Business Continuity and You - Tips, Tales, and Tools

A Security Executive Council Thought Leader Paper

By Dean Correia, Emeritus Faculty, Security Executive Council

Business continuity planning identifies an organization's exposure to various risks while bringing together various resources in order to provide effective assessment, preparedness, response, and recovery from risks negatively impacting the organization. Business continuity planning is an ongoing strategic practice governing how business is conducted. Long-term, fact-based, strategic business plans designed to attain the objectives of the business must be supported by parallel plans intended to ensure continuity of business operations regardless of the type of threat or risk encountered.

Business Value of a Business Continuity Program (BCP) and its Services

Over the past few decades, business continuity planning has evolved from something undertaken by a few companies, primarily for compliance purposes, to a mission critical part of every organization's annual strategic planning process.

In an ever-changing global economy, companies are challenged to maintain their position as leaders in their industry. A requirement of maintaining a leadership in the market is an understanding of various types and levels of risk. Business risks are unavoidable, quantifiable, foreseeable, manageable, and must be taken, especially by leaders.

In today's marketplace, all companies have a clear need to establish and execute a comprehensive BCP. If challenged with a critical incident, a company must be able to respond in the quickest and best way possible for their employees, customers, business, brand, and external stakeholders. The 4 pillars of an effective business continuity program should include:

1. An assessment of key organizational risks and their impact on the business.
2. Planning activities associated with specific incident preparedness in order to have an effective and coordinated approach to BCP and operational readiness
3. Incident response plans that mitigate the damage to people, assets, and brand should the organization become impacted by one of these key risks.
4. A documented incident recovery process that prioritizes the fundamental criticality of the process and other factors, including relationships to other processes, critical schedules, and regulatory requirements, as identified in the risk impact analysis.

Crisis Management

As today's security leader how do you show program value, both qualitatively and quantitatively? Why not start by asking your leadership team the question that business continuity planning often answers – "What if?" Not having an answer to this question can easily spell the difference between continuing operations versus bankruptcy.

Considering reviewing a few of these scenarios with leadership, tailoring them to align with your specific organization's top risks:

- Your company's network goes down for a day. You can't serve your customers who now start calling your competitors for service. What would you do?

- The local news is reporting that one of your company's products is responsible for the death of a local resident. How will you react to ensure that employee, consumer, and vendor confidence is maintained in your brand?
- A flu epidemic has broken out in your city. Its symptoms are debilitating and if left untreated, fatal. What precautions will you take and how will you maintain operations if the epidemic causes mass absenteeism?
- A local chemical spill shuts down your facility
- One of your employees has been murdered in a botched robbery attempt.
- A Category 3 hurricane is bearing down on your home office and 5 of your facilities.

I've been involved in managing some of the incidents noted above over my career. One specific incident that will always resonate with me was the SARS (Severe Acute Respiratory Syndrome) epidemic in Ontario in November2002. There was very little known information about the virus at the time. We had people and facilities immediately impacted. Four key challenges and learning from this crisis were:

1. The initial information stage of managing a crisis is like sipping water from a fire hose. Information is being received and sent in very large volumes. It is critical to have reliable sources of information close to the scene.
2. Take care of people first. Ensure employees are checking with their loved ones first to make sure that they are OK. Your employees cannot manage a crisis well if they are anxious about the well-being of their loved ones. Ensure that your employees and customers receive details of how you are taking care of them. If you don't, misinformation will be taken as fact as people are craving direction.
3. Have a clear plan. Ensure that people know their roles. Conduct regularly scheduled table top exercises (TTX) to sharpen and improve your plan. Prior to this incident, we believed that we had a robust communicable disease plan. Afterwards, we improved our plan. Some of these improvements would have come to the surface had we conducted a TTX beforehand, thus saving valuable time, energy, and resources.
4. Every crisis is a leadership opportunity, as an organization and as individuals. Don't assume that due to someone's title that they will or won't handle a crisis well. Managing a crisis takes a team. As a leader, remove the obstacles that may impede the experts from focusing on their specialty.

When terrorists first set off explosives at the World Trade Center in 1993, approximately 44% of businesses ceased operations at least temporarily due to the fires that raged. About 150 of the 350 businesses affected closed their doors for good. After this event, many companies implemented business continuity plans. When terrorists brought down the Twin Towers on September 11, 2001, some companies once again ceased operations permanently while others with comprehensive continuity plans were up and running again in days. Depending on your industry segment, studies have shown that 1 hour of downtime costs a business anywhere from $51,000 to $1,000,000 per hour.

