DHG views

September 2020

Business Continuity Management

Jared Forman, Principal | DHG Advisory

Greg Crouse, Principal | DHG Advisory

Risk management is a key component to making informed strategic decisions, protecting reputation and safeguarding the sustainability of any business. Business continuity management is a key facet of risk management and aims to make sure companies are operationally resilient to business disruption to its people, processes and technology.

Any incident – large, small, natural, accidental or deliberate – can cause major disruption to the organization. Businesses that are proactive rather than reactive will be able to resume "normal" operations in the quickest possible timeframe.

Current Challenges

The disruptions surrounding COVID-19 and related stay-at-home measures have put existing Business Continuity Plans (BCP) to the test. Fault lines have been identified within these plans, and the deficiencies experienced by multiple industries spans the entire BCP spectrum. The most obvious deficiencies include a lack of preparedness related to people deployment and remote work capabilities. Other less obvious deficiencies relate to cybersecurity and supplier failures. It is vital for organizations to plan for and expect failures to occur; including those related to technology.

Some challenges and points to consider when creating your organization's BCPs include:

Understanding Your Business

Companies should understand which of their processes are deemed business critical activities and others which can potentially impact their financials or impair their reputation. Clear documentation of essential roles, responsibilities and tasks is paramount. Identifying essential team members is also important to the overall success of a BCP. For example, a data center team member may need to remain on the premises as certain job responsibilities may include cabling, racking servers, performing preventative maintenance and essential activities that cannot be performed remotely.

Additionally, understanding key processes within an organization and the assets aligned to them, from end-to-end, are inputs into identifying critical dependencies. Critical dependencies include the assets, applications, employees, suppliers and facilities pertinent to a company. The identification of a company's critical dependencies must be performed by a knowledgeable representative of the department/area.

Focus on Your Assets

When a disruption occurs, companies can be challenged with entertaining multiple priorities coming from multiple stakeholders. Companies should focus on activities that are customer-facing and operations that enable your teams to continue performing their day-to-day responsibilities. Focusing on these areas will prevent companies from adorning the morning journals. Ensuring your customers can call into the organization to perform their transactions and other activities is also essential to recovering from a business disruption.

Understanding Time

Recovery time is not created equally; therefore, a BCP should consider that not all dependencies are important at the same time post a disruption. Management should confirm any business impact analysis (BIA) correctly prioritizes critical business processes based on priority and risk to the organization. The ability to identify the impact of a loss and the organization's tolerance capacity are input into identifying the critical business dependencies. Companies should ask themselves if this critical process can sustain their recovery time objective.

Supplier Resilience

Evaluating the services suppliers render to your organization is critical in avoiding misaligned contractual terms. Understanding the contractual terms, how the terms make sense for your company and how you use the supplier can save organizations significant costs. Some supplier contracts are missing salient details that have a widespread impact, such as the recovery time objective (RTO). An RTO provides the length of time a supplier can be unavailable. The absence of this information can potentially render an organization helpless in recovering timely from a business disruption.

Cybersecurity Threats

Those seeking to harm companies have become extremely sophisticated in exploiting organization vulnerabilities. Certifying your BIAs factor in cybersecurity is paramount. An example of a new risk that may be introduced within an organization is firewall effectiveness. Companies should be certain that the firewall regime in place during normal operating times is as effective when an organization is experiencing a crisis and that their workforce is, in large part, remote. Those organizations should factor in cybersecurity controls due to different vendors having different risks or business impacts.

Process Inventory

Inadvertently omitting a business process can be easily overlooked in the process inventory listing. For example, departments who provide monitoring for the organization's uptime and downtime, or prepares key reporting for stakeholders, may be inadvertently omitted from the process inventory listing. Management should identify a mechanism to confirm that a reconciliation of the organization's business processes has all been considered in the evaluation of the company's BCP process inventory.

Supplier Risk Management

A new risk that can be introduced to an organization includes any alterations in the supply chain or supplier makeup. More and more organizations have fragmented supplier operations working in different geographic areas who modify their supply chain. For key suppliers, some companies enter into a secondary contractual agreement with alternate suppliers who are ready to perform those tasks in the event that there is a vendor disruption at an existing supplier. The contracts are not exercised until needed, and a nominal administrative fee is paid each year to maintain the vendor, therefore reducing concentration risk.

Workforce

Most employees, clients or customers do not foresee an outage, and therefore do not plan for one. However, identifying, training and documenting the names of the essential skilled employees assigned to execute a BCP, per business process, and their contact information is vital to resuming "normal operations" more efficiently and effectively.

Additionally, companies that do not plan for an outage may lend the workforce to scrambling for equipment, hardware, soft tokens, internet connectivity, access to VPN, etc. The key is to plan for a remote workforce, test the company's remote infrastructure and address any deficiencies in a timely manner. The results of the test are insightful and will position the company to increase their remote infrastructure capacity to meet the needs of the company's remote workforce.

Training and Testing

Many employees are not made aware of their company's business continuity program and have not been trained on their responsibilities as a member of the company. All employees, temporary workers and consultants should understand their role and be required to undergo an annual business continuity training that educates the team on what business continuity is and its impact to the organization if not correctly implemented and maintained. Additionally, business continuity management training could coincide with a company's annual security refresh training.

In addition, deliberately devising a plan to test the company's ability to perform critical tasks remotely during "normal" operating times will lead to better preparedness in the event of an outage. Ensuring the BCPs are continuously updated to align with the strategic goals of the organization is equally important.

Sustainability – Keep Your BIAs Current

When the business has undergone change, an automated mechanism to initiate a review of an existing BIA should be in place. Some events that could trigger a BIA review include acquisition, upgrade, divesture and when a business process is outsourced. Key stakeholders should be involved when assessing that your BIAs are current and up-to-date when there any substantial changes are made.

Conclusion

In conclusion, management is charged with the responsibility of taking measures to adequately prepare for and document the organization's resumption plans during an outage. Understanding your business, its end-to-end dependencies and putting a sustainable program in place are key to maintaining and recovering from an outage. While developing BCPs can be challenging, take proactive measures to make sure BIAs are current, correctly prioritized and address strategies that have been tested in order to lessen the impact to your organization.

We Can Help

DHG has extensive experience with business continuity management at Fortune 100 organizations. We have worked with these organization to confirm processes are in place to define leading practice on how an organization should respond in order to recover successfully from business disruptions.

We stand ready to help you navigate the new risk landscape and have the expertise and capabilities to assist you and your organization through this difficult time. We can provide a full suite of consulting support and have vast cross-industry experience helping our clients through short-term and long-term risk mitigation.

Contact us for more information: dhgadvisory@dhg.com.