

National infrastructure protection plan nipp vs business continuity plans essay

[Law](#), [Security](#)



National Infrastructure Protection Plan (NIPP) vs. Business Continuity Plans

National Infrastructure Protection Plan (NIPP) is a collective framework incorporating several efforts that are meant to increase the safety of a nation's critical infrastructure. The main objective of NIPP is to make America more secure, safe and resistant. This is done by neutralizing, preventing and deterring or mitigating attack by terrorists. It also makes the country more strengthened and ready for these attacks and carries a reliance on recovery and response in the event the attacks take place. It is an effort of the federal government and both government and non-government agencies. Critical infrastructure is of core importance to the economy, public health and safety, national security and day to day life. It includes the networks, systems and assets whether virtual or physical which if destroyed or weakened would lead to paralysis of everyday life in America(Purpura, 2007 p. 36).

Some of the sectors, in addition to the ones already mentioned, that seek to be attacked are banking and finance, chemical, communications, agriculture, Information Technology, Energy among others. The paralysis of the society is minor as there is also human casualty that can be suffered as well as loss of copious amounts of data. National Infrastructure Protection Plan finds a way to prevent attack by making all stakeholders aware of loopholes that can be used in destruction of the society. With this information the companies or organizations realign their strategies to enable avert attack. New protection methods are suggested and applied and there is also a difference in approach to society at large. The protection plan also allows for room of error

with evacuation plans and salvage plans thought of should the main strategy of prevention fail (Broder, & Tucker, 2012 p. 48).

A business continuity plan on the other hand is a document that recognizes a company's exposure to external and internal threats and outlines methods that can be used to continue with operations despite these threats. It is a plan for a continuity of tasks under hostile conditions and relies heavily on risk management. Sometimes it is used as a tool for organizational education in an effort to reduce risk and also as a write-up in back up plans when starting a business. A business continuity plan is standardized for both the government and private sector and there are instructions in The United Kingdom that instruct the local authorities to plan and prepare actively for crises (Purpura, 2007 p. 94). The process of coming up with a BCP manual involves carrying out analysis on the threats, impacts and scenarios that would lead to a business catastrophe. This analysis is the Business impact analysis. Next is done the threat risk analysis and then recommendations are made on how to avoid the risks and threats.

Of the two the NIPP carries more weight than the BCP because it involves action before and after the threat. The Infrastructure protection plan makes its first priority protection while for the BCP continuity is the first and only priority. If a threat were to paralyze an avenue for continuity in the BCP then in many if not all chances the business is bound to fail (Broder, & Tucker, 2012 p. 81). There is also a heavy borrowing on methods used by past people and little innovation with the BCP evident in this is the use of structured outlines to draw its plans and its stringent implementation by law.

This raises eyebrows as to whether people write it for its importance to a business or because it is a requirement to business.

Reference

Broder, F. J. & Gene Tucker, G. (2012) Risk Analysis and the Security Survey.

Oxford: Elsevier Science, 2012.

Purpura, P. (2007) Security and Loss Prevention: An Introduction.

Amsterdam; Burlington, MA: Elsevier/Butterworth-Heinemann.