region, enabling companies to achieve greater growth and performance by filling critical resource and knowledge gaps. From emerging growth to global organizations, we provide the highest level of service to our clients. For more information, visit: www.fidatopartners.com.