Summary

Here are some lessons that I and my fellow colleagues have learned throughout the years about business continuity and crisis management specifically:

1. "I don't have time" - You can't afford to not be prepared. Garner buy-in from your "C" suite. Educate stakeholders. Learn to communicate the benefit of having a robust BCP and current incident response plans to all functions in your organization. Develop a team approach and make your BCP part of your organization's culture and not an incident based event.
2. "I don't know how to do this" – Most of us are not experts in every security function under our responsibility. Talk to colleagues and benchmark. Seek out organizations and resources that provide experience, guidance, and proven practices.
3. "We have insurance" – clearly, this is not enough. Plans are critical. Review the four pillars above. Establish crisis response teams, phone lists, and meeting areas. Conduct table top exercises to test and improve these plans.

The leadership required to manage each crisis is unique, truly situational. Before each one, the companies that I was with had a decent plan in place. After the incident recovery phase, we had a better plan. Regardless of the maturity of your security department, there are always key learning that come from incident management which enable you to better protect people, safeguard assets, and optimize profit – factors that appeal to every function in every organization.

Is your organization ready? The checklist below provides a simple checklist to help you answer this question.

Business Continuity Program (BCP) Checklist

Documented BCP Components	I Have It	I Don't Have It	I've Tested It (if applicable)	I Haven't Tested It (if applicable)	It Works	It Failed
BCP Purpose						
BCP Legal Requirements						
BCP Scope						
BCP Policies						
BCP Objectives						
BCP Budget						
BCP Advisory Committee						
BCP Records						
BCP Roles & Responsibilities						
BCP Training Needs						
BCP Annual Review						
Hazard Identification						
Business Impact Analysis						
Vendor Resiliency Questionnaire						
Mutual Aid Agreements						
Communication Systems						
Table Top Exercises						
Response Goals						
Incident Notification & Escalation Levels						
Crisis Management Team (CMT) Members, Roles, &						

Business Continuity Program (BCP) Checklist

Documented BCP Components	I Have It	I Don't Have It	I've Tested It (if applicable)	I Haven't Tested It (if applicable)	It Works	It Failed
Responsibilities						
CMT Locations (2)						
Emergency Operations Centre (EOC)						
Response Procedures						
Incident Damage Checklist						
Incident Recovery Records						
Incident Corrective Action Plans						

About Dean Correia

Dean Correia, Contributing Editor of the book, Business Continuity Essentials Playbook: A Framework with Tools to Create or Enhance Your Business Continuity Program, has had a career in operations and loss prevention in Canada spanning more than 20 years, holding senior leadership roles with global brands GAP, Starbucks Coffee, and Walmart. Dean is skilled at influencing stakeholders to embed an enduring legacy through process improvements and the creation of sustainable programs that contribute profit and add value through the protection of people and securing of assets.

Dean is a Certified Protection Professional and Licensed Private Investigator whose other certifications include Handwriting Content Analysis, Interview/Interrogation and Executive Protection. An experienced workshop facilitator and passionate public speaker globally, Dean is an Emeritus Faculty member of the Security Executive Council, the leading strategy, insight and resource provider for risk mitigation decision makers founded in 2005.

Dean served a three-year term on the Board of the US based National Food Safety Security Council and has been an engaged member of the Retail Council of Canada for more than a decade, having led the national Loss Prevention conferences for both of these organizations in 2006 and 2008 respectively.

Some of Dean's career highlights include successfully leading Walmart Canada's security event planning for the 2010 Vancouver Olympics and the G8/G20 summit. Dean spearheaded the creation of Business Continuity and Crisis Management plans for Walmart Canada and Walmart Canada Bank. At both Walmart Canada and Starbucks Coffee, he played a key role in the creation, development, and implementation of auditing and investigative programs that delivered millions of dollars to the bottom line.

Dean's publications include the February 2007 and September/October 2008 editions of Canadian Retailer magazine. In 2001, Dean was awarded the Spirit of Starbucks for his impact on the business in the U.S. and Canada.

About the Security Executive Council

The Security Executive Council is the leading research and advisory services firm for risk mitigation solutions. We offer risk mitigation leaders trusted and experienced advice, program decision assurance and help to get all their projects successfully done.

The Council develops proven practices that provide an array of strategies and tactics to solve pressing issues based on your situation. With a large community of subject matter experts (successful former security executives and current industry specialists) we work one-on-one with Tier 1 Security Leaders™ to help them reduce risk and add to corporate profitability in the process.

Through our pioneering approach of Collective Knowledge™ we serve businesses from all industries and sizes, government agencies, educational institutions and NGOs to help them effectively address their risk concerns. Are you interested in learning more about *Business Continuity and You - Tips, Tales, and Tools*? Contact Dean at contact@secleader.com.