SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Resilience >

Business Continuity and You – Tips, Tales and Tools

Created by Dean Correia, Security Executive Council Emeritus Faculty

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 are:

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.

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

- Your company's network goes down for a day. You can't serve your customers, so they 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 five of your facilities.

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.

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 Severe Acute Respiratory Syndrome (SARS) epidemic in Ontario in November 2002. There was very little known about the virus at the time. We had people and facilities immediately impacted. Four lessons learned 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 wellbeing of their loved ones. Ensure that your employees and customers receive details of how you are taking care of them. Otherwise, people who are craving direction will take misinformation as fact.

3. Have a clear plan. Ensure that people know their roles. Conduct regularly scheduled tabletop 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.

Launching and managing a BCP is not an easy task. But the reasons companies and security leaders give for not developing one can be easily countered:

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 rather than 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 tabletop exercises to test and improve these plans.

The leadership required to manage each crisis is 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 is always key learning that comes from incident management, which enables 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 can 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	I Haven't Tested It	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						

Documented BCP Components	I Have It	I Don't Have It	I've Tested It	I Haven't Tested It	It Works	It Failed
Incident Notification & Escalation Levels						
Crisis Management Team (CMT) Members, Roles, & Responsibilities						
CMT Locations (2)						
Emergency Operations Centre (EOC)						
Response Procedures						
Incident Damage Checklist						
Incident Recovery Records						
Incident Corrective Action Plans						

Visit the Security Executive Council website for other resources in the Program Best Practices: Resilience series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/