Business Continuity Awareness Week, March 17-21, 2014
Day 3: Business Continuity Requirements & Standards

Midway in this five part series and the topic is "requirements and standards?" At this point you might be questioning my sanity and I will admit it is not the most exciting topic, but it is important and no one wants to read about standards and requirements on a Monday or Friday. So here is the bottom line: you're required to do some things, highly recommended to do other things, and some things are voluntary. Clear as mud right? Maybe just a little more detail is required.

REQUIREMENTS:
- The OSH Act of 1970 general duty clause requires an employer to provide a *"place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees"* (Sec. 5.(a)(1)). This idea has evolved to include reasonable threats such as natural disasters or man made threats. An employer is expected to prepare for threats that could harm your employees at work. If you can't prove you took reasonable actions to comply with this concept, you could face fines and severe liability in court.
- OSHA 29 CFR 1910.38 requires employers to have an Emergency Action Plan (EAP) to inform their employees what actions they need to take during an emergency. OSHA has some general guidelines of mandatory and recommended topics. In my experience these minimums are a good start but there are other aspects you should include in your EAP. Developing an EAP for your company is also a good way to show compliance with the general duty clause.
- Sarbanes-Oxley Act of 2002 mandated financial controls for publicly traded companies which includes requirements for a risk management program. Many more companies are impacted by the law than initially thought and they have realized that a business continuity program is an effective way to comply with the risk management requirements.

STANDARDS:
Although these standards are not mandatory, many businesses find they are required to comply with contract requirements, customer expectations, or to be able to compete in certain markets. Companies can pursue voluntary certification to these standards based on their company needs with participation in the Department of Homeland Security PS-Prep™ program.
- NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs
- ISO 22301 (replaced BS 25999) Societal Security -- Preparedness and Continuity Management Systems
- ASIS SPC.1-2009, Organizational Resilience Standard

So there are the main requirements & standards dealing with business continuity in the United States. Other countries have their own programs and if you do business internationally, be advised they may have more stringent requirements than what we have here in the US.

As always – Be Aware, Be Prepared, Be Safe. *– Brian*