Dear Mom And Dad: Here's What I Mean By "Business Continuity"

When family and friends ask me what I do for a living, I'm almost always greeted by the same blank, confused stare when I respond with "Business Continuity." To me and others in our profession, the words seem to fit the job. However, even business-minded individuals do not always understand what business continuity means, let alone the important role it plays within organizations. To complicate matters even further, the focus of business continuity has evolved over recent years and will continue to do so as new issues such as cybersecurity and privacy compliance gain more attention. In the simplest sense, the goal of business continuity is to enable an organization to continue fulfilling its mission, vision and objectives, even during the worst of circumstances. Regardless of what Murphy's Law, mother nature, or those with bad intentions throw our way, we have prepared our organization to succeed. By now, you must be asking what it takes to build a successful Business Continuity program and how I can best explain it to my family and friends? I find that it's less about the technical details and more about the strategy explained in my 5 Steps to Success:

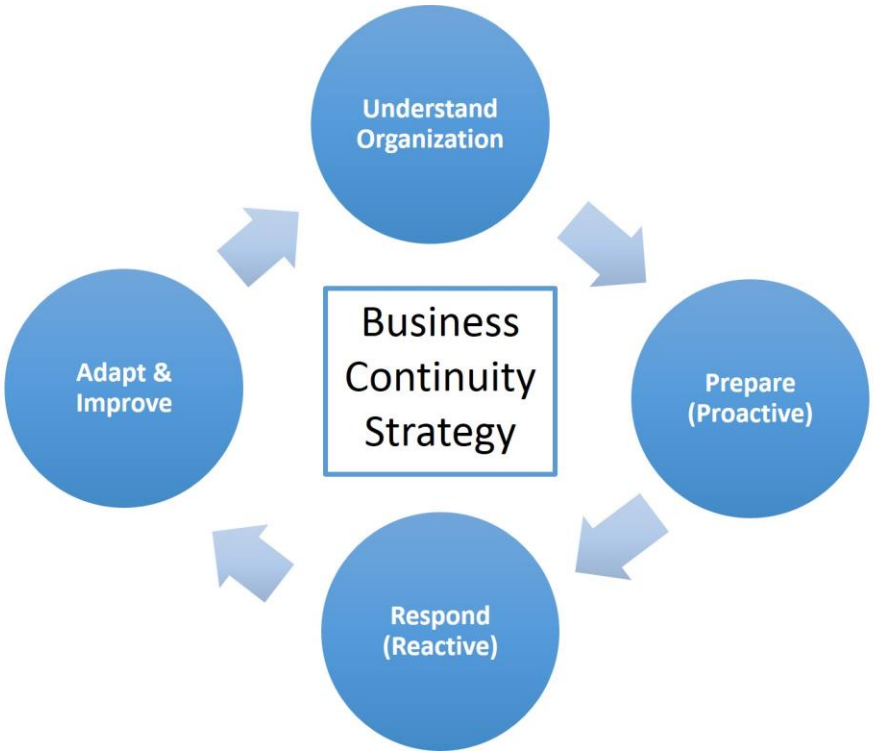
5 Steps to Success:

Step 1: Understand the culture and risk appetite of the organization. Each and every organization is different. This seems like a relatively simple concept, but truly understanding what makes your organization different is difficult; however, understanding its mission, vision, and culture is essential--the culture of the organization drives the risk appetite and the risk appetite drives the framework of the business continuity program. Senior leadership defines the organization's risk appetite, and the role of the business continuity professional is to build and maintain a program consistent with these risk tolerances. Notice I specifically used the term "organization" rather than "business." Not all organizations are run as businesses, and organizations like nonprofits or governments (and any other organizations who do not operate with the intention of generating profits) need to be equally prepared to respond to crisis (or even slow-burn disruptions). By recognizing the culture and risk appetite established by leadership, we can then focus on understanding the inner workings of the organization...

Step 2: Understand the inner workings of the organization. How is revenue generated (or does the organization even generate revenue)? What are the key processes that enable the organization to achieve it's mission? During the first 90 days on the job, business continuity professionals should meet with as many different teams as possible--from accounting, finance and HR to operations, engineering, and sales. Each and every department in an organization should play a role in advancing the mission (if not, why does it exist?). The thing to keep in mind is that while each team plays a role, not all functions are time critical during an unexpected emergency. Identifying which teams are time-sensitive during a disaster is crucial. It's important to note that just because a team is not time-sensitive doesn't make it any less important. For example, in a for-profit business, without sales the company will cease to exist--but generating new sales during a crisis isn't necessarily as important as meeting immediate obligations to existing customers. Next, the business continuity professional needs to understand how those time-sensitive departments operate and the key people, facilities, suppliers, and technology

required to perform the supporting activities. Priority should be placed on the departments that enable core products/services and departments which enable the organization to meet its critical obligations to internal and external stakeholders (employees, investors/shareholders, customers, users, compliance/regulatory organizations etc.). By understanding these inner workings, we can build a strategic plan to drive tactical execution…

