Business Continuity Planning - What's Trending?

Monica Goldstein, COO, RecoveryPlanner

Monica Goldstein, COO, RecoveryPlanner

Are you prepared for all aspects of your next big incident — or is your Business Continuity Plan (BCP) stuck in the past?

In a world where Cyber Security incidents and natural disasters stop global businesses in their tracks, do your Plans reflect new technology strategies, recovery procedures and policies of today or is your annual routine made up of "get through an audit"?

"With your supply chains, look at the entire chain and each of the risks associated with each supplier and how they can be mitigated."

This article provides some ideas on how to address 2016 business trends in your Recovery Plans based on our experience with working with 100s of organizations on their Business Continuity and Disaster Recovery Plans.

The Cyber Threat (Cyber Attacks, Data Breaches, Security Incidents)

What is your organization doing about the cyber threat?

It's real AND it's not if it will happen, it's when it will happen and how will your organization handle it.

There are more than enough examples in the headlines about companies affected by cyber-attacks. Although we do what we can to prevent attacks, it is just as important to be able to detect and counteract intrusions quickly and focus on recovery time. This is where Plans come in - here are some planning tips to prepare for cyber incidents:

□ Detection, Response, & Mitigation. This refers to the steps cyber incident management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities.
□ Develop a Cyber Security Incident Response Team connected to an IT Cyber-security scenario or create a specific Cyber Incident Response Plan.
□ Incorporate resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions, the destruction or corruption of data, and to recover ongoing operations during and following a cyber incident.
□ Require third-parties to notify you of a security breach, define the time frame of the notification and the notification process.
□ Escalating and Reporting. Define notification to appropriate stakeholders as required, such as, regulators, law enforcement, and customers. Inform the key stakeholders about the impact of the cyber incidents.

Workforce Resiliency

Today, there is much more focus on the continuity of the workforce than ever before ("Workforce Resiliency"). As a result, IT will need to be able to support the recovery strategies of having a large portion of the workforce working from alternate locations, such as, from home, from a hotel, or another company location, if an incident occurs. They will be using mobile technology and computers, both company and personal, that will need remote access. Issues to consider with this are ones like does the company authorize the use of home computers, is the home computer setup for their business needs (such as the correct images), and does the home computers

meet the company's security standards? If you expect them to use their company laptops, are they taking them home each night? Is this a policy? Is there enough capacity or licenses for everyone to log-in remotely and at the same time?

Consumers have Lower Tolerance for Downtime

Today, consumers want things instantly and expect no interruptions and when they do occur, the time recovery expectancy is minimal. Demand for "always-on" operations and resilient IT operations have increased. You need to ensure that your Disaster Recovery Plans have strategies for meeting consumers' lower tolerance for downtime, such as cloud computing.

Crisis Management

What technologies is your organization using to support crisis communications? It is essential that in managing a crisis a company provides information through multiple communication channels both within and outside the organization. Today companies are taking advantage of automatic notification systems, virtual command centers and mobile apps. They are also thinking through what if the internet or phones are unavailable and considering the use of alternate communications like satellite phones and radio.

Social Media will also be part of the company's Crisis Communications Plan. Often a Crisis Communications Plan will include a Social Media Team or Position that will include tasks such as checking social media to see what is being said about the organization due to the Incident and responding to those comments. Also the organization will utilize social media channels to communicate information related to the Incident.

Supply Chain / Third Party Disruption

In 2016, planning for disruptions with your third parties, such as outsource providers, IT third party providers, and those in your supply chain is vital. You may be prepared, but if your providers are NOT, then you can be impacted since in most cases they perform or support critical operations. Here are some basic steps for Third Party Continuity Management:

□ Identify

• Identify and document your critical suppliers, partners, and other third party providers.

• Do your Due Diligence of the third parties.

• Review and document pertinent contract terms related to continuity, like SLA's and RPO's.

• Determine and document the alternatives if an incident should happen your supplier.

• With your supply chains, look at the entire chain and each of the risks associated with each supplier and how they can be mitigated. Evaluate if something happens to one how it will it affect the entire chain.

□ Measure

• Investigate or validate the recovery readiness of your third parties.

• If you rely on them to have sufficient recovery capabilities within your established RTOs, you need to measure if they are doing so.

• Attain, review and/or audit your third parties' Business Continuity Plan.

□ Monitor

• Include business partners in your DR/BC testing at least once per year, especially of your critical suppliers.

• Ask to be part of your business partners' tests/exercises.

Although there are great frameworks and standards, like ISO 22301 and DRI International's Best Practices, to guide us in building and maintaining our Business Continuity and Disaster Recovery programs - these are just FRAMEWORKS. You need to continually evaluate how current threats affect your facilities, personnel, business processes and resources and address them in your Plans.