Step 3: Develop a strategic business continuity plan to drive tactical execution. Risk, corporate security, and crisis management are tightly interconnected. It's impossible to anticipate or plan for every crisis scenario, so developing a strategic framework to drive and guide future tactical response is critical. Proactively building an environment to prevent or reduce the likelihood of a risk should be coupled with a reactive plan to respond to an incident.



Resources should be dedicated to trying to prevent a disruptive incident from occurring, but we can't let ego cloud our judgement. We need to recognize that Murphy's Law and uncontrollable incidents will get the best of us at times, and we need to be prepared to respond accordingly. Strategic planning should drive tactical execution, but we need to be pragmatic and thoughtful in how we allocate resources...

Step 4: **Be pragmatic.** When making resource decisions about the size and scope of a business continuity program, be pragmatic. Executives want to know that cost-benefit analyses are being conducted to understand the impact of potential risks (financial, reputational, legal). The investment in your business continuity program should be proportional to the risks faced by the organization and the acceptable pre-defined risk tolerances and culture. The "best" business continuity program is not necessarily the "biggest." Sure I can build you the Fort Knox of a

business continuity program, but that might cost more than the worst case scenario caused by a disruptive incident. It's not worth spending $100,000 to mitigate a risk if the maximum lost value is $50,000 (should the risk even become a reality). It's perfectly acceptable to accept a risk without mitigation efforts as long as this is a conscious, pre-planned decision and not an afterthought. On the other hand, organizations might be willing to spend more than the maximum value lost to mitigate certain brand or reputational risks based on company values or culture. It might be worth paying $200,000 to avoid a negative impact to brand, even if the estimated financial losses of a risk are estimated to be $100,000. Balance is essential to obtain executive buy-in as is the ability to adapt to the changing role of business continuity...

Step 5: Adapt. The business continuity function has continued to evolve, shifting from a focus on technical aspects to a broader understanding of risk and resilience. Understanding how an organization functions from a business, operational, and risk perspective is essential to leading a business continuity program. Every organization has different operational and technical requirements, so it's impossible to have the technical skillset in every discipline. Knowing the right questions to ask and where to go to find the answers is the most important skill.

The most successful business continuity professionals understand that they are advisors, not auditors. While certain industries required compliance with specific laws and regulations, business continuity professionals should seek to advise rather than mandate. This approach will help build buy-in throughout the organization, and stakeholders (who you often rely on) will be more eager to partner with the business continuity team.

Conclusion: Sometimes complicated technical approaches tend to get in the way of progress. By taking a step back and carefully crafting a strategic business continuity program rather than pages and pages of complex details, we can be more agile in our planning and response. Afterall, who has the time to read 300 pages of documentation in the midst of a crisis? Sometimes simplicity is best. In the words of Leonardo da Vinci and Steve Jobs, "Simplicity is the ultimate sophistication."

About the Author:

Follow @BryanWeisbard on Twitter:
https://twitter.com/BryanWeisbard

Connect with Bryan Weisbard on LinkedIn:
https://www.linkedin.com/in/bryanweisbard/

Bryan Weisbard, CPA, CFE, is Head of Security Analysis, Investigations & Business Continuity at Twitter. In this capacity, Weisbard's team identifies, analyzes, and mitigates risks posed to the company from a geopolitical and corporate security perspective. Weisbard also leads all business continuity and crisis management functions globally. Prior to joining Twitter, Weisbard served in a variety of national security roles with the U.S. Government, both in the Washington D.C. area and overseas. Weisbard holds an MBA from the University of North Carolina at Chapel Hill, a Bachelor of Business Administration from the University of Miami, and a Certificate in Forensic Accounting from Georgetown University. Weisbard is a Certified Public Accountant (CPA) and a Certified Fraud Examiner (CFE). Weisbard serves on the Membership Committee of the CSO Center for Leadership & Development and is a member of The Pacific Council on International Policy and OSAC's Pan-Asia Regional Council (PARC) and Media & Entertainment Working Group (MEWG). Weisbard also serves as President of the Board of Directors

for Up On Top School Program, a 501(c)(3) charity providing free educational programs to children from low-income families.